PCI DSS Requirements	Testing Procedures	Guidance
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	**11.2** Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follows:	A vulnerability scan is a combination of automated or manual tools, techniques, and/or methods run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals. There are three types of vulnerability scanning required for PCI DSS: • Internal quarterly vulnerability scanning by qualified personnel (use of a PCI SSC Approved Scanning Vendor (ASV) is not required) • External quarterly vulnerability scanning, which must be performed by an ASV • Internal and external scanning as needed after significant changes Once these weaknesses are identified, the entity corrects them and repeats the scan until all vulnerabilities have been corrected. Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or cardholder data.
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. **11.2.1.b** Review the scan reports and verify that all "high risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved.	An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked "High" per Requirement 6.1) should be resolved with the highest priority. *(Continued on next page)*

PCI DSS Requirements	Testing Procedures	Guidance
	11.2.1.c Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a firewall administrator should not be responsible for scanning the firewall), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period.	As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV). A robust scanning program ensures that scans are performed and vulnerabilities addressed in a timely manner.
	11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures).	
	11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned.	The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Scanning an environment after any significant changes are made ensures that changes were completed appropriately such that the security of the environment was not compromised as a result of the change. All system components affected by the change will need to be scanned.
	11.2.3.b Review scan reports and verify that the scan process includes rescans until: • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. • For internal scans, all "high risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	

PCI DSS Requirements	Testing Procedures	Guidance
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	**11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that may include exploiting identified vulnerabilities. Conducting a vulnerability scan may be one of the first steps a penetration tester will perform in order to plan the testing strategy, although it is not the only step. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is generally a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way, a tester is able to simulate the methods performed by an attacker to identify areas of potential weakness in the environment. *Penetration testing techniques will be different for different organizations, and the type, depth, and complexity of the testing will depend on the specific environment and the organization's risk assessment.*

PCI DSS Requirements	Testing Procedures	Guidance
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: • Per the defined methodology • At least annually • After any significant changes to the environment.	Penetration testing conducted on a regular basis and after significant changes to the environment is a proactive security measure that helps minimize potential access to the CDE by malicious individuals. The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Performing penetration tests after network upgrades and modifications provides assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.
	11.3.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows. • Per the defined methodology • At least annually • After any significant changes to the environment.	
	11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	**11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	

PCI DSS Requirements	Testing Procedures	Guidance
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**11.3.4.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Penetration testing is an important tool to confirm that any segmentation in place to isolate the CDE from other networks is effective. The penetration testing should focus on the segmentation controls, both from outside the entity's network and from inside the network but outside of the CDE, to confirm that they are not able to get through the segmentation controls to access the CDE. For example, network testing and/or scanning for open ports, to verify no connectivity between in-scope and out-of-scope networks.
	11.3.4.b Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	
	11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3.4.1 ***Additional requirement for service providers only*:** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**11.3.4.1.a** Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* For service providers, validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.

PCI DSS Requirements	Testing Procedures	Guidance
	11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	**11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: • At the perimeter of the cardholder data environment • At critical points in the cardholder data environment.	Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.
	11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	
	11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *(Continued on next page)*	**11.5.a** Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files • Additional critical files determined by entity (for example, through risk assessment or other means).	Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.

PCI DSS Requirements	Testing Procedures	Guidance
Note: *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	**11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files, and to perform critical file comparisons at least weekly.	
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	**11.5.1** Interview personnel to verify that all alerts are investigated and resolved.	
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	**11.6** Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Testing Procedures	Guidance
12.1 Establish, publish, maintain, and disseminate a security policy.	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	**12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	Security threats and protection methods evolve rapidly. Without updating the security policy to reflect relevant changes, new protection measures to fight against these threats are not addressed.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	**12.2.a** Verify that an annual risk-assessment process is documented that: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business. Examples of different risk considerations include cybercrime, web attacks, and POS malware. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized. Performing risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends, and technologies.

PCI DSS Requirements	Testing Procedures	Guidance
12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:	**12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed:	Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation. If usage policies are not in place, personnel may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data.
12.3.1 Explicit approval by authorized parties	**12.3.1** Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies.	Without requiring proper approval for implementation of these technologies, individual personnel may innocently implement a solution to a perceived business need, but also open a huge hole that subjects critical systems and data to malicious individuals.
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token).	If technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), malicious individuals may easily use this unprotected technology to access critical systems and cardholder data.
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies define: • A list of all critical devices, and • A list of personnel authorized to use the devices.	Malicious individuals may breach physical security and place their own devices on the network as a "back door." Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations.

PCI DSS Requirements	Testing Procedures	Guidance
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	**12.3.4** Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	Malicious individuals may breach physical security and place their own devices on the network as a "back door." Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations. Consider establishing an official naming convention for devices, and log all devices with established inventory controls. Logical labeling may be employed with information such as codes that can correlate the device to its owner, contact information, and purpose.
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies define acceptable uses for the technology.	By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to ensure a "back door" is not opened for a malicious individual to gain access to critical systems and cardholder data.
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies define acceptable network locations for the technology.	
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies include a list of company-approved products.	
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8.a** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	Remote-access technologies are frequent "back doors" to critical resources and cardholder data. By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS vendor, other vendors, or business partners), access and risk to networks is minimized.
	12.3.8.b Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity.	
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	

PCI DSS Requirements	Testing Procedures	Guidance
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	To ensure all personnel are aware of their responsibilities to not store or copy cardholder data onto their local personal computers or other media, your policy should clearly prohibit such activities except for personnel that have been explicitly authorized to do so. Storing or copying cardholder data onto a local hard drive or other media must be in accordance with all applicable PCI DSS requirements.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4.a** Verify that information security policies clearly define information security responsibilities for all personnel. **12.4.b** Interview a sample of responsible personnel to verify they understand the security policies.	Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.
12.4.1 ***Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**12.4.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance. **12.4.1.b** Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization. Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. The level of detail provided to executive management should be appropriate for the particular organization and the intended audience.

PCI DSS Requirements	Testing Procedures	Guidance
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Examine information security policies and procedures to verify: • The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. • The following information security responsibilities are specifically and formally assigned:	Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned.	
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.	
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned.	
12.5.4 Administer user accounts, including additions, deletions, and modifications.	**12.5.4** Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned.	
12.5.5 Monitor and control all access to data.	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned.	
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	**12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures .	If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.
	12.6.b Examine security awareness program procedures and documentation and perform the following:	

PCI DSS Requirements	Testing Procedures	Guidance
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). **12.6.1.b** Verify that personnel attend security awareness training upon hire and at least annually. **12.6.1.c** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security.	If the security awareness program does not include periodic refresher sessions, key security processes and procedures may be forgotten or bypassed, resulting in exposed critical resources and cardholder data.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually, that they have read and understand the information security policy.	Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	Performing thorough background investigations prior to hiring potential personnel who are expected to be given access to cardholder data reduces the risk of unauthorized use of PANs and other cardholder data by individuals with questionable or criminal backgrounds.
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	**12.8** Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows:	If a merchant or service provider shares cardholder data with a service provider, certain requirements apply to ensure continued protection of this data will be enforced by such service providers. Some examples of the different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, entities that receive data for fraud-modeling purposes, etc.

PCI DSS Requirements	Testing Procedures	Guidance
12.8.1 Maintain a list of service providers including a description of the service provided.	**12.8.1** Verify that a list of service providers is maintained and includes a description of the service provided.	Keeping track of all service providers identifies where potential risk extends to outside of the organization.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	**12.8.2** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity. In conjunction with Requirement 12.9, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.	The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider. Specific due-diligence processes and goals will vary for each organization. Examples of considerations may include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their PCI DSS compliance and what evidence they will provide, etc.

PCI DSS Requirements	Testing Procedures	Guidance
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	Knowing your service providers' PCI DSS compliance status provides assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and those services in scope for the client's PCI DSS assessment. The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. The intent is for the assessed entity to understand which PCI DSS requirements their providers have agreed to meet.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	
12.9 ***Additional requirement for service providers only:*** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	**12.9** ***Additional testing procedure for service provider assessments only:*** Review service provider's policies and procedures and observe templates used for written agreements to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between service providers and their customers about their applicable PCI DSS responsibilities. The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The service provider's internal policies and procedures related to their customer engagement process and any templates used for written agreements should include provision of an applicable PCI DSS acknowledgement to their customers. The method by which the service provider provides written acknowledgment should be agreed between the provider and their customers.

PCI DSS Requirements	Testing Procedures	Guidance
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following:	Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	**12.10.1.a** Verify that the incident response plan includes: • Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) • Coverage and responses for all critical system components • Reference or inclusion of incident response procedures from the payment brands. **12.10.1.b** Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	The incident response plan should be thorough and contain all the key elements to allow your company to respond effectively in the event of a breach that could impact cardholder data.
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	**12.10.2** Interview personnel and review documentation from testing to verify that the plan is tested at least annually, and that testing includes all elements listed in Requirement 12.10.1.	Without proper testing, key steps may be missed, which could result in increased exposure during an incident.

PCI DSS Requirements	Testing Procedures	Guidance
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	**12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained.	
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the incident response plan.	These monitoring systems are designed to focus on potential risk to data, are critical in taking quick action to prevent a breach, and must be included in the incident-response processes.
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Incorporating "lessons learned" into the incident response plan after an incident helps keep the plan current and able to react to emerging threats and security trends.
12.11 ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**12.11.a** Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes **12.11.b** Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly.	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.

PCI DSS Requirements	Testing Procedures	Guidance
12.11.1 ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**12.11.1** Examine documentation from the quarterly reviews to verify they include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.

Appendix A: Additional PCI DSS Requirements

This appendix contains additional PCI DSS requirements for different types of entities. The sections within this Appendix include:

- Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers
- Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS
- Appendix A3: Designated Entities Supplemental Validation

Guidance and applicability information is provided within each section.

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

As referenced in Requirement 12.8 and 12.9, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.6 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

A1 Requirements	Testing Procedures	Guidance
A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A1.1 through A1.4 below:	*Appendix A* of PCI DSS is intended for shared hosting providers who wish to provide their merchant and/or service provider customers with a PCI DSS compliant hosting environment.
A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID. • All CGI scripts used by an entity must be created and run as the entity's unique user ID.	If a merchant or service provider is allowed to run their own applications on the shared server, these should run with the user ID of the merchant or service provider, rather than as a privileged user.

A1 Requirements	Testing Procedures	Guidance
A1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**A1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).	To ensure that access and privileges are restricted such that each merchant or service provider has access only to their own environment, consider the following: 1. Privileges of the merchant's or service provider's web server user ID; 2. Permissions granted to read, write, and execute files; 3. Permissions granted to write to system binaries; 4. Permissions granted to merchant's and service provider's log files; and 5. Controls to ensure one merchant or service provider cannot monopolize system resources.
	A1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) **Important:** An entity's files may not be shared by group.	
	A1.2.c Verify that an entity's users do not have write access to shared system binaries.	
	A1.2.d Verify that viewing of log entries is restricted to the owning entity.	
	A1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU	
A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review by the owning entity. • Log locations are clearly communicated to the owning entity.	Logs should be available in a shared hosting environment so the merchants and service providers have access to, and can review, logs specific to their cardholder data environment.
A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.	Shared hosting providers must have processes to provide quick and easy response in the event that a forensic investigation is needed for a compromise, down to the appropriate level of detail so that an individual merchant's or service provider's details are available.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

The PCI DSS requirements directly affected are:

Requirement 2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
Requirement 2.3	Encrypt all non-console administrative access using strong cryptography.
Requirement 4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/early TLS, the following provisions are included:

- New implementations must not use SSL or early TLS as a security control.
- All service providers must provide a secure service offering by June 30, **2016.**
- After June 30, **2018**, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet below).
- Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after June 30, 2018.

This Appendix applies to entities using SSL/early TLS as a security control to protect the CDE and/or CHD (for example, SSL/early TLS used to meet PCI DSS Requirement 2.2.3, 2.3, or 4.1), Refer to the current *PCI SSC Information Supplement Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.

A2 Requirements	Testing Procedures	Guidance
A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: • Confirm the devices are not susceptible to any known exploits for those protocols. ***Or:*** • Have a formal Risk Mitigation and Migration Plan in place.	**A2.1** *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS:* • Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. *Or:* • Complete A2.2 below.	POIs can continue using SSL/early TLS when it can be shown that the POI is not susceptible to the currently known exploits. However, SSL is an outdated technology and may be subject to additional security vulnerabilities in the future; it is therefore strongly recommended that POI environments upgrade to a secure protocol as soon as possible. If SSL/early TLS is not needed in the environment, use of and fallback to these versions should be disabled. If the POS POI environment is susceptible to known exploits, then planning for migration to a secure alternative should commence immediately. ***Note:*** *The allowance for POS POIs that are not currently susceptible to exploits is based on current, known risks. If new exploits are introduced for which POI environments are susceptible, the POI environments will need to be updated.*
A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	**A2.2** Review the documented Risk Mitigation and Migration Plan to verify it includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; • Risk-assessment results and risk-reduction controls in place; • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; • Overview of migration project plan including target migration completion date no later than June 30, 2018.	The Risk Mitigation and Migration Plan is a document prepared by the entity that details their plans for migrating to a secure protocol, and also describes controls the entity has in place to reduce the risk associated with SSL/early TLS until the migration is complete. Refer to the current PCI SSC Information Supplement Migrating from SSL and Early TLS for further guidance on Risk Mitigation and Migration Plans.

A2 Requirements	Testing Procedures	Guidance
A2.3 ***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016. ***Note:*** *Prior to June 30, 2016, the service provider must either have a secure protocol option included in their service offering,* ***or*** *have a documented Risk Mitigation and Migration Plan (per A2.2) that includes a target date for provision of a secure protocol option no later than June 30, 2016. After this date, all service providers must offer a secure protocol option for their service.*	**A2.3** Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for their service.	Refer to "Service Providers" in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for further guidance.

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Examples of entities that this Appendix ***could*** apply to include:

- Those storing, processing, and/or transmitting large volumes of cardholder data,
- Those providing aggregation points for cardholder data, or
- Those that have suffered significant or repeated breaches of cardholder data.

These supplemental validation steps are intended to provide greater assurance that PCI DSS controls are maintained effectively and on a continuous basis through validation of business-as-usual (BAU) processes, and increased validation and scoping consideration.

The additional validation steps in this document are organized into the following control areas:

A3.1 *Implement a PCI DSS compliance program.*

A3.2 *Document and validate PCI DSS scope.*

A3.3 *Validate PCI DSS is incorporated into business-as-usual (BAU) activities.*

A3.4 *Control and manage logical access to the cardholder data environment.*

A3.5 *Identify and respond to suspicious events.*

Note: *Some requirements have defined timeframes (for example, at least quarterly or every six months) within which certain activities are to be performed. For initial assessment to this document, it is not required that an activity has been performed for every such timeframe during the previous year, if the assessor verifies:*

1) The activity was performed in accordance with the applicable requirement within the most recent timeframe (that is, the most recent quarter or six-month period), and

2) The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe.

For subsequent years after the initial assessment, an activity must have been performed for each timeframe for which it is required (for example, a quarterly activity must have been performed for each of the previous year's four quarters).

Note: *An entity is required to undergo an assessment according to this Appendix* ***ONLY if instructed to do so by an acquirer or a payment brand.***

A3 Requirements	Testing Procedures	Guidance
A3.1 Implement a PCI DSS compliance program		
A3.1.1 Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program • Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least annually ***PCI DSS Reference:*** *Requirement 12*	**A3.1.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance. **A3.1.1.b** Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized. **A3.1.1.c** Examine executive management and board of directors meeting minutes and/or presentations to ensure PCI DSS compliance initiatives and remediation activities are communicated at least annually.	Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.
A3.1.2 A formal PCI DSS compliance program must be in place to include: • Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities • Annual PCI DSS assessment processes • Processes for the continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions ***PCI DSS Reference:*** *Requirements 1-12*	**A3.1.2.a** Examine information security policies and procedures to verify that processes are specifically defined for the following: • Maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business-impact analysis to determine potential PCI DSS impacts for strategic business decisions	A formal compliance program allows an organization to monitor the health of its security controls, be proactive in the event that a control fails, and effectively communicate activities and compliance status throughout the organization. The PCI DSS compliance program can be a dedicated program or part of an over-arching compliance and/or governance program, and should include a well-defined methodology that demonstrates consistent and effective evaluation. Example methodologies include: Deming Circle of Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC, and Six Sigma. *(Continued on next page)*

A3 Requirements	Testing Procedures	Guidance
	A3.1.2.b Interview personnel and observe compliance activities to verify that the defined processes are implemented for the following: • Maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business-impact analysis to determine potential PCI DSS impacts for strategic business decisions	Maintaining and monitoring an organization's overall PCI DSS compliance includes identifying activities to be performed daily, weekly, monthly, quarterly, or annually, and ensuring these activities are being performed accordingly (for example, using a security self-assessment or PDCA methodology). Examples of strategic business decisions that should be analyzed for potential PCI DSS impacts may include mergers and acquisitions, new technology purchases, or new payment-acceptance channels.
A3.1.3 PCI DSS compliance roles and responsibilities must be specifically defined and formally assigned to one or more personnel, including at least the following: • Managing PCI DSS business-as-usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions ***PCI DSS Reference:*** *Requirement 12*	**A3.1.3.a** Examine information security policies and procedures and interview personnel to verify that roles and responsibilities are clearly defined and that duties are assigned to include at least the following: • Managing PCI DSS business-as-usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions **A3.1.3.b** Interview responsible personnel and verify they are familiar with and performing their designated PCI DSS compliance responsibilities.	The formal definition of specific PCI DSS compliance roles and responsibilities helps to ensure accountability and monitoring of ongoing PCI DSS compliance efforts. These roles may be assigned to a single owner or multiple owners for different aspects. Ownership should be assigned to individuals with the authority to make risk-based decisions and upon whom accountability rests for the specific function. Duties should be formally defined and owners should be able to demonstrate an understanding of their responsibilities and accountability.

A3 Requirements	Testing Procedures	Guidance
A3.1.4 Provide up-to-date PCI DSS and/or information security training at least annually to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). ***PCI DSS Reference:*** *Requirement 12*	**A3.1.4.a** Examine information security policies and procedures to verify that PCI DSS and/or information security training is required at least annually for each role with PCI DSS compliance responsibilities.	Personnel responsible for PCI DSS compliance have specific training needs exceeding that which is typically provided by general security awareness training. Individuals with PCI DSS compliance responsibilities should receive specialized training that, in addition to general awareness of information security, focuses on specific security topics, skills, processes, or methodologies that must be followed for those individuals to perform their compliance responsibilities effectively. Training may be offered by third parties—for example, SANS or PCI SSC (PCI Awareness, PCIP, and ISA), payment brands, and acquirers—or training may be internal. Training content should be applicable for the particular job function and be current to include the latest security threats and/or version of PCI DSS. For additional guidance on developing appropriate security training content for specialized roles, refer to the PCI SSC's Information Supplement on *Best Practices for Implementing a Security Awareness Program.*
	A3.1.4.b Interview personnel and examine certificates of attendance or other records to verify that personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least annually.	

A3 Requirements	Testing Procedures	Guidance
A3.2 Document and validate PCI DSS scope		
A3.2.1 Document and confirm the accuracy of PCI DSS scope at least quarterly and upon significant changes to the in-scope environment. At a minimum, the quarterly scoping validation should include: • Identifying all in-scope networks and system components • Identifying all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented • Identifying all connected entities—e.g., third-party entities with access to the cardholder data environment (CDE) ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*	**A3.2.1.a** Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least quarterly • After significant changes to the in-scope environment **A3.2.1.b** Examine documented results of quarterly scope reviews to verify the following is performed: • Identification of all in-scope networks and system components • Identification of all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented • Identification of all connected entities—e.g., third-party entities with access to the CDE	Validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.
A3.2.2 Determine PCI DSS scope impact for all changes to systems or networks, including additions of new systems and new network connections. Processes must include: • Performing a formal PCI DSS impact assessment • Identifying applicable PCI DSS requirements to the system or network • Updating PCI DSS scope as appropriate • Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3) ***PCI DSS Reference:*** *Scope of PCI DSS Requirements; Requirements 1-12*	**A3.2.2** Examine change documentation and interview personnel to verify that for each change to systems or networks: • A formal PCI DSS impact assessment was performed. • PCI DSS requirements applicable to the system or network changes were identified. • PCI DSS scope was updated as appropriate for the change. • Sign-off by responsible personnel (as defined in A3.1.3) was obtained and documented.	Changes to systems or networks can have significant impact to PCI DSS scope. For example, firewall rule changes can bring whole network segments into scope, or new systems may be added to the CDE that have to be appropriately protected. Processes to determine the potential impact that changes to systems and networks may have on an entity's PCI DSS scope may be performed as part of a dedicated PCI DSS compliance program, or may fall under an entity's over-arching compliance and/or governance program.

A3 Requirements	Testing Procedures	Guidance
A3.2.2.1 Upon completion of a change, all relevant PCI DSS requirements must be verified on all new or changed systems and networks, and documentation must be updated as applicable. Examples of PCI DSS requirements that should be verified include, but are not limited to: ▪ Network diagram is updated to reflect changes. ▪ Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. ▪ Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging. ▪ Verify that sensitive authentication data (SAD) is not stored and that all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures ▪ New systems are included in the quarterly vulnerability scanning process. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements; Requirement 1-12*	**A3.2.2.1** For a sample of systems and network changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	It is important to have processes to analyze all changes made to ensure that all appropriate PCI DSS controls are applied to any systems or networks added to the in-scope environment due to a change. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process.

A3 Requirements	Testing Procedures	Guidance
A3.2.3 Changes to organizational structure—for example, a company merger or acquisition, change or reassignment of personnel with responsibility for security controls—result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. ***PCI DSS Reference:*** *Requirement 12*	**A3.2.3** Examine policies and procedures to verify that a change to organizational structure results in formal review of the impact to PCI DSS scope and applicability of controls.	An organization's structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported PCI DSS controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit PCI DSS scope and controls when there are changes to ensure controls are in place and active.
A3.2.4 If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***PCI DSS Reference:*** *Requirement 11*	**A3.2.4** Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	If segmentation is used to isolate in-scope networks from out-of-scope networks, those segmentation controls must be verified using penetration testing to confirm they continue to operate as intended and effectively. Penetration-testing techniques should follow the existing penetration methodology as specified in PCI DSS Requirement 11. For additional information on effective penetration testing, refer to the PCI SSC's Information Supplement on *Penetration Testing Guidance*.

A3 Requirements	Testing Procedures	Guidance
A3.2.5 Implement a data-discovery methodology to confirm PCI DSS scope and to locate all sources and locations of clear-text PAN at least quarterly and upon significant changes to the cardholder environment or processes. Data-discovery methodology must take into consideration the potential for clear-text PAN to reside on systems and networks outside of the currently defined CDE. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*	**A3.2.5.a** Examine documented data-discovery methodology to verify the following: • Data-discovery methodology includes processes for identifying all sources and locations of clear-text PAN. • Methodology takes into consideration the potential for clear-text PAN to reside on systems and networks outside of the currently defined CDE. **A3.2.5.b** Examine results from recent data discovery efforts, and interview responsible personnel to verify that data discovery is performed at least quarterly and upon significant changes to the cardholder environment or processes.	PCI DSS requires that, as part of the scoping exercise, assessed entities must identify and document the existence of all clear-text PAN in their environments. Implementing a data-discovery methodology that identifies all sources and locations of clear-text PAN, and takes into consideration the potential for clear-text PAN to reside on systems and networks outside of the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file— helps to ensure that previously unknown locations of clear-text PAN are detected and properly secured. A data-discovery process can be performed via a variety of methods, including but not limited to: (1) commercially available data-discovery software, (2) an in-house developed data-discovery program, or (3) a manual search. Regardless of the method used, the goal of the effort is to find all sources and locations of clear-text PAN (not just in the defined CDE).
A3.2.5.1 Ensure effectiveness of methods used for data discovery——e.g., methods must be able to discover clear-text PAN on all types of system components (for example, on each operating system or platform) and file formats in use. The effectiveness of data-discovery methods must be confirmed at least annually. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*	**A3.2.5.1.a** Interview personnel and review documentation to verify: ▪ The entity has a process in place to test the effectiveness of methods used for data discovery. ▪ The process includes verifying the methods are able to discover clear-text PAN on all types of system components and file formats in use. **A3.2.5.1.b** Examine the results of recent effectiveness tests to verify the effectiveness of methods used for data discovery is confirmed at least annually.	A process to test the effectiveness of the methods used for data discovery ensures the completeness and accuracy of cardholder data detection. For completeness, at least a sampling of system components in both the in-scope and out-of-scope networks should be included in the data-discovery process. Accuracy can be tested by placing test PANs on a sample of system components and file formats in use and confirming that the data-discovery method detected the test PANs.

A3 Requirements	Testing Procedures	Guidance
A3.2.5.2 Implement response procedures to be initiated upon the detection of clear-text PAN outside of the CDE to include: ▪ Procedures for determining what to do if clear-text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE, as applicable ▪ Procedures for determining how the data ended up outside of the CDE ▪ Procedures for remediating data leaks or process gaps that resulted in the data being outside of the CDE ▪ Procedures for identifying the source of the data ▪ Procedures for identifying whether any track data is stored with the PANs	**A3.2.5.2.a** Examine documented response procedures to verify that procedures for responding to the detection of clear-text PAN outside of the CDE are defined and include: ▪ Procedures for determining what to do if clear-text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE, as applicable ▪ Procedures for determining how the data ended up outside the CDE ▪ Procedures for remediating data leaks or process gaps that resulted in the data being outside of the CDE ▪ Procedures for identifying the source of the data ▪ Procedures for identifying whether any track data is stored with the PANs	Having documented response procedures that are followed in the event clear-text PAN is found outside of the CDE helps to identify the necessary remediation actions and prevent future leaks. For example, if PAN was found outside of the CDE, analysis should be performed to (1) determine whether it was saved independently of other data (or was it part of a full track?), (2) to identify the source of the data, and (3) identify the control gaps that resulted in the data being outside the CDE.
	A3.2.5.2.b Interview personnel and examine records of response actions to verify that remediation activities are performed when clear-text PAN is detected outside of the CDE.	
A3.2.6 Implement mechanisms for detecting and preventing clear-text PAN from leaving the CDE via an unauthorized channel, method, or process, including generation of audit logs and alerts. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*	**A3.2.6.a** Examine documentation and observe implemented mechanisms to verify that the mechanisms are: • Implemented and actively running • Configured to detect and prevent clear-text PAN leaving the CDE via an unauthorized channel, method, or process • Generating logs and alerts upon detection of clear-text PAN leaving the CDE via an unauthorized channel, method, or process	Mechanisms to detect and prevent unauthorized loss of clear-text PAN may include appropriate tools—such as data loss prevention (DLP) solutions—and/or manual processes and procedures. Coverage of the mechanisms should include, but not be limited to, e-mails, downloads to removable media, and output to printers. Use of these mechanisms allows an organization to detect and prevent situations that may lead to data loss.
	A3.2.6.b Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	

A3 Requirements	Testing Procedures	Guidance
A3.2.6.1 Implement response procedures to be initiated upon the detection of attempts to remove clear-text PAN from the CDE via an unauthorized channel, method, or process. Response procedures must include: ▪ Procedures for the timely investigation of alerts by responsible personnel ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	**A3.2.6.1.a** Examine documented response procedures to verify that procedures for responding to the attempted removal of clear-text PAN from the CDE via an unauthorized channel, method, or process include: ▪ Procedures for the timely investigation of alerts by responsible personnel ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	Attempts to remove clear-text PAN via an unauthorized channel, method, or process may indicate malicious intent to steal data, or may be the actions of an authorized employee who is unaware of or simply not following the proper methods. Timely investigation of these occurrences can identify where remediation needs to be applied and provides valuable information to help understand where the threats are coming from.
	A3.2.6.1.b Interview personnel and examine records of actions taken when clear-text PAN is detected leaving the CDE via an unauthorized channel, method, or process, and verify that remediation activities were performed.	
A3.3 Validate PCI DSS is incorporated into business-as-usual (BAU) activities		
A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) ***PCI DSS Reference:*** *Requirements 1-12*	**A3.3.1.a** Examine documented policies and procedures to verify that processes are defined to immediately detect and alert on critical security control failures.	Without formal processes for the prompt (as soon as possible) detection and alerting of critical security control failures, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.
	A3.3.1.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	

A3 Requirements	Testing Procedures	Guidance
A3.3.1.1 Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: ▪ Restoring security functions ▪ Identifying and documenting the duration (date and time start to end) of the security failure ▪ Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ▪ Identifying and addressing any security issues that arose during the failure ▪ Performing a risk assessment to determine whether further actions are required as a result of the security failure ▪ Implementing controls to prevent cause of failure from reoccurring ▪ Resuming monitoring of security controls ***PCI DSS Reference:*** *Requirements 1-12*	**A3.3.1.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: ▪ Restoring security functions ▪ Identifying and documenting the duration (date and time start to end) of the security failure ▪ Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ▪ Identifying and addressing any security issues that arose during the failure ▪ Performing a risk assessment to determine whether further actions are required as a result of the security failure ▪ Implementing controls to prevent cause of failure from reoccurring ▪ Resuming monitoring of security controls **A3.3.1.1.b** Examine records to verify that security control failures are documented to include: ▪ Identification of cause(s) of the failure, including root cause ▪ Duration (date and time start and end) of the security failure ▪ Details of the remediation required to address the root cause	Documented evidence (e.g., records within a problem-management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.

A3 Requirements	Testing Procedures	Guidance
A3.3.2 Review hardware and software technologies at least annually to confirm whether they continue to meet the organization's PCI DSS requirements. (For example, a review of technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.) The process includes a plan for remediating technologies that no longer meet the organization's PCI DSS requirements, up to and including replacement of the technology, as appropriate. ***PCI DSS Reference:*** *Requirements 2, 6*	**A3.3.2.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to review hardware and software technologies to confirm whether they continue to meet the organization's PCI DSS requirements. **A3.3.2.b** Review the results of the recent reviews to verify reviews are performed at least annually. **A3.3.2.c** For any technologies that have been determined to no longer meet the organization's PCI DSS requirements, verify a plan is in place to remediate the technology.	Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies. Organizations also need to be aware of changes made by technology vendors to their products or support processes, to understand how such changes may impact the organization's use of the technology. Regular reviews of technologies that impact or influence PCI DSS controls can assist with purchasing, usage, and deployment strategies, and ensure controls that rely on those technologies remain effective.

A3 Requirements	Testing Procedures	Guidance
A3.3.3 Perform reviews at least quarterly to verify BAU activities are being followed. Reviews must be performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include the following: • Confirmation that all BAU activities (e.g., A3.2.2, A3.2.6, and A3.3.1) are being performed • Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Documenting how the reviews were completed, including how all BAU activities were verified as being in place. • Collection of documented evidence as required for the annual PCI DSS assessment • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program (as identified in A3.1.3) • Retention of records and documentation for at least 12 months, covering all BAU activities ***PCI DSS Reference:*** *Requirements 1-12*	**A3.3.3.a** Examine policies and procedures to verify that processes are defined for reviewing and verifying BAU activities. Verify the procedures include: • Confirming that all BAU activities (e.g., A3.2.2, A3.2.6, and A3.3.1) are being performed • Confirming that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Documenting how the reviews were completed, including how all BAU activities were verified as being in place • Collecting documented evidence as required for the annual PCI DSS assessment • Reviewing and sign-off of results by executive management assigned responsibility for PCI DSS governance • Retaining records and documentation for at least 12 months, covering all BAU activities **A3.3.3.b** Interview responsible personnel and examine records of reviews to verify that: • Reviews are performed by personnel assigned to the PCI DSS compliance program. • Reviews are performed at least quarterly.	Implementing PCI DSS controls into business-as-usual activities is an effective method to ensure security is included as part of normal business operations on an ongoing basis. Therefore, it is important that independent checks are performed to ensure BAU controls are active and working as intended. The intent of these independent checks is to review the evidence that confirms business-as-usual activities are being performed. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.

A3 Requirements	Testing Procedures	Guidance
A3.4 Control and manage logical access to the cardholder data environment		
A3.4.1 Review user accounts and access privileges to in-scope system components at least every six months to ensure user accounts and access remain appropriate based on job function, and authorized. ***PCI DSS Reference:*** *Requirement 7*	**A3.4.1** Interview responsible personnel and examine supporting documentation to verify that: • User accounts and access privileges are reviewed at least every six months. • Reviews confirm that access is appropriate based on job function, and that all access is authorized.	Access requirements evolve over time as individuals change roles or leave the company, and as job functions change. Management needs to regularly review, revalidate, and update user access, as necessary, to reflect changes in personnel, including third parties, and users' job functions.
A3.5 Identify and respond to suspicious events		
A3.5.1 Implement a methodology for the timely identification of attack patterns and undesirable behavior across systems—for example, using coordinated manual reviews and/or centrally managed or automated log-correlation tools—to include at least the following: • Identification of anomalies or suspicious activity as it occurs • Issuance of timely alerts upon detection of suspicious activity or anomaly to responsible personnel • Response to alerts in accordance with documented response procedures ***PCI DSS Reference:*** *Requirements 10, 12*	**A3.5.1.a** Review documentation and interview personnel to verify a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a timely manner, and includes the following: • Identification of anomalies or suspicious activity as it occurs • Issuance of timely alerts to responsible personnel • Response to alerts in accordance with documented response procedures **A3.5.1.b** Examine incident response procedures and interview responsible personnel to verify that: • On-call personnel receive timely alerts. • Alerts are responded to per documented response procedures.	The ability to identify attack patterns and undesirable behavior across systems is critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something goes wrong. Determining the cause of a compromise is very difficult, if not impossible, without a process to corroborate information from critical system components, and systems that perform security functions—such as firewalls, IDS/IPS, and file-integrity monitoring (FIM) systems. Thus, logs for all critical systems components and systems that perform security functions should be collected, correlated, and maintained. This could include the use of software products and service methodologies to provide real-time analysis, alerting, and reporting—such as security information and event management (SIEM), file-integrity monitoring (FIM), or change detection.

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

Note: *The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, multi-factor authentication is a PCI DSS requirement for remote access. Multi-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Multi-factor authentication may be an acceptable compensating control if: (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) multi-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement noted as being "in place" via compensating controls.

Requirement Number: *8.1.1 – Are all users identified with a unique user ID before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers using their regular user accounts, and then use the "sudo" command to run any administrative commands. This allows use of the "root" account privileges to run pre-defined commands that are recorded by sudo in the security log. In this way, each user's actions can be traced to an individual user account, without the "root" password being shared with the users.*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the sudo command is configured properly using a "sudoers" file, that only pre-defined commands can be run by specified users, and that all activities performed by those individuals using sudo are logged to identify the individual performing actions using "root" privileges.*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure sudo configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually identified, tracked and logged.*

Appendix D: Segmentation and Sampling of Business Facilities/System Components

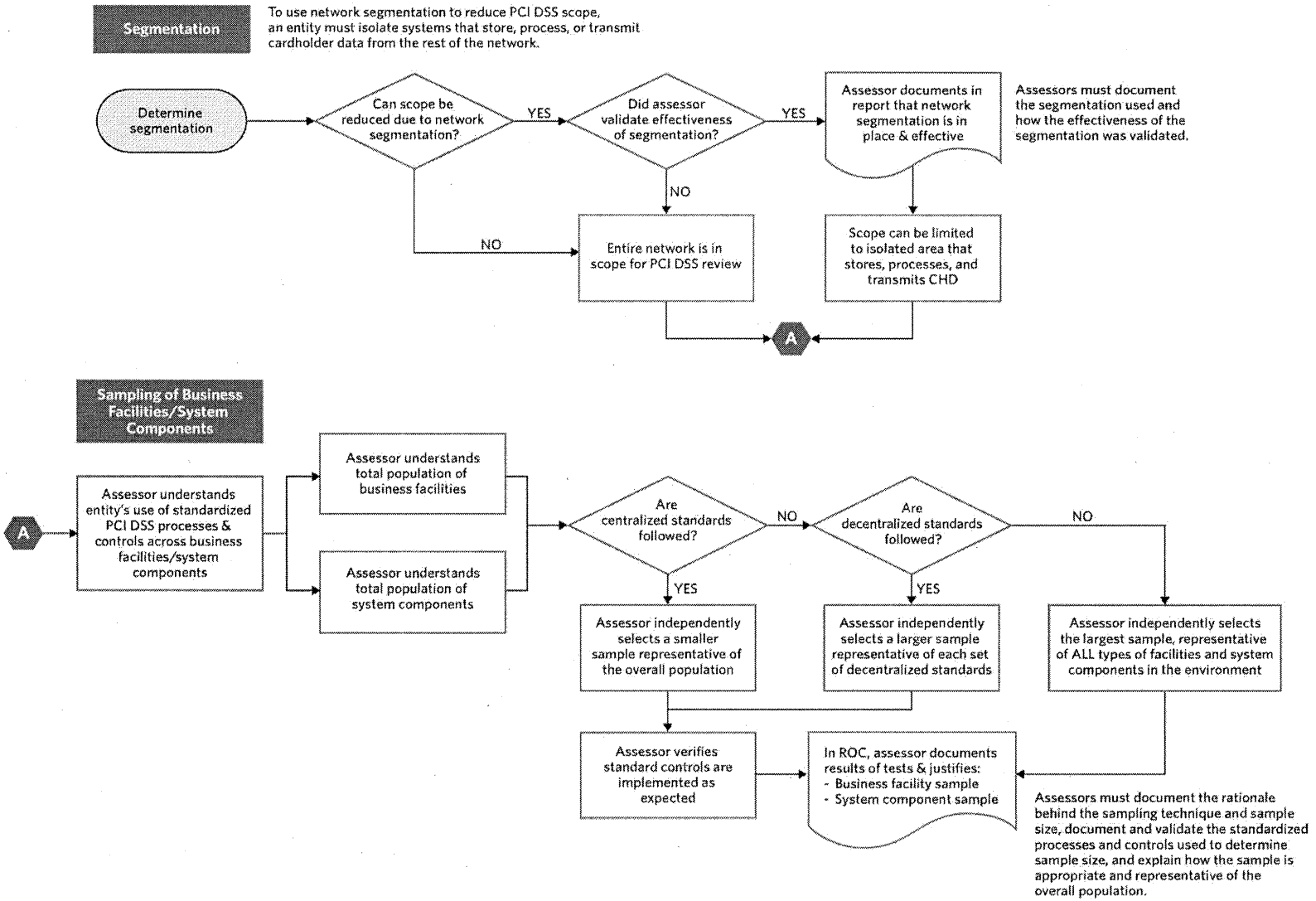
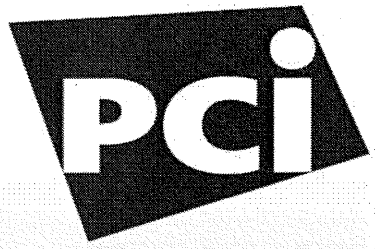


Exhibit B



Security Standards Council®

Standard:	PCI Data Security Standard (PCI DSS)
Version:	2.0
Date:	November 2012
Author:	Risk Assessment Special Interest Group (SIG) PCI Security Standards Council

Information Supplement:
PCI DSS Risk Assessment Guidelines

Table of Contents

1 Introduction

1.1 Objective

The objective of this document is to provide supplemental guidance and recommendations for performing a risk assessment in accordance with PCI DSS Requirement 12.1.2.

A risk assessment, as required in the PCI DSS, is a formal process used by organizations to identify threats and vulnerabilities that could negatively impact the security of cardholder data.

This document does not replace, supersede, or extend any PCI DSS requirements; rather it provides guidance for organizations to identify, analyze, and document the risks that may affect their cardholder data environment (CDE).

1.2 Intended Audience

This guidance is intended for any organization that stores, processes, or transmits cardholder data (CHD). Examples include merchants, service providers, acquirers (merchant banks), and issuers. The intended audience includes large, medium, or small organizations.

2 Risk Assessments and the PCI DSS

2.1 Risk Definition

Risk has many interpretations, and is often used to describe dangers or threats to a particular person, environment, or business. The following is just one definition:

> *Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization*[1]

Understanding risk includes understanding of the different elements and how they fit together. For example, considerations from a business perspective may include:

- What are the different types of threats to the organization?
- What are the organization's assets that need protecting from the threats?
- How vulnerable is the organization to different threats?
- What is the likelihood that a threat will be realized?
- What would be the impact if a threat was realized?
- How can the organization reduce the likelihood of a threat being realized, or reduce the impact if it does occur?

2.2 PCI DSS Requirement 12.1.2

PCI DSS Requirements	Testing Procedures
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.

Figure 1.0 – PCI DSS Requirement 12.1.2

PCI DSS Requirement 12.1.2 requires organizations to establish an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.

[1] NIST SP800-30

A risk assessment enables an organization to identify threats and the associated vulnerabilities which have the potential to negatively impact their business. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threats being realized.

Performing risk assessments at least annually allows organizations to keep up to date with business changes and provides a mechanism to evaluate those changes against the evolving threat landscape, emerging trends, and new technologies. Examples of changes include the introduction of a new product line or service offering that is different from existing products or services, introduction of a new software application in the CDE, change of a network topology impacting the CDE, etc.

2.3 Risk Management Strategy

Because the PCI DSS risk assessment takes into account only a subset of the organization's overall risks, organizations should maximize the benefits of a risk assessment by incorporating the PCI DSS risk assessment into their overall organization-wide risk management program.

The risk assessment process should include people, processes, and technologies that are involved in the storage, processing, or transmission of CHD including those that may not be directly involved in processing CHD but still have the potential to impact the security of the CDE—for example, perimeter building security at the facility where the CDE is located. Consideration should also be given to business processes outsourced and/or managed by third-party service providers or merchants.

To ensure adequate coverage, an organization-wide risk management program would need to ensure that risks across all areas of the organization are considered, that there is a coordinated strategy for addressing identified risks, and that the risk mitigation efforts are aligned across all business processes.

2.4 PCI DSS Requirements

PCI DSS provides a baseline of technical and operational controls that work together to provide a defense-in-depth approach to the protection of cardholder data. PCI DSS comprises of a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks. Risk assessments provide valuable information to help organizations determine whether additional controls are necessary to protect their sensitive data and other assets.

Note: *The result of a risk assessment must not be used by organizations as a means of avoiding or bypassing applicable PCI DSS requirements (or related compensating controls).*

In order to achieve compliance with the PCI DSS, an organization must meet all applicable PCI DSS requirements.

2.5 Benefits of Conducting a PCI DSS Risk Assessment

Conducting a PCI DSS risk assessment helps an organization to identify and understand the potential risks to their CDE. By understanding these risks, an organization can prioritize risk-mitigation efforts to address the most critical risks first. Organizations can also implement threat-reducing controls more effectively, for example, by choosing a technology or solution that best addresses identified risks.

Risk assessments can help identify the presence of cardholder data that is not fundamental to business operations and that can be removed from an organization's environment, reducing both the risk to the environment and potentially the scope of their CDE.

In addition, risk assessments can identify areas containing data that need protection versus areas that are more open and do not need access to sensitive data. Information obtained through a risk assessment can be used to determine how to segment environments to isolate sensitive networks (CDE) from non-sensitive networks and, thus, save unnecessary investment in security controls where they are not needed. Isolation of these less sensitive networks helps to define the CDE and contributes to an effective scoping methodology.

Performing risk assessments at regular intervals provides an organization with the insight into changing environments and assists it to identify where mitigation controls need to be adjusted or added before new threats can be realized. This practice may provide the opportunity to identify whether future investment in resources may be warranted.

Ideally, a continuous risk assessment process would be implemented to enable ongoing discovery of emerging threats and vulnerabilities that could negatively impact the cardholder data environment (CDE), allowing an organization to mitigate such threats and vulnerabilities in a proactive and timely manner.

2.6 Risk Assessment and the Prioritized Approach

For organizations working towards their initial PCI DSS compliance validation, the PCI DSS Prioritized Approach provides a roadmap of compliance activities based on risks associated with storing, processing, and/or transmitting cardholder data. It helps organizations prioritize efforts to achieve compliance, establish milestones, and lower the risk of CHD breaches early in the compliance process. As part of Milestone 1, the organization needs to implement a formalized risk assessment process to identify threats and vulnerabilities that could negatively impact the security of their cardholder data.

Organizations working towards compliance may find that the initial risk assessment requires additional time and resources, as it may be the first time the environment has been reviewed and evaluated from a risk-based perspective. Furthermore, if a risk assessment process is not already established, organizations will need to define and document their risk assessment methodology, identify individuals who will need to be involved, assign roles and responsibilities, and allocate resources.

For organizations maintaining compliance, it is important to understand that the annual PCI DSS validation is only a snapshot of compliance at a given time, as noted on the Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). To ensure compliance is maintained, a risk assessment may be undertaken after any significant changes to the CDE including, but not limited to, any changes in technologies, business processes, personnel, and/or third-party relationships that could impact the security of CHD.

3 Industry-Standard Risk Methodologies

3.1 Common Elements

A number of industry-accepted methodologies are available to assist organizations to develop their risk assessment process. Examples of these methodologies include:

- **International Organization of Standardization (ISO)** has published a wide array of standards appropriate to information security and risk management. The most relevant document for understanding and providing guidance on risk assessment is *ISO 27005,* which is a risk management guideline. This document covers the standard information security risk management processes that are undertaken encompassing risk assessment.

  The guidance provided in ISO 27005 is useful for conducting formal information security risk assessments.

- **The National Institute of Standards and Technology (NIST)** develops standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services. Overall guidance on risk management for information systems is covered in Managing Information Security Risk: Organization, Mission and Information System View (NIST SP 800-39), while the NIST SP 800-30 (Revision 1) focuses exclusively on risk assessments. Much of the work conducted by NIST aligns with the work undertaken in Europe by organizations such as ITSEC and subsequently Common Criteria.
- **Operationally Critical Threat, Asset, and Vulnerability Evaluation** [SM] **(OCTAVE®)** is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning. The OCTAVE method lists eight processes for a formal risk assessment. It leverages people's knowledge of their organization's security-related practices and processes to capture the current state of security within the organization. Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization. OCTAVE resources provide a useful source for guidance.

Other risk frameworks, such as Factor Analysis of Information Risk (FAIR) and the Australian/New Zealand Standard AS/NZS 4360, can either be used on their own or to supplement assessments performed using traditional methodologies, such as OCTAVE and those published by ISO and NIST.

All of the methodologies mentioned above have common goals, albeit from slightly differing perspectives. They are all suitable for PCI DSS risk assessments. Each risk methodology incorporates the following core activities:

- Identifying critical assets and the threats to those assets
- Identifying the vulnerabilities, both organizational and technological, that could potentially expose assets to those threats, resulting in risk to the organization

- Developing a risk strategy and risk mitigation plans to address identified risks in support the organization's mission and priorities

Many risk assessment methodologies follow similar steps; however the approaches they undertake for identification of risks and their measurement techniques differ. Most methodologies have options for both *quantitative* and *qualitative* approaches (discussed later in this document).

Organizations may choose to incorporate a formalized risk assessment methodology (such as the ones covered above) and adapt it to the culture and requirements of the organization.

4 Key Elements of a Risk Assessment

4.1 Develop a Risk Assessment Team

The risk assessment team should include representation from all the departments within the organization, including those that are involved in the processing, storage, and transmission of CHD. Such departments may include business processes, technology and support departments, such as Human Resources, Marketing, Operations, Information Technology, Information Security and Security Administration.

Where possible it is recommended the risk assessment is led by an individual and/or individuals who have sufficient knowledge of the PCI DSS requirements and the risk assessment methodology being utilized by the organization. The risk assessment process leader is typically responsible for driving the risk assessment process within the organization and reporting the results to management. Organizations without the internal resources or skills to conduct risk assessments may consider engaging external resources to assist with their risk assessment process.

4.2 Building a Risk Assessment Methodology

When developing their own risk assessment methodology, organizations may consider adapting an industry-standard methodology that is most appropriate for their particular culture and business climate, to ensure their particular risk objectives are met. Figure 2.0 illustrates typical risk assessment components.

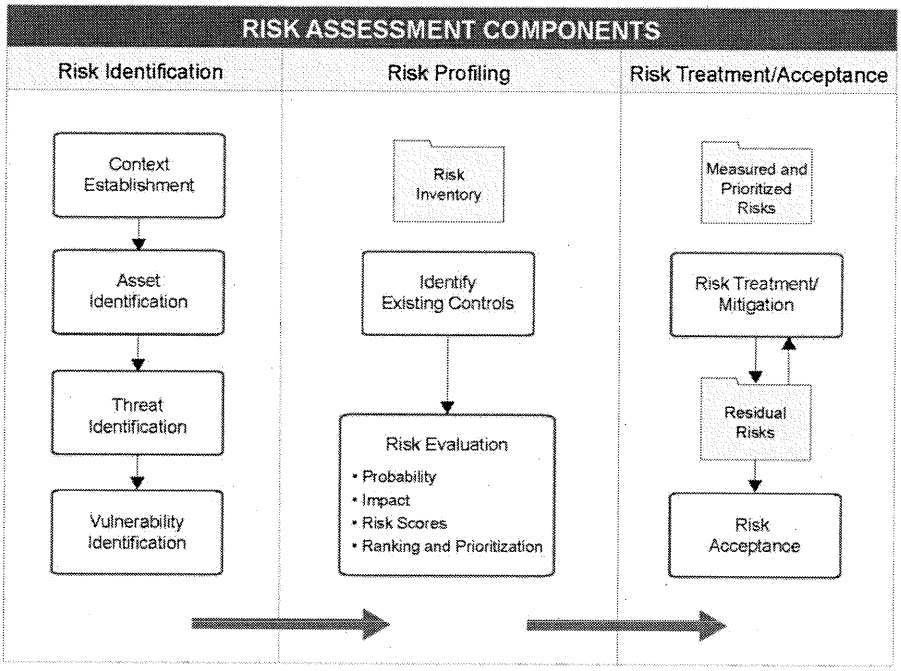


Figure 2.0 – Risk assessment components

4.2.1 Risk Identification

Before an organization can assess its risks, it should understand its business processes, assets, threats, and vulnerabilities.

- **Context Establishment** – The risk assessment team needs to understand the internal and external parameters when defining the scope of the risk assessment and/or have access to the persons in the organization who can provide this information—for example, the organization's hierarchy, business processes, CHD flows, and any associated system components.
- **Asset identification** – Generally, assets could be anything of value to an organization. In the context of PCI DSS, assets include the people, processes, and technologies that are involved in the processing, storage, transmission, and protection of CHD. Each asset may be identified to an asset owner who will then be responsible for adequately protecting the asset. The asset may also be assigned an asset value based on its importance and criticality.

  When identifying assets for a PCI DSS risk assessment, all payment channels should be considered—for example, face-to-face, e-commerce, mail order/telephone order (MOTO), etc.—as the assets identified for each payment-acceptance channel may carry different levels of risk.

  To help categorize the assets as relevant to the organization's business, it may be helpful to structure the assets into groups and sub-groups such as those shown in Figure 3.0:

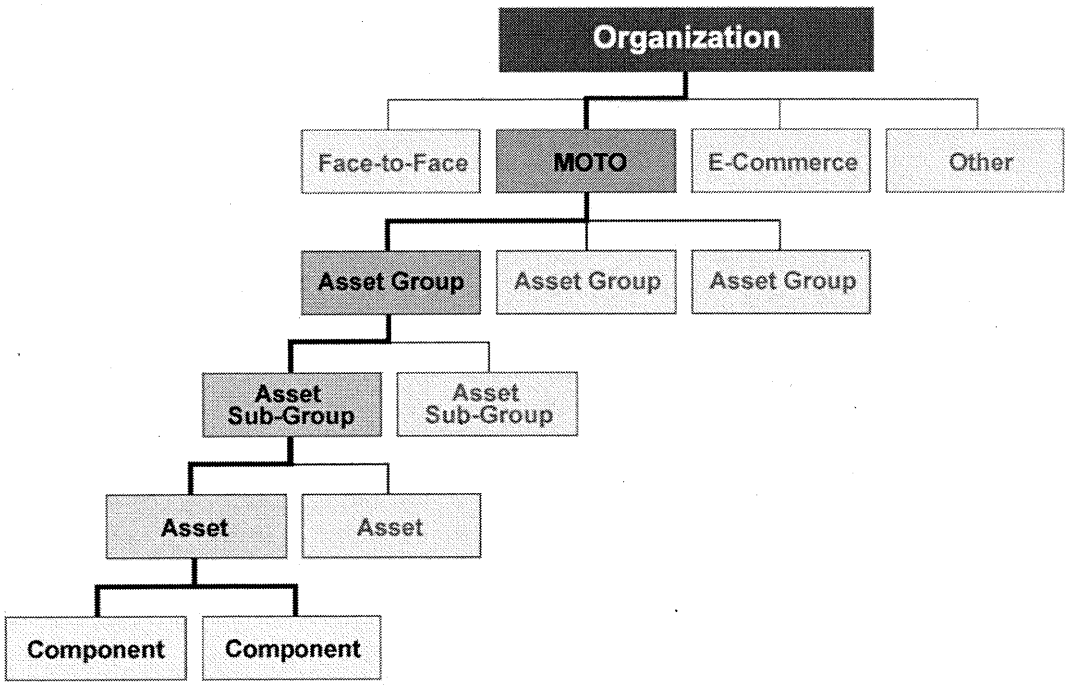


Figure 3.0 - Asset Grouping

- **Threat identification** – Threats may include people, the systems they use, and conditions that could cause harm to an organization. Talking to staff across all areas of an organization will help the risk assessor understand where they see the potential for threats to emerge. Personnel at different levels of the organization will have different perspectives and can provide information that the risk assessor may not have previously considered.

  In addition, security incidents that may have occurred, within either the organization or industry, can be reviewed to help an organization identify potential threats. Threats are commonly measured in terms of the capability of the "threat agent" (anything that has the potential to realize a threat), the intent of the threat agent, relevance to the organization, likelihood that a threat will occur, and the potential for adverse impacts.

- **Vulnerability identification** – A vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organization, the environment, or a business process. In a risk assessment, all vulnerabilities should be considered. For example, vulnerabilities can occur as a result of design, development, and/or deployment deficiencies of systems or software. Organizational and business-process vulnerabilities may exist because of non-existent or ineffective policies and procedures. Vulnerabilities may be identified from vulnerability assessment reports, penetration-test reports and technical security audits such as firewall rule reviews, secure code reviews and database configuration reviews.

Table 1.0 on the following page provides just a few examples of threats and vulnerabilities, together with the possible outcome and impact to an organization's business operations. This is not an exhaustive list, as an organization will encounter many other threats and vulnerabilities that will have the potential to negatively affect their business.

Table 1.0 – Threats, Vulnerabilities, Risk, and Impact

Threats	Vulnerabilities	Potential Outcome/Risk	Potential Impact to Business
External hackers, malicious individuals, cyber criminals	▪ Lack of network security—e.g., properly configured firewalls, lack of intrusion detection ▪ Weak password policy ▪ Transmission of unprotected CHD ▪ Lack of security awareness to social engineering, phishing ▪ Insufficient system hardening, malware protection	▪ Network intrusion ▪ Compromise of user credentials ▪ System compromise ▪ Introduction of malicious code ▪ System downtime ▪ Compromise of sensitive data	▪ Theft of CHD and/or SAD ▪ Reputational impact ▪ Loss of business due to decreased customer confidence ▪ Interruption to business processes ▪ Financial loss—cost of recovery, forensic investigation, lost revenue, possible fines/penalties
Internal malicious individuals, internal user mistakes, human error	▪ Lack of effective change control ▪ Lack of user knowledge/training ▪ Inappropriate assignment of access permissions (e.g., not based on need to know or least privilege) ▪ Lack of separation of duties ▪ Insufficient system hardening ▪ Weak encryption/poor key-management practices	▪ Introduction of malicious code through web browsing/email ▪ Untested system changes ▪ Privilege escalation of user accounts ▪ Unauthorized access to sensitive data	
Thief/intruder intending to cause physical damage or steal assets	▪ Lack of physical security/monitoring ▪ Insecure handling of payment terminals ▪ Lack of tamper-detection ▪ Disposal of storage media without deleting data ▪ Failure to properly supervise visitors/vendors	▪ Theft/replacement of payment terminals ▪ Undetected skimmers added to POS systems ▪ Unintended access to CHD ▪ Installation of rogue devices leading to network compromise	

4.2.2 Risk Profiling

Risk profiling is the presentation of all risks to an asset, together with threats and vulnerabilities and their respective risk scores. Risk profiling enables asset owners to evaluate risks and take necessary risk-mitigation measures.

Risk profiling generally includes the following:

Table 2.0 – Risk Profiling Characteristics

Category	Characteristics
Assets	▪ Asset type (primary or supporting asset, information or business process, hardware or software, etc.) ▪ Asset Value
Threat	▪ Threat Properties (insider or outsider, accidental or deliberate, physical or network, etc.) ▪ Threat likelihood/probability
Vulnerabilities	▪ Vulnerability description ▪ Level of Vulnerability
Risk	Risk score is a function of: ▪ Asset value, ▪ Likelihood of threat, and ▪ Level of vulnerability

4.2.2.1 Existing controls

Existing controls are those that are already present in an organization to protect against the identified threats and vulnerabilities. The identification of existing controls is necessary to determine their adequacy. The effectiveness of existing controls can be identified by reviewing existing policies/procedures, interviewing people, observing processes, and reviewing previous audit reports and incident logs.

4.2.2.2 Risk evaluation

Risk evaluation allows an organization to determine the significance of risks in order to prioritize mitigation efforts. This helps organizations achieve the optimum usage of resources. Risk-measurement techniques used during the evaluation process can be quantitative, qualitative, or a combination of both:

a) **Quantitative risk assessment** – A quantitative risk assessment assigns numerical values to elements of the risk assessment (usually in monetary terms). This is accomplished by incorporating historical data, financial valuation of assets, and industry trends.

Quantitative risk assessments can be regarded as more objective than qualitative risk assessments as they are based on statistical information. However, performing a purely quantitative assessment is often difficult since it may be difficult to determine a monetary value for some assets, such as an organization's "reputation."

b) **Qualitative risk assessment** – Qualitative risk assessments categorize risk parameters according to the level of intensity or impact to an asset. The categorization of risk parameters is accomplished by evaluating the risk components using expert judgment, experience, and situational awareness. The scales are typically based on an escalating set of values—for example, low, moderate, and high.

Tables 2.1 and 2.2 are examples of some commonly used measurement techniques. Table 2.1 evaluates risk as a factor of impact and probability, whereas Table 2.2 represents risk as a factor of asset value, likelihood of threat, and ease of exploitation.

Table 2.1 – Example of a risk calculation matrix

		Consequence		
		Minor Impact	***Moderate Impact***	***Major Impact***
Likelihood	***Very likely***	Medium Risk	High Risk	High Risk
	Likely	Medium Risk	Medium Risk	High Risk
	Possible	Low Risk	Medium Risk	High Risk
	Unlikely	Low Risk	Low Risk	Medium Risk

Table 2.2 – Example of a risk calculation matrix using Asset Value, Threat, and Ease of Exploitation (or Level of Vulnerability)

	Likelihood of Threat	**Low**			**Medium**			**High**		
	Ease of Exploitation	**Low**	**Med**	**High**	**Low**	**Med**	**High**	**Low**	**Med**	**High**
Asset value	***Low***	0	1	2	1	2	3	2	3	4
	Medium	1	2	3	2	3	4	3	4	5
	High	2	3	4	3	4	5	4	5	6
	Very High	3	4	5	4	5	6	5	6	7
	Critical	4	5	6	5	6	7	6	7	8

Low Risk 0-2	Medium Risk 3-5	High Risk 6-8

Qualitative risk assessments are more subjective than quantitative risk assessments but may result in a better understanding of the business, as well as improving communication between the different business departments contributing to the overall risk assessment.

In some cases, numbers are assigned to each value to create a numeric equivalent to the scale. This approach is sometimes referred to as "semi-quantitative" measurement. Such methods are used when it is not possible to use quantitative methods, or when there is a need to reduce the subjectivity in qualitative methods.

Many organizations perform risk assessments using a combination of quantitative and qualitative methods.

4.2.3 Risk Treatment

Once risks have been identified and measured, it is important to define risk treatment strategies. Because the elimination of all risk is usually impractical or close to impossible, it is important to implement the most appropriate controls to decrease risk to an acceptable level. Risk treatment strategies include:

- **Risk reduction** – Taking the mitigation steps necessary to reduce the overall risk to an asset. Often this will include selecting countermeasures that will either reduce the likelihood of occurrence or reduce the severity of loss, or achieve both objectives at the same time. Countermeasures can include technical or operational controls or changes to the physical environment. For example, the risk of computer viruses can be mitigated by acquiring and implementing antivirus software. When evaluating the strength of a control, consideration should be given to whether the controls are preventative or detective. The remaining level of risk after the controls/countermeasures have been applied is often referred to as "residual risk." An organization may choose to undergo a further cycle of risk treatment to address this.
- **Risk sharing/transference**[2] – The organization shares its risk with third parties through insurance and/or service providers. Insurance is a post-event compensatory mechanism used to reduce the burden of loss if the event were to occur. Transference is the shifting of risk from one party to another. For example, when hard-copy documents are moved offsite for storage at a secure-storage vendor location, the responsibility and costs associated with protecting the data transfers to the service provider. The cost of storage may include compensation (insurance) if documents are damaged, lost, or stolen.
- **Risk avoidance** – The practice of eliminating the risk by withdrawing from or not becoming involved in the activity that allows the risk to be realized. For example, an organization decides to discontinue a business process in order to avoid a situation that exposes the organization to risk.
- **Risk acceptance**[2] – An organization decides to accept a particular risk because it falls within its risk-tolerance parameters and therefore agrees to accept the cost when it occurs. Risk acceptance is a viable strategy where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are accepted by default

[2] ***Note:*** *A risk assessment cannot result in the acceptance, transferring, or sharing of any risk that will result in the failure to comply with any applicable PCI DSS requirements.*

5 Third-Party Risks

5.1 Risks Shared With Third Parties

Organizations may outsource business processes, obtain services, or have business relationships with third party merchants, service providers, or other entities that could influence the security of CHD. Performing a risk assessment is essential to understanding the level of risk that could be introduced to the organization by conducting business with third-party merchants and/or service providers. Third parties represent three major areas to consider for risk management: they may introduce risk, they may share risk, or they may manage risk:

	Third Parties may:	Such as:
1	**Introduce risk**	The development of an application that processes, stores, or transmits CHD
2	**Manage risks**	An outsourced business process
3	**Share risk**	A shared business process

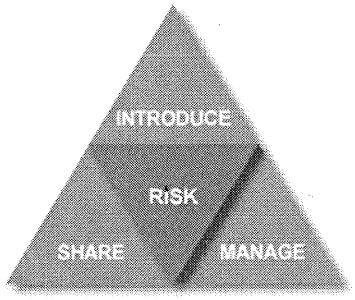


Figure 4.0 - Asset Grouping

A single third-party entity can represent all of these areas at the same time and impact the organization's overall risk posture. The first step to understanding the risks posed by third parties is to know the scope of the business relationship or service provided by the third party. To identify every applicable third party, an organization should study their CHD flows and any business processes involving CHD. In addition, an organization should consider third parties that are involved in the development, operation, or maintenance of their CDE (even those who do not directly handle cardholder information could still indirectly have an impact on the organization's CDE). Some examples of third parties and/or service providers to consider include:

- Application developers
- Data-center providers
- Web-hosting providers
- Data-storage providers
- Data/media/hardware-destruction service providers
- Managed services—for example, IT operations, security
- Outsourced operational teams–for example, call centers
- Contractors

It may be helpful to organizations to understand the key attributes of each third-party relationship, including but not limited to whether the third party is PCI DSS compliant (for instances where the CDE is impacted) or whether their payment application is PA-DSS compliant (for application development); the level of the service provider (often based upon transaction volume); whether appropriate legal contracts are in place between the third party and the organization regarding the management of CHD; and the number of people or systems at the third party who have access to the CHD.

Reviewing a third party's key attributes, such as those listed above, will help an organization to establish a risk level for each third party involved in the development, operation, or maintenance of their CDE and help to prioritize those that appear to carry the highest level of risk.

In addition, it should be noted that a third party may itself be dependent upon other third parties for critical PCI-related services. It may not be necessary or appropriate to extend the risk assessment to the second level of third parties but it is appropriate to know that they exist and may have an impact.

5.2 Risk Sharing/Transference

Once a risk assessment is complete, there are a number of risk treatment options that might be possible. These have previously been discussed in Section 4.2.3, Risk Treatment, and each could apply to a third party.

Risk transference is one of the most relevant risk treatment strategies to third parties, and an organization may manage this relationship by written agreement, via a contractual obligation that states that the third party assumes responsibility for the security of CHD they process, store, or transmit on behalf of the organization. However, the remaining reputational risk means it is unlikely that the full risk to an organization will ever be truly transferred.

Written agreements might help put in place processes to mitigate third-party risks, but it is likely that further assurance is needed to assess whether they have the appropriate security controls and processes in place.

Approaches to the management of third-party risks may include a reliance on a PCI DSS assessment of the third party conducted by a QSA and the completion of a ROC, or where the third party attests compliance to PCI DSS via a Self-Assessment Questionnaire. Alternatively, the organization may perform a risk assessment of the third-party merchant and/or service provider with internal resources and/or work with the third party to determine whether the third party is managing an organization's risks to their satisfaction.

It is recommended that the written agreement (as per PCI DSS Requirement 12.8.2) includes the requirement for the third-party merchant and/or service provider to inform the organization if there is an incident that adversely affects an organization's CHD. Additionally, the organization may wish to conduct a risk assessment to determine the impact, steps for remediation, and associated time frames. Regular communication with the third-party merchant and/or service provider is

recommended so that the details of the incident are known and the status can be reported back to the appropriate stakeholders where necessary.

During the risk assessment process, an organization may determine that continuing business with the third-party merchant and/or service provider may increase the organization's overall risk in respect of CHD and may take appropriate measures to reduce their residual risk to an acceptable level. These measures may include the termination of the business relationship with the third party. As part of the annual risk assessment process, any business relationships with third-party merchants and/or service providers should be re-evaluated.

6 Reporting Results

It is suggested that each risk assessment results in a risk assessment report detailing the identified risks, including those affecting the cardholder data environment. The objective of the report would be to clearly articulate the various risks that concern the organization and may also explain the actions taken by the organization to remediate these risks. The following table includes suggested topics that a report may contain.

Table 3.0 – Risk Assessment Reporting Topics

Topic	Explanation of Content
Scope of Risk Assessment	A risk assessment report should clearly describe the organization and the internal and external parameters taken into consideration when defining the scope of the risk assessment. This may include the purpose of the risk assessment, the technologies in place, business processes, third-party relationships, key stakeholders, and any additional pertinent details. For the purpose of PCI DSS Requirement 12.1.2, the scope may also include an overview of the cardholder data environment and the organizations involved in supporting and operating the processing of cardholder data.
Asset Inventory	This process involves making a comprehensive list of assets that are in scope for the risk assessment, for example, software, hardware, networking and communications infrastructure and personnel. An asset inventory may also include asset value, asset type, asset owner, and asset location for each asset identified.
Threats	The threats that can harm the identified assets should be listed. This list may also include a description of each threat to help understand the characteristics of the identified threats. The likelihood of the threats being realized will be calculated based on the risk assessment methodology used by the organization (expressed as either a percentage probability or a qualitative ranking (e.g., low, medium, or high).
Vulnerabilities	The risk assessment report may also contain a list of vulnerabilities, both technological and organization-related, that can affect the organization's assets. The type of threats that are likely to leverage the vulnerability may also be listed.
Risk Evaluation	The report should describe the risk-measurement technique used to prioritize the identified risks—for example, quantitative or qualitative measures.

Topic	Explanation of Content
Risk Treatment	The risk assessment report should document the list of actions taken for each of the risks identified, along with their completion status—for example, risk reduction, risk transference, etc.
Version History	The risk assessment report may include the date, author, and the approver of the document. The risk assessment date can help an organization to monitor the frequency of their risk assessments, and may help to confirm that assessments are performed at least annually as required by PCI DSS Requirement 12.1.2.
Executive Summary	It can be good practice to include an executive summary of the risk assessment report. The executive summary can detail the risk posture of the organization before and after risk mitigation. The summary can also provide a suitable dashboard of risks for management in terms of number of assets, threats, vulnerabilities, and risks.

7 Critical Success Factors

Identification – The correct identification of assets plays an important role in the risk assessment process. Therefore, organizations should gather input from all stakeholders (such as Human Resources, Information Security, business departments, etc.) that are involved in the processing, storage, and transmission of CHD.

To properly identify threats and vulnerabilities, assessors should have an open mind and factor in the various conditions that could negatively impact the CDE. Historical events, audit reports, and security incidents (within the organization or industry) can also provide additional insight.

Proactive approach – The risk assessment process should be proactive instead of reactive. This will allow the organization to proactively identify, analyze, and document their risks. Taking a proactive approach helps organizations avoid costly corrective measures. Therefore, there is a need for the continuous monitoring of risks throughout the year.

Keeping it simple – The risk assessment process can be kept simple by developing a methodology that best suits the needs of an organization. Published industry-standard methodologies may assist in this process.

Measurement scales should be limited to a small number of categories. Inclusion of numerous categories will often introduce unnecessary complexity and reduce the likelihood that risk stakeholders will understand the results. Each value on a measurement scale should be explicitly defined. Without clear definitions, stakeholders will often form differing opinions on the data. Once the measurements are defined, they should be validated by the individuals who participated in the risk assessment process to ensure that the results are interpreted consistently across the organization.

Training – It is also suggested that risk assessors are trained on formal risk assessment processes to ensure they are better prepared to understand the threats and vulnerabilities that could negatively impact the security of cardholder data, and ultimately their organization.

8 Acknowledgements

The PCI SSC would like to acknowledge the contribution of the Risk Assessment Special Interest Group in the preparation of this document. The members include representatives from the following organizations:

ABC Financial Services	Liquid Networx
Accuvant Inc.	Market America, Inc.
Airlines Reporting Corporation	McGladrey LLP
A-lign Security and Compliance Services	Nationwide Building Society
AOL Inc.	PayPal Inc.
Assurant, Inc.	Progressive Casualty Insurance Company
Bank of America N.A.	Protegrity USA, Inc.
Bankalararası Kart Merkezi (BKM) A.Ş.	Retalix
Barclaycard	Royal Bank of Scotland Group
Bell Canada	SecureState LLC
BrightLine CPAs & Associates, Inc.	Security Risk Management Ltd
BT Counterpane	SecurityMetrics, Inc.
Capita Plc	Sense of Security Pty Ltd
CHS INC	SISA Information Security Inc.
CIPHER Security	Sprint Nextel
Citibank NA, Sucursal Uruguay	Store Financial Services, LLC
Coalfire, Inc.	Suncor Energy Inc.
Compass Group UK & Ireland Limited	Symantec Corp.
Crowe Horwath LLP	Tesco
D+H	Thales eSecurity Limited
Deloitte LLP - UK	The Co-operative Group
Deluxe Corporation	The Members Group
First Data Merchant Services	Tripwire, Inc.
Fiscal Systems, Inc.	Trustwave
Global Payments Inc.	TUI Travel PLC
HP Enterprise Security Services	VeriFone, Inc.
IQ Information Quality	Verizon Enterprise Solutions
Kilrush Consultancy Ltd.	Verizon Wireless
LBMC Security Services	Vodat International Ltd
Levi Strauss and Co.	Yum! Brands, Inc.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT

Plaintiff,

v.

JOHNSON & JOHNSON CONSUMER INC.; and JOHNSON & JOHNSON,

Defendants.

Docket No. 443-7-14 Wncv

FINAL CONSENT JUDGMENT

Plaintiff, the State of Vermont ("State"), has filed an action pursuant to the Chapter 63 of the Vermont Consumer Protection Act, 9 V.S.A. § 2451, *et seq.* alleging violations thereof. Plaintiff, by its counsel, and Defendants, by their counsel, have consented to entry of this Final Consent Judgment ("Judgment") without trial or adjudication of any issue of fact or law or finding of wrongdoing or liability of any kind.

I. Findings

A. The Court has jurisdiction over the subject matter of this lawsuit and over the Parties. Johnson & Johnson consents to the jurisdiction of the Court solely for the purposes of this Judgment.

B. The terms of this Consent Judgment shall be governed by the laws of the State of Vermont.

C. Entry of this Consent Judgment is in the public interest and reflects a negotiated agreement among the Parties.

D. Johnson & Johnson Consumer Inc. operates a division known as McNeil Consumer Healthcare Division ("McNeil"). McNeil's executive offices are located at 7050 Camp Hill Road, Fort Washington, PA 19034. Johnson & Johnson Consumer Inc. is a subsidiary of Johnson & Johnson. Johnson & Johnson's executive offices are located at One Johnson & Johnson Plaza, New Brunswick, NJ, 08933. At all times relevant hereto, McNeil engaged in commerce affecting Vermont consumers within the meaning of the CPA, including, but not limited to, in Washington County.

E. The Attorneys General of the Multistate Working Group (defined below and collectively referred to hereinafter as the "State Attorneys General"), conducted a multistate investigation into certain McNeil acts and practices.

F. The State Attorneys General have individually and collectively determined to resolve the investigation by entering into similar settlement agreements between defendants and each signatory Attorney General.

G. By entering into this Judgment, the Parties have agreed to resolve claims related to certain McNeil business practices under each state's Consumer Protection Laws.

H. This Judgment does not constitute an admission by McNeil for any purpose, of any fact or of a violation of any state law, rule, or regulation, nor does this Judgment constitute evidence or admission of any liability, fault or wrongdoing, all of which McNeil denies. McNeil does not admit any violation of law, and

does not admit any wrongdoing that was or could have been alleged by the State before the date of this Judgment.

I. This Judgment is made without trial or adjudication of any issue of fact or law or finding of liability of any kind. It is the intent of the Parties that this Judgment shall not be binding or admissible in any other matter, including, but not limited to, any investigation or litigation, other than in connection with the enforcement of this Judgment. No part of this Judgment shall create a private cause of action or confer any right to any third party for violation of any federal or state statute except that a State may file an action to enforce the terms of this Judgment.

J. McNeil is entering into this Judgment solely for the purpose of the settlement of the instant action. This Judgment does not create a waiver of or limit McNeil's legal rights, remedies, or defenses in any other action by the Vermont Attorney General, and does not waive or limit McNeil's right to defend itself from, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of this Judgment. Nothing in this Judgment shall waive, release, or otherwise affect any claims, defenses, or positions McNeil may have in connection with any investigations, claims, or other matters the State is not releasing hereunder. Notwithstanding the foregoing, a State may file an action to enforce the terms of this Judgment.

K. Nothing in this Judgment shall require McNeil to:

1. Take any action that is prohibited by the Federal Food, Drug and Cosmetic Act ("FDCA") or any regulation promulgated thereunder, or by the U.S. Food and Drug Administration ("FDA"); or

2. Fail to take any action that is required by the FDCA or any regulation promulgated thereunder, or by the FDA.

L. This Judgment (or any portion thereof) shall in no way prohibit, limit, or restrict McNeil from making representations with respect to its products that are permitted or authorized under Federal law, the FDCA, or the FDA or FDA Guidance for Industry, so long as those representations, taken in their entirety, are not false, misleading, or deceptive. Further, the Judgment shall in no way prohibit, limit, or restrict McNeil from making representations with respect to its products that are required or authorized by, or consistent with, the FDA-approved labeling requirements for McNeil products, so long as the representation, taken in its entirety, is not false, misleading, or deceptive.

M. The State's acceptance of this Judgment shall not be deemed approval by the State of any of McNeil's advertising or business practices. Further, neither McNeil, nor anyone acting on its behalf shall state or imply, or cause to be stated or implied, that the State or any other governmental unit of the State has approved, sanctioned or authorized any practice, act, advertisement or conduct of McNeil.

N. Any failure by any party to this Judgment to insist upon the strict performance by another party of any provision of this Judgment shall not be deemed a waiver of any such provision. Notwithstanding such failure, the party shall have the right thereafter to insist upon the specific performance of any and all of the provisions of this Judgment, the payment of attorney's fees, the imposition of any applicable penalties, and any other applicable remedies, including but not limited to,

contempt and civil penalties as set forth in the CPA and/or other applicable state law.

II. Definitions

A. "CPA" shall mean the laws of Vermont, as cited among those listed in footnote 1.[1]

B. "Covered Conduct" shall mean McNeil's business practices relating to the Covered Products that were the subject of recalls or retrievals during the calendar

[1] ALASKA - ; ARIZONA – *Arizona Consumer Fraud Act*, A.R.S. § 44-1521 et seq.; ARKANSAS - *Ark. Code Ann.* § 4-88-101, *et seq.*,; CALIFORNIA – Bus. & Prof Code §§ 17200 et seq. and 17500 *et seq.*; COLORADO – *Colorado Consumer Protection Act*, Colo. Rev. Stat. § 6-1-101 *et seq.*; CONNECTICUT – *Connecticut Unfair Trade Practices Act,* Conn. Gen. Stat. §§ 42-110a *et seq.;* DELAWARE – DELAWARE – *Delaware Consumer Fraud Act and Delaware Deceptive Trade Practice Act*, Del. CODE ANN. tit. 6, §§ 2511 to 2527; DISTRICT OF COLUMBIA, *District of Columbia Consumer Protection Procedures Act*, D.C. Code §§ 28-3901 *et seq.*; FLORIDA – *Florida Deceptive and Unfair Trade Practices Act, Part II*, Chapter 501, Florida Statutes, 501.201 *et. seq.*; HAWAII –*Uniform Deceptive Trade Practice Act,* Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Chpt. 480; IDAHO – *Consumer Protection Act*, Idaho Code Section 48-601 *et seq.*; ILLINOIS – *Consumer Fraud and Deceptive Business Practices Act*, 815 ILCS 505/2 *et seq.*; INDIANA - *Deceptive Consumer Sales Act*, I.C. § 24-5-0.5*et seq*; KANSAS - *Kansas Consumer Protection Act*, K.S.A. 50-623 *et seq.*; KENTUCKY - KRS 367.110 et seq.; LOUISIANA – *Unfair Trade-Practices and Consumer Protection Law*, LSA-R.S. 51:1401, *et seq.*; MAINE – *Unfair Trade Practices Act*, 5 M.R.S.A. § 207 *et seq.*; MARYLAND - *Maryland Consumer Protection Act*, Md. Code Ann., Com. Law § 13-101 *et seq.*; MASSACHUSETTS – *Mass. Gen. Laws* c. 93A, §§ 2 and 4; MICHIGAN – *Michigan Consumer Protection Act*, MCL § 445.901 *et seq.*; MINNESOTA - *Minnesota Deceptive Trade Practices Act*, Minn. Stat. §§ 325D.43-48; *Minnesota False Advertising Act*, Minn. Stat. § 325F.67; *Minnesota Consumer Fraud Act*, Minn. Stat. §§ 325F.68-70; *Minnesota Deceptive Trade Practices Against Senior Citizens or Disabled Persons Act*, Minn. Stat. § 325F.71.; MISSOURI – Merchandising Practices Act, Chapter 407, RSMo. MONTANA - *Mont. Code Ann. § 30-14-101 et. seq.*; NEBRASKA – *Uniform Deceptive Trade Practices Act*, NRS §§ 87-301 *et seq.*; NEVADA – *Deceptive Trade Practices Act*, Nevada Revised Statutes 598.0903 *et seq.*; NEW HAMPSHIRE – *New Hampshire Consumer Protection Act*, RSA 358-A; NEW JERSEY – *New Jersey Consumer Fraud Act*, NJSA 56:8-1 *et seq.*; NEW MEXICO - *New Mexico Unfair Practices Act* NMSA 1978, S 57-12-1 *et seq.* (1967); NEW YORK – General Business Law Art. 22-A, §§ 349-50, and Executive Law § 63(12); NORTH CAROLINA – *North Carolina Unfair and Deceptive Trade Practices Act*, N.C.G.S. §§ 75-1.1, *et seq.*; NORTH DAKOTA – *Unlawful Sales or Advertising Practices*, N.D. Cent. Code § 51-15-02 *et seq.*; OHIO – *Ohio Consumer Sales Practices Act*, R.C. 1345.01, *et seq.*; PENNSYLVANIA – *Pennsylvania Unfair Trade Practices and Consumer Protection Law*, 73 P.S. 201-1 *et seq.*; RHODE ISLAND - *Rhode Island Deceptive Trade Practices Act*, Rhode Island General Laws § 6-13.1-1, *et seq.*; SOUTH CAROLINA - ; SOUTH DAKOTA – *South Dakota Deceptive Trade Practices and Consumer Protection*, SDCL ch. 37-24; TENNESSEE – *Tennessee Consumer Protection Act*, Tenn. Code Ann. 47-18-101 *et seq.*; TEXAS – Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. And Com. Code 17.41, *et seq.*; VERMONT – *Consumer Protection Act*, 9 V.S.A. §§ 2451 *et seq.*; VIRGINIA - *Virginia Consumer Protection Act*, Va. Code Ann. §§ 59.1-196 through 59.1-207; WASHINGTON – *Unfair Business Practices/Consumer Protection Act*, RCW §§ 19.86 *et seq.*; WEST VIRGINIA – *West Virginia Consumer Credit and Protection Act,* W.Va. §46A-1-101 et seq.; WISCONSIN – Wis. Stat. § 100.18 (Fraudulent Representations).

years 2009 through 2011, meaning (1) alleged representations prior to the Effective Date of this Judgment regarding the quality or safety of Covered Products during the above-referenced time period; or (2) the introduction into the stream of commerce of Vermont during the same time period of Covered Products that Vermont alleges or could have alleged were not manufactured in accordance with current Good Manufacturing Practices.

C. "Covered Products" shall mean the products listed in Exhibit A hereto.

D. "current Good Manufacturing Practices" or "cGMP" shall mean those practices that comply with the current Good Manufacturing Practice regulations promulgated by the FDA at 21 C.F.R. parts 210-211, together with any subsequent amendments or additions.

E. "Effective Date" shall mean the date on which a copy of this Judgment, duly executed by McNeil and by the Vermont Attorney General, is approved by and becomes a judgment of the Court.

F. "McNeil" shall mean (i) McNeil Consumer Healthcare, a division of Johnson & Johnson Consumer Inc.; (ii) the legal entity responsible for manufacturing, selling, offering for sale, promoting, or distributing the Covered Products to the extent that such successor manufactures, sells, offers for sale, promotes or distributes the Covered Products; and (iii) all successors to these entities to the extent that such successor manufactures, sells, offers for sale, promotes, or distributes the Covered Products.

G. "Multistate Executive Committee" shall mean the Attorneys General and their staffs representing Arizona, Delaware, District of Columbia, Florida, Kentucky, Maryland, Massachusetts, Montana, New Jersey, Ohio, Pennsylvania, and Texas.

H. "Multistate Working Group" shall mean the Attorneys General and their staffs representing Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Hawaii[2], Idaho, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, and Wisconsin.

I. "OTC Drug Product," for the purposes of this Judgment, shall mean an OTC drug whose product brand name is included on Exhibit A hereto.

J. "Parties" shall mean McNeil and the Vermont Attorney General.

K. "Recall" shall mean Recall as defined by 21 C.F.R. §§ 7.3(g), provided that the recall is assigned the classification "Class I" by the FDA as defined in 21 C.F.R. §7.3(m)(1) or assigned the classification "Class II" by the FDA as defined in 21 C.F.R. § 7.3(m)(2).

III. Injunctive Terms

IT IS ORDERED THAT McNeil shall not:

---

[2] Hawaii is being represented in this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity, the entire group will be referred to as the "Attorneys General," and such designation, as it includes Hawaii, refers to the Executive Director of the State of Hawaii Office of Consumer Protection.

A. Represent on www.mcneil-consumer.com or any other McNeil-operated website that McNeil's OTC Drug Product manufacturing facilities meet current Good Manufacturing Practices (cGMP) outlined by the FDA if McNeil has had a Class I or Class II Recall of OTC Drug products within the prior twelve (12) months caused by cGMP noncompliance at its Fort Washington, Pennsylvania or Las Piedras, Puerto Rico manufacturing facilities.

B. For a period of five (5) years from the Effective Date, fail to follow its operative internal standard operating policies regarding whether to open a Corrective Action/Preventive Action (CAPA) during the manufacture of OTC Drug Products.

C. For a period of five (5) years from the Effective Date, fail to provide within sixty (60) days of a written request from the Vermont Attorney General, who shall distribute to any other requesting State Attorneys General, information concerning the identity of wholesalers or warehouses to which any OTC Drug Product that is subject to a Recall was distributed in its State, to the extent that any such requested information is in McNeil's possession. McNeil may enter into agreements with the Vermont Attorney General to ensure the confidentiality of any records or information produced under this provision, and reserves the right to invoke any available protection or privilege for trade secrets or other legally protected information under state or federal law. Nothing in this section shall be interpreted to limit the State's Civil Investigative Demand ("CID") or investigative subpoena authority.

IV. Payment

A. No later than thirty (30) days after the Effective Date of this Judgment, McNeil shall pay $33,000,000 to be divided and paid by McNeil directly to the State Attorneys General of the Multistate Working Group in amounts to be designated by and in the sole discretion of the Multistate Executive Committee.

Said payments to the State Attorneys General shall be used by each State Attorney General for attorneys' fees and other costs of investigation and litigation, or to be placed in, or applied to, the consumer protection enforcement fund, consumer education or litigation or local consumer aid or revolving fund, used to defray the costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of each State Attorney General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II, § 27 and 32 V.S.A. § 462. The parties acknowledge that the payment described herein is not a fine, penalty, or payment in lieu thereof. The State of Vermont's share is $377,832.59.

V. Release

A. Upon full and complete performance of the monetary provisions set forth in paragraph IV, the State releases McNeil, and its parent, subsidiaries, affiliates, predecessors, and successors, (the "Released Parties") from the following: all civil claims, causes of action, damages, restitution, fines, costs, attorney's fees, and penalties that the State has asserted or could have asserted against the Released Parties under the Consumer Protection Laws (as identified in footnote 1) or under common law concerning unfair, deceptive, or fraudulent trade practices, other than those reserved or excluded under Section V. B. below

resulting from the Covered Conduct up to and including the Effective Date of this Judgment (collectively, the "Released Claims").

B. Notwithstanding any term of this Judgment, specifically reserved and excluded from the Released Claims as to any entity or person, including Released Parties, are any and all of the following:

1. Any criminal liability that any person or entity, including Released Parties, has or may have to the State;

2. Any civil or administrative liability that any person or entity, including Released Parties, has or may have to the State under any statute, regulation, or rule not expressly covered by the release in Section V.A including, but not limited to, any and all of the following claims:

   a. State or federal antitrust and tax violations;

   b. Medicaid violations including, but not limited to, federal Medicaid drug rebate statute violations, Medicaid fraud or abuse, and/or kickback violations related to the State's Medicaid program;

   c. Claims involving "best price," "average wholesale price," or "wholesale acquisition cost"; and

   d. State false claims violations;

3. Claims to enforce the terms and conditions of this Judgment;

4. Actions of state program payors of the State arising from the Covered Conduct, except for the release of civil penalties under the CPA; and

5. Any claims individual consumers have or may have against any person or entity, including Released Parties.

VI. Dispute Resolution

A. For purposes of resolving any disputes with respect to compliance with this Judgment, should the Vermont Attorney General believe that McNeil has violated a provision of this Judgment subsequent to the Effective Date, the Vermont Attorney General shall notify McNeil in writing of the specific objection, identify with particularity the provisions of this Judgment that the practice allegedly violates, and give McNeil thirty (30) business days to respond to the notification.

B. Upon receipt of written notice from the Vermont Attorney General, McNeil shall provide a good-faith written response to the Vermont Attorney General's notification, containing either a statement explaining why McNeil believes it is in compliance with the Judgment or a detailed explanation of how the alleged violation occurred and statement explaining how and when McNeil intends to remedy the alleged violation.

C. Except as set forth in Section VI Paragraph D or E below, the Vermont Attorney General may not take any action during the 30-day response period. Nothing shall prevent the Vermont Attorney General from agreeing in writing to provide McNeil with additional time to respond to the notice.

D. Nothing in this Dispute Resolution Section shall be interpreted to limit Vermont's CID authority and McNeil reserves all of its rights with respect to a CID issued pursuant to such authority.

E. The Vermont Attorney General may assert any claim that McNeil has violated this Judgment in a separate civil action to enforce compliance with this Judgment, or may seek any other relief afforded by law, but only after providing McNeil an opportunity to respond to the notification as described above and to remedy the

alleged violation within the 30-day response period as described above, or within any other period as agreed to by McNeil and the Vermont Attorney General; provided, however, that the Vermont Attorney General may take any action if the Vermont Attorney General believes that, because of the specific practice, a threat to the health or safety of the public requires immediate action.

VII. General Provisions

A. McNeil shall not cause third parties acting on its behalf to engage in practices from which McNeil is prohibited by this Judgment.

B. This Judgment represents the full and complete terms of the settlement entered into by the Parties hereto. In any action undertaken by the Parties, neither prior versions of this Judgment, nor prior versions of any of its terms that were not entered by the Court in this Judgment, may be introduced for any purpose whatsoever. The Parties acknowledge that no other promises, representations, or agreements of any nature have been made or entered into by the Parties. The Parties further acknowledge that this Judgment constitutes a single and entire agreement that is not severable or divisible, except that if any provision herein is found to be legally insufficient or unenforceable, the remaining provisions shall continue in full force and effect.

C. This Court retains jurisdiction over this Judgment and the Parties hereto for the purpose of enforcing and modifying this Judgment and for the purpose of granting such additional relief as may be necessary and appropriate.

D. This Judgment may be executed in counterparts, and a facsimile or .pdf signature shall be deemed to be, and shall have the same force and effect as, an original signature.

E. All notices under this Judgment shall be provided to:

For McNeil:

Ethan M. Posner, Esq.
COVINGTON & BURLING LLP
850 Tenth Street NW
Washington, DC 20001
(202) 662-5317
eposner@cov.com

For the Vermont Attorney General:

Jill S. Abrams
Assistant Attorney General
109 State Street
Montpelier, Vermont 05609

_____
Superior Court Judge

For Plaintiff State of Vermont
Thomas J. Donovan, Jr.
Attorney General

By: _____
Jill S. Abrams
Assistant Attorney General

Date: 5/23/2017

Defendants Johnson & Johnson Consumer, Inc. and Johnson & Johnson

Johnson & Johnson Consumer Inc.

Date: 05/18/2017

By:_____
Parisa Mazaheri Tameh
Secretary

Johnson & Johnson

Date: 5/18/17

By:_____
Lacey P. Elberg
Assistant Secretary

Approved as to form:

Date: 5-17-17

By: _____
Ethan M. Posner
Stephen P. Anthony
Christopher M. Denig
Joshua N. DeBold
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
Counsel for Defendants

Date:

By: _____
Edward H. Dixon
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
Local Counsel for Defendants

Approved as to form:

Date:

By: _____
Ethan M. Posner
Stephen P. Anthony
Christopher M. Denig
Joshua N. DeBold
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
Counsel for Defendants

Date: May 18, 2017

By: _____
Edward H. Dixon
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
Local Counsel for Defendants

EXHIBIT A

Recall Date	Product Name	UPC	Lot
4/2/2009	Motrin IB Tablets, 200mg 8 count vial	300450481689	SHC003
4/2/2009	Motrin IB Tablets, 200mg 8 count vial	300450481689	SHC004
9/11/2009	Children's Tylenol Plus Cold MS Suspension 4 oz. Grape	300450391049	SBM041
9/11/2009	Children's Tylenol Suspension 4oz. Grape	300450296047	SBM042
9/11/2009	Children's Tylenol Suspension 4oz. Bubble Gum	300450407047	SBM043
9/11/2009	Children's Tylenol Suspension 4oz. Bubble Gum	300450407047	SBM044
9/11/2009	Children's Tylenol Suspension 4oz. Strawberry	300450493040	SBM045
9/11/2009	Infant's Tylenol Grape Suspension Drops 1/4oz	300450122407	SBM064
9/11/2009	Infant's Tylenol Suspension 1/2oz. Cherry	300450186157	SBM065
9/11/2009	Children's Dye Free Suspension 4oz. Cherry	300450166043	SBM066
9/11/2009	Children's Tylenol Plus Cold MS Suspension 4 oz. Grape	300450391049	SBM067
9/11/2009	Children's Tylenol Suspension 4oz. Cherry	300450123046	SBM068
9/11/2009	Children's Tylenol Plus Cough & Runny Nose 4oz. Cherry	300450249043	SBM069
9/11/2009	Children's Tylenol Plus Cough & Runny Nose 4oz. Cherry	300450249043	SBM070
9/11/2009	Infant's Tylenol Suspension 1/2oz. Cherry	300450186157	SCM005
9/11/2009	Infant's Tylenol Suspension 1/2oz. Cherry	300450186157	SCM006
9/11/2009	Children's Tylenol Suspension 4oz. Strawberry	300450493040	SCM011
9/11/2009	Infant's Tylenol Suspension Drops 1/2oz. Grape	300450122155	SCM012
9/11/2009	Children's Tylenol Plus Flu 4oz. Bubble Gum	300450386045	SCM013
9/11/2009	Children's Tylenol Plus Flu 4oz. Bubble Gum	300450386045	SCM014
9/11/2009	Children's Tylenol Suspension 4oz. Grape	300450296047	SCM015
9/11/2009	Children's Tylenol Plus Cold Suspension 4oz. Grape	300450387042	SCM016
9/11/2009	Children's Tylenol Plus Cough/ST Suspension 4oz. Cherry	300450247049	SCM017
9/11/2009	Children's Tylenol Suspension 4oz. Bubble Gum	300450407047	SCM029
9/11/2009	Children's Tylenol Suspension 4oz. Strawberry	300450493040	SCM030
9/11/2009	Infant's Tylenol Grape Suspension Drops 1/4oz	300450122407	SCM033
9/11/2009	Infant's Tylenol Grape Suspension Drops H/G 1/2oz.	350580144183	SCM034
9/11/2009	Children's Tylenol Suspension 4oz. Cherry	300450123046	SCM035
9/11/2009	Children's Tylenol Suspension 4oz. Grape	300450296047	SCM036
9/11/2009	Children's Tylenol Plus Cold MS Suspension 4 oz. Grape	300450391049	SCM037
9/11/2009	Infant's Tylenol Suspension Drops 1/2oz. Grape	300450122155	SCM067
9/11/2009	Children's Dye Free Suspension 4oz. Cherry	300450166043	SCM068
9/11/2009	Children's Tylenol Plus Flu 4oz. Bubble Gum	300450386045	SCM069
9/11/2009	Children's Tylenol Suspension 4oz. Cherry	300450123046	SCM070
9/11/2009	Children's Tylenol Suspension 4oz. Cherry	300450123046	SCM080
9/11/2009	Children's Tylenol Plus Cough & Runny Nose 4oz. Cherry	300450249043	SCM081
9/11/2009	Infant's Tylenol Suspension Drops 1oz. Grape	300450122018	SCM082
9/11/2009	Infant's Tylenol Dye Free Suspension 1oz. Cherry	300450167019	SCM083
9/11/2009	Infant's Tylenol Dye Free Suspension 1oz. Cherry	300450167019	SCM084
9/11/2009	Children's Tylenol Suspension 4oz. Cherry	300450123046	SDM005
9/11/2009	Children's Tylenol Plus Cough & Runny Nose 4oz. Cherry	300450249043	SDM006
9/11/2009	Infant's Tylenol Suspension Drops 1/2oz. Grape	300450122155	SDM007
9/11/2009	Infant's Tylenol Dye Free Suspension 1oz. Cherry	300450167019	SDM008
9/11/2009	Infant's Tylenol Suspension Drops 1oz. Cherry	300450186300	SDM009
9/11/2009	Infant's Tylenol Grape Suspension Drops 1/4oz	300450122407	SDM020
9/11/2009	Children's Tylenol Plus Cold MS Suspension 4 oz. Grape	300450391049	SDM027
9/11/2009	Children's Tylenol Suspension 4oz. Cherry, Hospital Govt.	350580123034	SDM028
9/11/2009	Infant's Tylenol Suspension 1/2oz. Cherry	300450186157	SDM032
9/11/2009	Children's Tylenol Plus Cold/Allergy 4oz. Bubble Gum	300450390042	SDM033
9/11/2009	Children's Tylenol Suspension 4oz. Grape	300450296047	SDM034
9/11/2009	Children's Tylenol Suspension 4oz. Strawberry	300450493040	SDM035
9/11/2009	Infant's Tylenol Suspension Drops 1oz. Cherry	300450186300	SDM038
9/11/2009	Infant's Tylenol Suspension Drops 1oz. Grape	300450122018	SDM039
9/11/2009	Infant's Tylenol Grape Suspension Drops 1oz.	300450122018	SDM040
9/11/2009	Children's Tylenol Pediatric Suspension 1oz. Cherry	300450123015	SDM064
9/11/2009	Infant's Tylenol Suspension Drops 1/2oz. Grape	300450122155	SDM068
9/11/2009	Infant's Tylenol Drops 1oz. Grape	300450122100	SDM078
9/11/2009	Children's Tylenol Plus Cold MS Suspension 4 oz. Grape	300450391049	SEM109
9/11/2009	Children's Tylenol Plus Cold Suspension 4oz. Grape	300450387042	SFM024
10/2/2009	Johnson's Baby Relief Kit	381370026426	1498J
10/2/2009	Johnson's Baby Relief Kit	381370026426	1508J

Recall Date	Product Name	UPC	Lot
10/2/2009	Johnson's Baby Relief Kit	381370026426	1518J
10/2/2009	Johnson's Baby Relief Kit	381370026426	2068J
10/2/2009	Johnson's Baby Relief Kit	381370026426	2348J
10/2/2009	Johnson's Baby Relief Kit	381370026426	2358J
10/2/2009	Johnson's Baby Relief Kit	381370026426	2738J
11/6/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08BMC013
11/6/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08BMC020
11/6/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09BMC034
11/6/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09CMC036
11/6/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09CMC040
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07CMC011
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07DMC022
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07DMC024
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07FMC032
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07FMC033
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07GMC038
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07GMC039
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07HMC045
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07HMC051
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07HMC053
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07JMC064
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07JMC069
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07JMC070
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07JMC071
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07XMC055
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07XMC058
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	07XMC062
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08AMC002
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08AMC005
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08CMC026
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08DMC029
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08EMC037
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08EMC039
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08FMC044
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08FMC045
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08GMC050
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08GMC053
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08GMC063
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08GMC065
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08JMC103
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08JMC109
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08JMC110
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08JMC111
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08KMC124
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08KMC127
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08KMC131
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08KMC132
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08XMC093
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08XMC094
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	08XMC095
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09AMC010
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09CMC041
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09EMC075
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09EMC076
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09EMC079
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09GMC096
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09GMC097
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09GMC099
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09JMC118
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09JMC126
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09KMC133
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09KMC134
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09XMC114
12/18/2009	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09XMC116
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 300ct	300450126030	AHM368

Recall Date	Product Name	UPC	Lot
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 300ct	300450126030	ALM377
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 300ct	300450126030	ALM378
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 300ct	300450126030	AMM354
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 300ct	300450126030	APM427
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AEM050
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AHM374
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AJM320
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AJM402
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	ALM341
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AMM365
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AMM366
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	AMM367
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	APM350
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 100ct	300450126108	APM351
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 180ct	300450126184	AMM323
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 180ct	300450126184	AMM433
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 180ct	300450126184	APM304
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	AFM026
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	AHM327
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	AHM432
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	AJM321
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	ALM327
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	AMM324
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	APM349
1/15/2010	ST. JOSEPH ASPIRIN ENTERIC TAB 36ct	300450126368	APM420
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 3x36ct	300450173089	AFM360
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 3x36ct	300450173089	AHM423
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 3x36ct	300450173089	ALM346
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 3x36ct	300450173089	AMM434
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 36ct	300450173362	AHM440
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 36ct	300450173362	AMM325
1/15/2010	ST. JOSEPH ASPIRIN CHEWABLE ORANGE TABLET 36ct	300450173362	APM430
1/15/2010	Extra Strength TYLENOL PM GELTAB 24ct	300450176240	ABA001
1/15/2010	Extra Strength TYLENOL PM GELTAB 24ct	300450176240	ABA370
1/15/2010	Extra Strength TYLENOL PM GELTAB 24ct	300450176240	AFA310
1/15/2010	Extra Strength TYLENOL PM GELTAB 24ct	300450176240	AHA083
1/15/2010	Extra Strength TYLENOL PM GELTAB 24ct	300450176240	AJA051
1/15/2010	Extra Strength TYLENOL PM GELTAB 50ct	300450176509	AFA177
1/15/2010	Extra Strength TYLENOL PM GELTAB 50ct	300450176509	AFA326
1/15/2010	Extra Strength TYLENOL PM GELTAB 50+20ct	300450176707	AJA098
1/15/2010	BENADRYL ALLERGY TABLET 148ct	350580226148	AAA422
1/15/2010	BENADRYL ALLERGY TABLET 148ct	350580226148	ABA392
1/15/2010	BENADRYL ALLERGY TABLET 148ct	300450226143	AJA094
1/15/2010	BENADRYL ALLERGY TABLET 148ct	300450226143	ALA034
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 20ct	300450244208	ABA002
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 20ct	300450244208	ABA265
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 20ct	300450244208	ADA281
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 20ct	300450244208	AFA327
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 40ct	300450244406	ACA422
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 40ct	300450244406	AEA077
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 40ct	300450244406	AEA258
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 40ct	300450244406	AFA059
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 40ct	300450244406	AFA192
1/15/2010	TYLENOL PM RAPID RELEASE GELCAP 40ct	300450244406	AHA172
1/15/2010	TYLENOL ARTHRITIS GELTAB 20ct	300450292209	09BMC031
1/15/2010	TYLENOL ARTHRITIS GELTAB 40ct	300450292407	08KMC130
1/15/2010	TYLENOL ARTHRITIS GELTAB 40ct	300450292407	09BMC024
1/15/2010	TYLENOL ARTHRITIS GELTAB 80ct	300450292803	ALM345
1/15/2010	TYLENOL ARTHRITIS GELTAB 80ct	300450292803	APM305
1/15/2010	TYLENOL ARTHRITIS GELTAB 80ct	300450292803	APM419
1/15/2010	TYLENOL ARTHRITIS GELTAB 80ct	300450292803	ASM357
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	ACM037
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	AFM351
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	AHM316
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	AHM376

Recall Date	Product Name	UPC	Lot
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	AHM422
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	ALM388
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	ALM458
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	AMM368
1/15/2010	TYLENOL 8 HOUR CAPLET 100ct	300450297112	AMM435
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297242	ADM032
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	ACM056
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	ADM031
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	AEM087
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	AEM105
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	ALM325
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	AMM322
1/15/2010	TYLENOL 8 HOUR CAPLET 24ct	300450297266	ASM379
1/15/2010	Extra Strength TYLENOL EZTAB 24ct	300450422248	ABA154
1/15/2010	Extra Strength TYLENOL EZTAB 24ct	300450422248	ADA193
1/15/2010	Extra Strength TYLENOL EZTAB 24ct	300450422248	AFA243
1/15/2010	Extra Strength TYLENOL EZTAB 24ct	300450422248	AHA039
1/15/2010	Extra Strength TYLENOL EZTAB 50ct	300450422507	ADA013
1/15/2010	Extra Strength TYLENOL EZTAB 50ct	300450422507	AEA259
1/15/2010	Extra Strength TYLENOL EZTAB 50ct	300450422507	AHA091
1/15/2010	Extra Strength TYLENOL EZTAB 50ct	300450422507	AJA010
1/15/2010	Extra Strength TYLENOL EZTAB 50ct	300450422507	AJA123
1/15/2010	Extra Strength TYLENOL EZTAB 50+25ct	300450422750	ACA562
1/15/2010	Extra Strength TYLENOL EZTAB 50+25ct	300450422750	ACA743
1/15/2010	Extra Strength TYLENOL EZTAB 50+25ct	300450422750	ALA173
1/15/2010	Extra Strength TYLENOL COOL CAPLET 100ct	300450444103	ALA249
1/15/2010	Extra Strength TYLENOL CAPLET 225ct	300450444271	SSA011
1/15/2010	Extra Strength TYLENOL CAPLET 24+12ct	300450444318	ABA565
1/15/2010	Extra Strength TYLENOL CAPLET 24+12ct	300450444318	AHA040
1/15/2010	Extra Strength TYLENOL CAPLET 24+12ct	300450444318	AJA028
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	09BMC018
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	09CMC048
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	09FMC082
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	09FMC084
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	AAA405
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	ADA014
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	ADA087
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	ADA270
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	ADA271
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	ADA417
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	AEA348
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	AFA102
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	AJA045
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	ALA028
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SFA179
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SFA237
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SFA295
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SHA002
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SJA025
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SJA189
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SJA232
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SLA004
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SLA160
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SLA296
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SMA173
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SMA174
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SPA005
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SPA038
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SPA058
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SPA386
1/15/2010	Extra Strength TYLENOL CAPLET 325ct	300450444325	SSA055
1/15/2010	Extra Strength TYLENOL COOL CAPLET 50ct	300450444509	ABA029
1/15/2010	Extra Strength TYLENOL COOL CAPLET 50ct	300450444509	ACA563
1/15/2010	Extra Strength TYLENOL COOL CAPLET 50ct	300450444509	ADA190
1/15/2010	Extra Strength TYLENOL COOL CAPLET 50ct	300450444509	AHA081

Recall Date	Product Name	UPC	Lot
1/15/2010	Extra Strength TYLENOL COOL CAPLET 50ct	300450444509	AJA095
1/15/2010	Extra Strength TYLENOL COOL CAPLET 50ct	300450444509	AJA175
1/15/2010	Extra Strength TYLENOL CAPLET 50+25ct	300450444752	ACA599
1/15/2010	Extra Strength TYLENOL CAPLET 50+25ct	300450444752	ACA755
1/15/2010	Extra Strength TYLENOL CAPLET 100+25ct	300450449009	SDA203
1/15/2010	Extra Strength TYLENOL CAPLET 100+25ct	300450449009	SHA035
1/15/2010	Extra Strength TYLENOL CAPLET 24ct	300450449054	AAA408
1/15/2010	Extra Strength TYLENOL CAPLET 24ct	300450449054	ABA169
1/15/2010	Extra Strength TYLENOL CAPLET 24ct	300450449054	ABA568
1/15/2010	Extra Strength TYLENOL CAPLET 24ct	300450449054	ADA192
1/15/2010	Extra Strength TYLENOL CAPLET 24ct	300450449054	AHA048
1/15/2010	Extra Strength TYLENOL CAPLET 24ct	300450449054	AJA145
1/15/2010	Extra Strength TYLENOL CAPLET 50ct	300450449078	AEA206
1/15/2010	Extra Strength TYLENOL CAPLET 50ct	300450449078	AFA176
1/15/2010	Extra Strength TYLENOL CAPLET 50ct	300450449078	AFA325
1/15/2010	Extra Strength TYLENOL CAPLET 50ct	300450449078	AHA072
1/15/2010	Extra Strength TYLENOL CAPLET 50ct	300450449078	AJA021
1/15/2010	Extra Strengh TYLENOL CAPLET 100ct	300450449092	AMA008
1/15/2010	Extra Strengh TYLENOL CAPLET 100ct	300450449092	SSA013
1/15/2010	Extra Strengh TYLENOL CAPLET 100ct	300450449092	SSA150
1/15/2010	Extra Strength TYLENOL CAPLET 150ct	300450449238	AAA419
1/15/2010	Extra Strength TYLENOL CAPLET 150ct	300450449238	SEA199
1/15/2010	Extra Strength TYLENOL CAPLET 150ct	300450449238	SPA007
1/15/2010	Extra Strength TYLENOL CAPLET 150+50ct	300450449467	SFA071
1/15/2010	MOTRIN IB TABLET 24ct	300450463029	ABA003
1/15/2010	MOTRIN IB TABLET 24ct	300450463029	ADA258
1/15/2010	MOTRIN IB TABLET 24ct	300450463029	AFA309
1/15/2010	MOTRIN IB TABLET 24ct	300450463029	AJA055
1/15/2010	MOTRIN IB TABLET 50ct	300450463036	ABA004
1/15/2010	MOTRIN IB TABLET 50ct	300450463036	ABA152
1/15/2010	MOTRIN IB TABLET 50ct	300450463036	AFA228
1/15/2010	MOTRIN IB TABLET 50ct	300450463036	AHA024
1/15/2010	MOTRIN IB TABLET 50ct	300450463036	AJA007
1/15/2010	MOTRIN IB TABLET 50ct	300450463036	AJA243
1/15/2010	MOTRIN IB TABLET 100ct	300450463043	AEA078
1/15/2010	MOTRIN IB TABLET 100ct	300450463043	AEA261
1/15/2010	MOTRIN IB TABLET 100ct	300450463043	AFA241
1/15/2010	MOTRIN IB TABLET 100+25ct	300450463296	AFA017
1/15/2010	MOTRIN IB TABLET 100+25ct	300450463296	AJA168
1/15/2010	MOTRIN IB TABLET 100+50ct	300450463753	ALA109
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	ABA019
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	ACA469
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	ADA245
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	AEA260
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	AFA015
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	AJA049
1/15/2010	MOTRIN IB CAPLET 100ct	300450481016	AJA186
1/15/2010	MOTRIN IB CAPLET 50ct	300450481023	ABA153
1/15/2010	MOTRIN IB CAPLET 50ct	300450481023	ABA541
1/15/2010	MOTRIN IB CAPLET 50ct	300450481023	ADA173
1/15/2010	MOTRIN IB CAPLET 50ct	300450481023	AHA025
1/15/2010	MOTRIN IB CAPLET 24ct	300450481030	AAA435
1/15/2010	MOTRIN IB CAPLET 24ct	300450481030	ABA369
1/15/2010	MOTRIN IB CAPLET 24ct	300450481030	ADA174
1/15/2010	MOTRIN IB CAPLET 24ct	300450481030	AHA026
1/15/2010	MOTRIN IB CAPLET 24ct	300450481030	AJA006
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	ACA442
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	ACA759
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	ADA018
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	ADA419
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	AFA098
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	AFA112
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	AHA034
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	AHA068
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	ALA254

Recall Date	Product Name	UPC	Lot
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	ALA359
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	AMA177
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	AMA350
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	APA217
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SEA208
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SFA184
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SFA259
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SHA107
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SJA131
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SLA049
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SLA162
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SMA013
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SMA082
1/15/2010	MOTRIN IB CAPLET 300ct WAREHOUSE CLUB	300450481375	SSA157
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24526
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24544
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24591
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24604
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24634
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24687
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24762
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24794
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24795
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24818
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24864
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24905
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24915
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24935
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24939
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	24977
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	25013
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	25044
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	25980
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	25996
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26051
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26085
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26134
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26192
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26241
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26335
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26423
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26455
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26508
1/15/2010	MOTRIN IB CAPLET 225ct	300450481627	26533
1/15/2010	MOTRIN IB CAPLET 24+6ct	300450481641	ADA246
1/15/2010	MOTRIN IB CAPLET 100+50ct	300450481757	ABA538
1/15/2010	MOTRIN IB CAPLET 100+50ct	300450481757	AJA023
1/15/2010	MOTRIN IB CAPLET 100+50ct	300450481757	AJA120
1/15/2010	MOTRIN IB CAPLET 100+25ct	300450481955	ADA287
1/15/2010	MOTRIN IB CAPLET 100+25ct	300450481955	AFA016
1/15/2010	Extra Strength TYLENOL PM CAPLET 100ct	300450482105	AJA174
1/15/2010	Extra Strength TYLENOL PM CAPLET 100ct	300450482105	ALA250
1/15/2010	Extra Strength TYLENOL PM CAPLET 100+20ct	300450482136	ALA251
1/15/2010	Extra Strength TYLENOL PM CAPLET 150ct	300450482150	SEA188
1/15/2010	Extra Strength TYLENOL PM CAPLET 24ct	300450482242	ABA021
1/15/2010	Extra Strength TYLENOL PM CAPLET 24ct	300450482242	ABA368
1/15/2010	Extra Strength TYLENOL PM CAPLET 24ct	300450482242	AJA025
1/15/2010	Extra Strength TYLENOL PM CAPLET 24ct	300450482242	AJA026
1/15/2010	Extra Strength TYLENOL PM CAPLET 24+12ct	300450482310	AJA027
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ABA415
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ACA033
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ACA440
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ACA441
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ADA179
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ADA418

Recall Date	Product Name	UPC	Lot
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AEA073
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AFA278
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AFA319
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AHA067
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AJA181
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	ALA255
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AMA053
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AMA176
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	AMA349
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	APA010
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	APA216
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SFA084
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SHA044
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SHA157
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SHA230
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SJA026
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SLA050
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SLA272
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SMA081
1/15/2010	Extra Strength TYLENOL PM CAPLET 225ct CLUB	300450482358	SSA158
1/15/2010	Extra Strength TYLENOL PM CAPLET 50ct	300450482501	AFA005
1/15/2010	Extra Strength TYLENOL PM CAPLET 50ct	300450482501	AFA280
1/15/2010	Extra Strength TYLENOL PM CAPLET 50ct	300450482501	AFA289
1/15/2010	Extra Strength TYLENOL PM CAPLET 50ct	300450482501	AFA357
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 150ct	300450488152	ASA015
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 100+20ct	300450488176	ALA253
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 100+20ct	300450488176	AMA015
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	09AMC008
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AAA049
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AAA360
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	ADA022
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	ADA178
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	ADA272
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	ADA482
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AEA194
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AFA010
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AFA292
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AHA035
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AHA089
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	AJA167
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	ALA095
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	ALA096
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SFA296
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SHA039
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SHA234
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SLA270
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SMA236
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SPA037
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SPA357
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SSA019
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SSA030
1/15/2010	Extra Strength TYLENOL RAPID RLS GC 290ct-NASCAR	300450488213	SSA054
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 24ct	300450488244	ABA020
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 24ct	300450488244	ABA371
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 24ct	300450488244	ADA280
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 24ct	300450488244	AHA082
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SEA191
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SEA192
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SFA025
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SFA026
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SFA136
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SLA052
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 290ct	300450488299	SLA198
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	ACA451
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AEA061

Recall Date	Product Name	UPC	Lot
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AEA244
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AFA103
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AFA240
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AHA046
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AHA080
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AJA040
1/15/2010	Extra Strength TYLENOL RAPID RELEASE GELCAP 50ct	300450488503	AJA041
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	ADM013
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	AFM024
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	AHM402
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	AJM345
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	ALM326
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	ALM456
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	AMM381
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	APM306
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct ORANGE	300450494245	APM421
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	ABA148
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	ABA266
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	ABA373
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	ACA432
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	AFA101
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	AHA070
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	AJA009
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	ALA099
1/15/2010	Regular Strength TYLENOL TABLET 100ct	300450496607	AMA018
1/15/2010	Junior Strength MOTRIN IB CAPLET 24ct	300450498243	AJM322
1/15/2010	Junior Strength MOTRIN IB CAPLET 24ct	300450498243	APM348
1/15/2010	Extra Strength TYLENOL TABLET 60ct	300450499684	AEA243
1/15/2010	CHILDREN TYLENOL GRAPE MELTAWAYS 30ct	300450518309	AHA023
1/15/2010	CHILDREN TYLENOL GRAPE MELTAWAYS 30ct	300450518309	AHA057
1/15/2010	CHILDREN Tylenol BUBBLEGUM MELTAWAYS 30ct	300450519306	AHA069
1/15/2010	CHILDREN Tylenol BUBBLEGUM MELTAWAYS 30ct	300450519306	SPA022
1/15/2010	TYLENOL ARTHRITIS CAPLET 150ct	300450838155	09GMC101
1/15/2010	TYLENOL ARTHRITIS CAPLET 150ct	300450838155	ASA065
1/15/2010	TYLENOL ARTHRITIS CAPLET 150ct	300450838155	ASA304
1/15/2010	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09XMC114
1/15/2010	Tylenol Arthritis Pain Caplet 100ct EZ-Open Cap	300450838216	09XMC116
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AEA180
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AHA076
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AHA077
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AJA019
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AJA116
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AJA117
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	ALA029
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AMA025
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	AMA270
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	APA011
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	APA214
1/15/2010	TYLENOL ARTHRITIS CAPLET 290ct	300450838292	APA266
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	07BMC009
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	07EMC027
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	09EMC073
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	09HMC108
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	ASA088
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	ASA119
1/15/2010	TYLENOL ARTHRITIS PAIN ER CPLT 225ct	300450838377	ASA293
1/15/2010	TYLENOL ARTHRITIS CAPLET 50ct	300450838506	08KMC123
1/15/2010	TYLENOL ARTHRITIS CAPLET 50ct	300450838506	09DMC066
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	ADM015
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	ADM016
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	AFM014
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	AFM352
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	AJM319
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	AJM364
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	ALM387

Recall Date	Product Name	UPC	Lot
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	AMM436
1/15/2010	SIMPLY SLEEP MINI CAPLET 100ct	300450843104	AMM438
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	ADM006
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	ADM052
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	AFM016
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	AFM350
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	AHM420
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	AJM346
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	ALM344
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	ALM399
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	AMM379
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	APM303
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	APM418
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	APM429
1/15/2010	Junior Strength MOTRIN CHEWABLE TABLET 24ct GRAPE	300450909244	SLM084
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AAA011
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AAA083
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AAA399
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ABA397
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ACA439
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ADA086
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ADA180
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AEA197
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AEA250
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AFA053
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AFA224
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AFA293
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AJA043
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AJA114
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ALA105
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ALA159
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	ALA273
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	AMA178
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	APA054
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SJA113
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SJA114
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SJA115
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SJA116
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SJA259
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SLA149
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SMA032
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SMA222
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SMA248
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SPA024
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SPA128
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SPA161
1/15/2010	Extra Strength ROLAIDS FRESHMINT TABLET 100ct	312547650212	SSA351
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AAA086
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	ABA262
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	ACA256
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	ADA028
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	ADA082
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AEA195
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AFA234
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AJA017
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AJA018
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AJA180
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	ALA026
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AMA051
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	AMA208
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	APA152
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	SMA031
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	SMA099
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	SMA100
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	SMA101

Recall Date	Product Name	UPC	Lot
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	SSA331
1/15/2010	Extra Strength ROLAIDS FRUIT TABLET 100ct	312547650243	SSA332
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AAA009
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AAA202
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AAA232
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	ABA141
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	ABA268
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	ABA416
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	ABA554
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	ACA567
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	ADA268
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AEA072
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AFA009
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AFA171
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AJA178
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AMA024
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AMA267
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	AMA268
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	APA041
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SJA110
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SJA111
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SJA112
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SJA148
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SLA084
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SLA217
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SLA367
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SLA370
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SMA123
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SMA124
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SMA332
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SPA129
1/15/2010	Original ROLAIDS PEPPERMINT TABLET 150ct	312547651158	SSA439
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	ACA013
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	AEA057
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	AFA317
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	AJA016
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	AMA165
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	APA009
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	SLA087
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	SPA036
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	SSA334
1/15/2010	Original ROLAIDS CHERRY TABLET 150ct	312547652421	SSA438
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	AAA359
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	SHA016
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	SHA017
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	SHA018
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	SJA204
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	SLA151
1/15/2010	Extra Strength ROLAIDS TROPICAL PUNCH TABLET 100ct	312547654234	SSA175
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ABA009
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ABA010
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ABA011
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ABA417
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ABA620
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ACA438
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ALA256
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	APA042
1/15/2010	Multi-Symptom ROLAIDS BERRY TABLET 100ct	312547654579	ASA012
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	24862
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	24881
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	24901
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	24970
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	25994
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26054
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26213

Recall Date	Product Name	UPC	Lot
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26305
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26356
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26377
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26515
1/15/2010	Extra Strength TYLENOL CAPLET 50ct HOSPITAL	350580451502	26541
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	24777
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	24900
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	24971
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	25971
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	26019
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	26133
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	26271
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	26422
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	26482
1/15/2010	Regular Strength TYLENOL CAPLET 50ct HOSPITAL	350580501504	26521
2/17/2010	TYLENOL ES Daytime/PM Nighttime CAPLET 50+24 Value Pack	300450527103	All lots within expiry on 2/17/10
2/17/2010	Motrin IB 24 count caplets	300450481030	SDA149
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	AAM099
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SEM099
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SFM003
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SJM088
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SMM009
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SMM082
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SSM019
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape	300450122018	SSM080
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SDM079
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SDM080
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SDM081
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SDM100
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SDM101
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SEM047
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SJM015
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SJM089
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Grape (Dual)	300450122100	SJM162
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	AAM004
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	AAM021
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	ABM030
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SDM124
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SEM051
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SFM027
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SHM018
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SJM130
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SLM105
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SMM059
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SMM072
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SMM152
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape	300450122155	SSM040
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	AAM085
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	AAM120
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SDM128
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SEM098
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SFM004
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SFM005
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SFM006
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SHM024
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SHM041
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SJM087
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SJM189
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SLM038
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SLM039
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SLM110
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SLM111
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SLM112
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SMM068
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SMM083

Recall Date	Product Name	UPC	Lot
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SPM038
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SPM065
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	SSM018
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Dye Free Cherry	300450167019	AAM005
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SDM097
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SDM129
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SDM130
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SDM131
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SEM046
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SHM042
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SHM061
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SJM057
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SJM157
3/26/2010	Conc. Tylenol Infants' Drops 1 OZ Dye Free Cherry (Dual)	300450167118	SMM008
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	AAM093
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SDM093
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SEM050
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SEM113
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SHM032
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SJM049
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SLM052
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SLM104
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SMM043
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SMM073
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SPM009
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SPM059
3/26/2010	Concentrated Tylenol Infants' Drop 1/2 OZ Cherry	300450186157	SSM061
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Cherry	300450186300	SJM137
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Cherry	300450186300	SLM113
3/26/2010	Concentrated Tylenol Infants' Drops 1 OZ Cherry	300450186300	SPM039
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SDM010
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SDM011
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SDM037
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SDM132
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM048
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM079
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM080
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM101
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM120
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM121
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM122
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SEM123
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SHM033
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SJM056
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SJM090
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SLM058
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SLM059
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SLM060
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SMM010
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SMM011
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SMM066
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SMM067
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SSM048
3/26/2010	Concentrated Motrin Infants' Drops 1 OZ Dye Free Berry	300450198013	SSM067
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SDM098
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SDM099
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SEM049
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SEM100
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SFM007
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SFM008
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SFM009
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SHM062
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SJM055
3/26/2010	Conc. Motrin Infants' Drops 1 OZ Dye Free Berry (Dual)	300450198112	SJM158
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Dye Free Berry	300450198150	SCM079

Recall Date	Product Name	UPC	Lot
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Dye Free Berry	300450198150	SEM072
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Dye Free Berry	300450198150	SJM081
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Dye Free Berry	300450198150	SMM004
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Dye Free Berry	300450198150	SMM166
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Dye Free Berry	300450198150	SSM072
3/26/2010	Children's Zyrtec Allergy Syrup 1/2 OZ Bubble Gum	300450205155	SMM153
3/26/2010	Children's Zyrtec Allergy Syrup 1/2 OZ Bubble Gum	300450205155	SPM010
3/26/2010	Children's Zyrtec Allergy Syrup 1/2 OZ Bubble Gum	300450205155	SPC019
3/26/2010	Children's Zyrtec Allergy Syrup 1/2 OZ Bubble Gum	300450205155	SPC022
3/26/2010	Children's Zyrtec Allergy Syrup 1/2 OZ Bubble Gum	300450205155	SPC023
3/26/2010	Children's Zyrtec Allergy Syrup 1/2 OZ Bubble Gum	300450205155	SPM010A
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	AAM118
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	AAM119
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SDM031
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SDM069
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SDM092
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SEM071
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SJM007
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SLM053
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SMM003
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SMM044
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SMM167
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SSM012
3/26/2010	Concentrated Motrin Infants' Drops 1/2 OZ Berry	300450524157	SSM062
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	AAM062
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	SDM123
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	SJM131
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	SMM005
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	SPM008
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	SSM003
3/26/2010	Concentrated Tylenol Infants' Drops 1/2 OZ Grape Hospital	350580144183	SSM034
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2058J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2748J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2808J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2818J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	3088J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	3098J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	3438J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	3458J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0129J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0149J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0709J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0719J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0729J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0759J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0969J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0979J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	0989J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2059J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2089J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2109J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2119J
3/26/2010	JOHNSON'S® Baby Relief Kit	381370026426	2449J
3/26/2010	CH TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	ALM336
3/26/2010	CH TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	ALM404
3/26/2010	CH TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	AMM312
3/26/2010	CH TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	ASM317
3/26/2010	CH TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	ASM328
3/26/2010	CH TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	ASM396
3/26/2010	CH ZYRTEC SUGAR FREE DYE FREE SYRUP 4 OZ GRAPE	300450209047	ASM308
3/26/2010	CH ZYRTEC SUGAR FREE DYE FREE SYRUP 4 OZ GRAPE	300450209047	ASM388
3/26/2010	CH ZYRTEC SUGAR FREE DYE FREE SYRUP 4 OZ GRAPE	300450209047	ASM433
3/26/2010	CH TYLENOL+COLD/STUFFY NOSE DYE FREE SUSP 4OZ GRAPE	300450253040	ALM409
3/26/2010	CH TYLENOL+MULTI-SYMP COLD DYE FREE SUSP 4OZ GRAPE	300450255044	ALM353
3/26/2010	CH TYLENOL+MULTI-SYMP COLD DYE FREE SUSP 4OZ GRAPE	300450255044	AMM309

Recall Date	Product Name	UPC	Lot
3/26/2010	CH TYLENOL+MULTI-SYMP COLD DYE FREE SUSP 4OZ GRAPE	300450255044	AMM344
3/26/2010	CH TYLENOL+MULTI-SYMP COLD DYE FREE SUSP 4OZ GRAPE	300450255044	ASM392
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ALM302
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ALM351
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ALM411
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ALM412
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	AMM346
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ASM315
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ASM316
3/26/2010	CHILDREN'S TYLENOL SUSP 4OZ GRAPE	300450296047	ASM329
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	AJM405
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	AJM417
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	ALM306
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	ALM315
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	ALM339
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	ALM340
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	AMM313
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	AMM347
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	APM401
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	APM402
3/26/2010	CHILDREN'S TYLENOL+FLU SUSP 4OZ BUBBLE GUM	300450386052	APM403
3/26/2010	CHILDREN'S TYLENOL PLUS COLD SUSP 4OZ GRAPE	300450387059	ALM335
3/26/2010	CHILDREN'S TYLENOL PLUS COLD SUSP 4OZ GRAPE	300450387059	ASM369
3/26/2010	CHILDREN'S TYLENOL PLUS COLD SUSP 4OZ GRAPE	300450387059	ASM395
3/26/2010	CHILDREN'S TYLENOL+COLD/ALLERGY SUSP 4OZ BUBBLE GUM	300450390059	AHM453
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM303
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM304
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM305
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM354
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM356
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM410
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM419
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ALM420
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	APM406
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	APM407
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ASM307
3/26/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4OZ GRAPE	300450391056	ASM340
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE2425
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE2425A
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE2426
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE2427
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE5608
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE6160
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JE6160A
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JG5286
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JG5286A
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JG5286B
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JG7349
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JJ6419
3/29/2010	Zyrtec Itchy Eye Drops 5mL bottle	300450208057	JJ6422
4/30/2010	CONCENTRATED TYLENOL INFANTS' DROPS 1 OZ GRAPE	300450122018	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED TYLENOL INFANTS' DROPS 1 OZ GRAPE (DUAL)	300450122100	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED TYLENOL INFANTS' DROPS 1/2 OZ GRAPE	300450122155	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED TYLENOL INFANTS' DROPS 1/4 OZ GRAPE SPL	300450122407	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSPENSION 1 OZ CHERRY SPL	300450123015	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSPENSION 2 OZ CHERRY	300450123022	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSPENSION 4 OZ CHERRY	300450123046	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL DYE FREE SUSP 4 OZ CHERRY	300450166043	All lots within expiry on 4/30/10
4/30/2010	CONC. TYLENOL INFANTS' DROPS DYE FREE 1 OZ CHERRY	300450167019	All lots within expiry on 4/30/10
4/30/2010	CONC. TYLENOL INFANTS' DROPS DYE FREE 1 OZ CHERRY (DUAL)	300450167118	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSP DYE FREE 4 OZ BERRY	300450184047	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED TYLENOL INFANTS' DROPS 1/2 OZ CHERRY	300450186157	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED TYLENOL INFANTS' DROPS 1 OZ CHERRY	300450186300	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 1 OZ BERRY SAMPLE	300450192011	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 2 OZ BERRY	300450192028	All lots within expiry on 4/30/10

Recall Date	Product Name	UPC	Lot
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 4 OZ BERRY	300450192042	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED MOTRIN INFANTS' DROPS DYE FREE 1 OZ BERRY	300450198013	All lots within expiry on 4/30/10
4/30/2010	CONC. MOTRIN INFANT'S DROPS DYE FREE 1 OZ BERRY (DUAL)	300450198112	All lots within expiry on 4/30/10
4/30/2010	CONC. MOTRIN INFANTS' DROPS DYE FREE 1/2 OZ BERRY	300450198150	All lots within expiry on 4/30/10
4/30/2010	CHLD'S ZYRTEC SUGAR FREE DYE FREE SYRUP 4 OZ BUBBLE GUM	300450205049	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S ZYRTEC SUGAR FREE DYE FREE 1/2 OZ BUBBLE GUM	300450205155	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S ZYRTEC SUGAR FREE DYE FREE SYRUP 4 OZ GRAPE	300450209047	All lots within expiry on 4/30/10
4/30/2010	CHLD'S ZYRTEC SUGAR FREE DYE FREE PERFECT MEASURE GRAPE	300450209108	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S ZYRTEC SUGAR FREE DYE FREE 1/2 OZ GRAPE SPL	300450209153	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 4 OZ TROPICAL PUNCH	300450215048	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COUGH/SORE THROAT SUSP 4 OZ CHERRY	300450247049	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COUGH/SORE THROAT SUSP 4 OZ CHERRY	300450247056	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COUGH/RUNNY NOSE SUSP 4 OZ CHERRY	300450249043	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COUGH/RUNNY NOSE SUSP 4 OZ CHERRY	300450249050	All lots within expiry on 4/30/10
4/30/2010	CHLD'S TYLENOL+COLD/STUFFY NOSE DYE FREE SUSP 4 OZ GRP	300450253040	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COLD/COUGH DYE FREE SUSP 4 OZ GRP	300450254047	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+MULTI-SYMP COLD DYE FREE 4 OZ GRP	300450255044	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSPENSION 4 OZ GRAPE	300450296047	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+FLU SUSP 4 OZ BUBBLE GUM	300450386045	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+FLU SUSP 4 OZ BUBBLE GUM	300450386052	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COLD SUSP 4 OZ GRAPE	300450387042	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COLD SUSP 4 OZ GRAPE	300450387059	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+COLD/ALLERGY SUSP 4 OZ BUBBLE GUM	300450390059	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4 OZ GRP	300450391049	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL+MULTI-SYMPTOM COLD SUSP 4 OZ GRP	300450391056	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSPENSION 4 OZ BUBBLE GUM	300450407047	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSPENSION 4 OZ STRAWBERRY	300450493040	All lots within expiry on 4/30/10
4/30/2010	CONCENTRATED MOTRIN INFANTS' DROPS 1/2 OZ BERRY	300450524157	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 1 OZ GRAPE SAMPLE	300450603012	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 4 OZ GRAPE	300450603043	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 1 OZ BUBBLE GUM SAMPLE	300450604019	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 4 OZ BUBBLE GUM	300450604040	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN COLD SUSPENSION 4 OZ BERRY	300450902047	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S TYLENOL SUSP 4 OZ CHERRY HOSPITAL	350580123034	All lots within expiry on 4/30/10
4/30/2010	CONC. TYLENOL INFANTS' DROPS 1/2 OZ GRAPE HOSP	350580144183	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S BENADRYL ALLERGY DYE FREE 4 OZ BUBBLE GUM	350580535042	All lots within expiry on 4/30/10
4/30/2010	CHILDREN'S MOTRIN SUSPENSION 4 OZ BERRY HOSPITAL	350580601501	All lots within expiry on 4/30/10
4/30/2010	JOHNSON'S® Baby Relief Kit	381370026426	All lots within expiry on 4/30/10
4/30/2010	JOHNSON'S® Baby Relief Kit	381371021086	All lots within expiry on 4/30/10
4/30/2010	JOHNSON'S® Baby Relief Kit	381371021086	All lots within expiry on 4/30/10
4/30/2010	CONC. TYLENOL INFANTS' DROPS 1 OZ + 1/2 OZ GRAPE PK	300450122025	All lots within expiry on 4/30/10
4/30/2010	CONC. MOTRIN INFANTS' DROPS 1 OZ + 1/2 OZ BERRY PK	300450198051	All lots within expiry on 4/30/10
4/30/2010	CHLD'S ZYRTEC SUGAR FREE DYE FREE 2 X 4 OZ BUBBLE GUM	--	All lots within expiry on 4/30/10
6/15/2010	TYLENOL Extra Strength RAPID RELEASE GELCAP 50ct	300450488503	ASA202
6/15/2010	BENADRYL ALLERGY ULTRATAB 100ct	312547170338	ABA022
6/15/2010	BENADRYL ALLERGY ULTRATAB 100ct	312547170338	ABA264
6/15/2010	BENADRYL ALLERGY ULTRATAB 100ct	312547170338	ADA194
6/15/2010	BENADRYL ALLERGY ULTRATAB 100ct	312547170338	AJA008
7/8/2010	Extra Strength TYLENOL EZTAB 50ct	300450422507	ABA005
7/8/2010	Extra Strength TYLENOL CAPLET 50ct	300450444530	ABA168
7/8/2010	CHILDREN Tylenol BUBBLEGUM MELTAWAYS 30ct	300450519306	ABA544
7/8/2010	Extra Strength TYLENOL COOL CAPLET 24ct	300450444240	ABA566
7/8/2010	BENADRYL ALLERGY ULTRA TAB 100ct	312547170338	ABA567
7/8/2010	BENADRYL ALLERGY ULTRA TAB 100ct	312547170338	ABA574
7/8/2010	MOTRIN IB CAPLET Bonus Pack 50+25ct	300450481764	ACA002
7/8/2010	MOTRIN IB CAPLET 24ct	300450481030	ACA003
7/8/2010	TYLENOL PM RAPID RLS GELCAP 20ct	300450244208	ACA004
7/8/2010	TYLENOL PM CAPLET 24ct	300450482242	ACA005
7/8/2010	TYLENOL Extra Strength RAPID RELEASE GELCAP 24ct	300450488244	ACA024
7/8/2010	Extra Strength TYLENOL CAPLET Bonus Pack 24+12ct	300450444318	ACA025
7/8/2010	TYLENOL PM CAPLET 24ct	300450482242	ADA259
7/8/2010	TYLENOL ES Daytime/PM Nighttime CAPLET 50+24 Value Pack	300450527103	ADC002
7/8/2010	TYLENOL ES Daytime/PM Nighttime CAPLET 50+24 Value Pack	300450527103	AEC005
7/8/2010	Extra Strength TYLENOL CAPLET 50ct	300450449078	AFA018
7/8/2010	MOTRIN IB TABLET 100ct	300450463043	AFA060

Recall Date	Product Name	UPC	Lot
7/8/2010	TYLENOL PM GELTAB 50ct	300450176509	AFA100
7/8/2010	TYLENOL ES Daytime/PM Nighttime CAPLET 50+24 Value Pack	300450527103	AFC005
7/8/2010	TYLENOL Extra Strength RAPID RELEASE GELCAP 225ct	300450488251	AJA119
7/8/2010	Extra Strength TYLENOL EZTAB 225ct	300450422378	ASA206
8/3/2010	Pepcid Complete Tropical Fruit 50 ct	716837246503	BEF062
8/3/2010	Pepcid AC 90 ct	716837872900	BFF010
10/18/2010	Tylenol 8 HOUR CAPLET 50ct	300450297518	BCM155
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ABC027
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ACC036
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ACC039
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ACC043
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	AHC095
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	AMC116
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ASC134
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ASC135
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	ASC136
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	BAC012
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	BAC019
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	BAC020
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	BCC033
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	BCC034
11/15/2010	Children's Benadryl Allergy FastMelt Cherry 18 ct	300450180186	SSC155
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ABC013
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ABC014
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ABC015
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ABC028
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ABC029
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ABC030
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ACC040
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ACC041
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ADC053
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AEC070
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AFC071
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AFC072
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AFC084
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AFC085
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AJC096
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AJC097
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AJC098
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AJC099
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AJC102
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AJC103
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ALC112
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ALC113
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ALC114
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AMC115
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	AMC117
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	ASC133
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	BAC001
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	BAC002
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	BAC003
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	BAC011
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	BCC035
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	BCC036
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	SSC156
11/15/2010	Children's Benadryl Allergy FastMelt Grape 18 ct	300450190185	SSC157
11/15/2010	Rolaids Extra Strength Softchews Cherry 36 ct	300450649362	0053AG2
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	AAM053
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	APM348
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	BDM227
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	SDM046
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	SHM001
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	SLM121
11/15/2010	Jr. Strength Motrin Caplet 24 ct	300450498243	SSM097
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	809518

Recall Date	Product Name	UPC	Lot
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	900009
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	901006
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	901658
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	902331
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	903117
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	903118
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	903230
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	904394
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	904395
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	905529
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	905530
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	BLEP
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	BLFA
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	BMBZ
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	CHFT
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	CKAT
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	CKDF
11/23/2010	Tylenol Cold Multi-Symptom Daytime Citrus Burst Liq.	300450257086	CKEG
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	003641
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	003642
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	003643
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	003644
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	005184
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	005661
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	005834
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	005835
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	005836
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	006145
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	006633
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	006634
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	006635
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	006636
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	809231
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	809232
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	809233
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	809515
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	809521
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	902336
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	903399
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	903903
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	904352
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	904397
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	905228
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	905528
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	906256
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	906257
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	906687
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	906688
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	906690
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	907211
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	907213
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	907214
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	907226
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	907916
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	907917
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	908253
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	908254
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	908255
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	005835A
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CCCB
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CFFE
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CFFF
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CFFG
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CGAM
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CGAN

Recall Date	Product Name	UPC	Lot
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CGAP
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CGBX
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CKFA
11/23/2010	Tylenol Cold Multi-Symptom Nighttime Cool Burst Liq.	300450269089	CKFB
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	004820
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	004821
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	004859
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005185
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005186
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005187
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005428
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005429
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005660
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	005793
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	809519
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	900007
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	902332
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	903113
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	903119
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	903120
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	903768
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	903769
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	904398
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	904399
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	905533
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	905534
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	905689
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	906254
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	906264
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	906265
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	907207
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	907209
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	907210
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	907918
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	907919
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	BMBU
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	BMDW
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	BMDX
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	BMER
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	CFFP
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	CGAB
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	CGAC
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	CGCH
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	CGCK
11/23/2010	Tylenol Cold Multi-Symptom Severe Day Cool Burst Liq.	300450521088	CGCL
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AAF075
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ABF005
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ABF033
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ABF068
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ACF008
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ACF054
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ADF063
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AEF024
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AHF004
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AHF016
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AHF051
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AJF026
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ALF030
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AMF016
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AMF046
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	AMF047
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	APF064
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	APF074
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	ASF041
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BAF028

Recall Date	Product Name	UPC	Lot
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BAF045
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BAF049
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BBF008
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BCF051
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BDF026
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BDF045
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BEF029
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BEF043
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BFF001
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BFF020
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BHF029
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BHF031
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BHF032
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BJF017
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BJF045
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BJF046
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BJF047
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BLF025
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BMF004
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	BMF023
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	SSF064
11/29/2010	RS MYLANTA LIQUID 12 OZ ORIGINAL	716837610120	SSF078
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	AAF071
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	AAF072
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	ADF048
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	ADF049
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	AFF016
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	AFF032
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	AJF038
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	AJF039
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	ASF056
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	BCF038
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	BDF046
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	BEF052
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	BFF003
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	BMF003
11/29/2010	RS MYLANTA LIQUID 5 OZ ORIGINAL	716837610557	SSF053
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	AAF022
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	ABF004
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	ABF067
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	ACF016
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	ADF011
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	ADF090
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	AEF051
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	AFF038
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	AHF003
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	AJF010
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	ALF050
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	APF028
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BAF023
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BCF010
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BCF071
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BCF086
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BDF056
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BEF054
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BFF019
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BFF034
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BFF035
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BFF042
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BHF003
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BJF005
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BJF030
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BMF005
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	BMF024
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	SPF066

Recall Date	Product Name	UPC	Lot
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	SSF017
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	SSF051
11/29/2010	MS MYLANTA LIQUID 12 OZ CHERRY	716837622123	SSF073
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	AAF091
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	ABF081
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	ACF039
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	ADF062
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	AEF030
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	AFF031
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	AHF015
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	ALF027
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	AMF033
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	APF063
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BAF046
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BCF035
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BDF030
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BEF028
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BEF056
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BFF018
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BHF004
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BJF018
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BJF040
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BJF041
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	BLF016
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	SPF067
11/29/2010	MS MYLANTA LIQUID 12 OZ MINT	716837624127	SSF016
11/29/2010	RS MYLANTA LIQUID 12 OZ MINT	716837629122	ADF026
11/29/2010	RS MYLANTA LIQUID 12 OZ MINT	716837629122	BCF037
11/29/2010	RS MYLANTA LIQUID 12 OZ MINT	716837629122	BHF028
11/29/2010	RS MYLANTA LIQUID 12 OZ MINT	716837629122	SSF006
11/29/2010	US MYLANTA LIQUID 12 OZ MINT	716837643128	AJF008
11/29/2010	US MYLANTA LIQUID 12 OZ MINT	716837643128	ASF017
11/29/2010	US MYLANTA LIQUID 12 OZ MINT	716837643128	BDF017
11/29/2010	US MYLANTA LIQUID 12 OZ MINT	716837643128	BDF017A
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	ABF078
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	ADF013
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	ADF093
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	AFF015
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	AHF043
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	AJF006
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	AJF006A
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	ALF004
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	AMF026
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	APF031
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	ASF055
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BBF014
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BBF014A
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BDF001
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BDF055
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BEF030
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BHF024
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BJF006
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BJF019
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	BLF002
11/29/2010	US MYLANTA LIQUID 12 OZ CHERRY	716837644125	SPF024
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AAF073
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AAF092
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	ACF007
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	ACF038
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	ACF059
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	ADF050
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AEF025
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AEF055
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AEF060
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AHF005

Recall Date	Product Name	UPC	Lot
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AHF044
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	AJF007
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	ALF049
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	APF076
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	ASF039
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BAF009
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BBF003
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BCF036
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BCF085
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BDF034
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BDF057
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BEF031
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BFF016
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BHF011
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BHF012
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BHF027
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BHF039
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BJF011
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BJF031
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BLF001
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BLF017
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BMF018
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	BMF025
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	SSF014
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	SSF062
11/29/2010	MS MYLANTA LIQUID 12 OZ ORIGINAL	716837652120	SSF075
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0089N11
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0089N11A
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0089N11B
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0369N11
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0369N21
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0559N28
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0689N12
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	0689N22
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1069N21A
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1079N11
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1209N22A
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1219N12
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1219N22
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1569N12
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1569N12A
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	1569N22
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	2229N11
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	2229N21
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	3068N12
11/29/2010	MYLANTA LIQUID 2 X 12OZ W/PNL CARD	716837652151	3588N21
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	AAF018
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	AAF023
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ABF034
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ABF066
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ACF021
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ACF027
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ADF024
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	AHF035
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	AHF037
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	AJF025
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ALF028
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	AMF039
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	ASF054
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BAF014
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BBF029
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BCF084
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BEF011
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BEF023
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BFF017

Recall Date	Product Name	UPC	Lot
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BHF006
11/29/2010	MS MYLANTA LIQUID 24 OZ ORIGINAL	716837652243	BJF037
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	ACF040
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	AEF029
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	AHF045
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	ALF051
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	ASF040
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	BBF015
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	BEF026
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	BHF001
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	BJF032
11/29/2010	MYLANTA SUPREME LIQUID 12 OZ CHERRY	716837825128	SPF068
11/29/2010	MYLANTA SUPREME LIQUID 24 OZ CHERRY	716837825241	AAF090
11/29/2010	MYLANTA SUPREME LIQUID 24 OZ CHERRY	716837825241	ADF023
11/29/2010	MYLANTA SUPREME LIQUID 24 OZ CHERRY	716837825241	AHF042
11/29/2010	MYLANTA SUPREME LIQUID 24 OZ CHERRY	716837825241	AMF040
11/29/2010	MYLANTA SUPREME LIQUID 24 OZ CHERRY	716837825241	BCF083
11/29/2010	MYLANTA SUPREME LIQUID 24 OZ CHERRY	716837825241	BHF038
11/29/2010	ALTERNAGEL LIQUID 12 OZ	716837860129	ADF012
11/29/2010	ALTERNAGEL LIQUID 12 OZ	716837860129	ASF057
11/29/2010	ALTERNAGEL LIQUID 12 OZ	716837860129	BLF006
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0015AG2
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0015AG3
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0050AG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0051AG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0053BG2
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0106BG2
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0107AG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0108AG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0108BG3
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0108CG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0129BG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0133AG1
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	0165BG2
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	9349AG2
12/9/2010	Rolaids ES Softchews Cherry 18 ct	300450649188	9350AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0012AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0013AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0014AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0015AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0015AG4
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0053AG2
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0053BG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0094AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0106AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0106BG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0108AG2
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0108BG2
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0139BG2
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0165BG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0191AG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	0191BG1
12/9/2010	Rolaids ES Softchews Cherry 36 ct	300450649362	9350AG2
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 6 ct	300450657060	0017B
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 6 ct	300450657060	0095A
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 6 ct	300450657060	0096B
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	0016AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	0059AG2
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	0059BG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	0059BG2
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	0060AG2
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	9351BG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 12 ct	300450657121	9352AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0016AG2
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0017AG1

Recall Date	Product Name	UPC	Lot
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0057BG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0058AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0059AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0059BG3
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0060AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0129AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0132AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	0205AG1
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	9352AG2
12/9/2010	Rolaids MS plus Anti-Gas Softchews Tropical Fruit 24 ct	300450657244	9352BG2
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 6 ct	312547065733	9005A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 6 ct	312547065733	9006A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 2 x 6 ct	312547065757	9022A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 2 x 6 ct	312547065757	9027A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 2 x 6 ct	312547065757	9118A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 2 x 6 ct	312547065757	9119A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 2 x 6 ct	312547065757	9195A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 2 x 6 ct	312547065757	9196A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 6 x 6 ct	312547065771	9166A
12/9/2010	Rolaids ES plus Gas Softchews Tropical Fruit 6 x 6 ct	312547065771	9167A
12/9/2010	Rolaids ES Softchews Cherry 6 ct	312547655200	0109A
12/9/2010	Rolaids ES Softchews Cherry 6 ct	312547655200	0114A
12/9/2010	Rolaids ES Softchews Cherry 6 ct	312547655200	0115A
12/9/2010	Rolaids ES Softchews Cherry 6 ct	312547655200	0134A
12/9/2010	Rolaids ES Softchews Cherry 6 ct	312547655200	0135A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9015A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9016A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9019A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9138A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9140A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9210A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9211A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9315A
12/9/2010	Rolaids ES Softchews Wild Cherry 6 ct	312547655200	9316A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9075A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9076A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9098A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9103A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9104A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9239A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9240A
12/9/2010	Rolaids ES Softchews Wild Cherry 3 x 6 ct	312547655255	9348A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9065A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9068A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9069A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9131A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9132A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9208A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9209A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9286A
12/9/2010	Rolaids ES Softchews Wild Cherrry 7 x 6 ct	312547655316	9287A
1/14/2011	BENADRYL ALLERGYCLD GELCAP 24	300450105240	ACC047
1/14/2011	BENADRYL ALLERGYCLD GELCAP 24	300450105240	ACC048
1/14/2011	BENADRYL ALLERGYCLD GELCAP 24	300450105240	ACC049
1/14/2011	BENADRYL ALLERGYCLD GELCAP 24	300450105240	ACC050
1/14/2011	BENADRYL ALLERGYCLD GELCAP 24	300450105240	ACC051
1/14/2011	BENADRYL ALLERGYCLD GELCAP 24	300450105240	ACC052
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AEC061
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AEC062
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AEC063
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AEC067
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AEC068
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AEC069
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AFC090
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AJC106

Recall Date	Product Name	UPC	Lot
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	ALC106
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AMC119
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AMC120
1/14/2011	BENADRYL ALLERGY plus CLD GELCAP 24	300450105240	AMC121
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AFC076
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AFC077
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AFC078
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AFC079
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AFC089
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AHC093
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AHC094
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AJC100
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AJC104
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	AJC105
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	ALC110
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	BAC021
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	BCC026
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	BCC027
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 24	300450107244	BCC028
1/14/2011	BENADRYL ALRGYSNS HEADACHE GELCP 48	300450107480	AJC101
1/14/2011	SUDAFED PE COLD/CGH DT/NT CAP 10+10	300450115201	AFC075
1/14/2011	SUDAFED PE COLD/CGH DT/NT CAP 10+10	300450115201	ALC109
1/14/2011	SUDAFED PE COLD/CGH DT/NT CAP 10+10	300450115201	APC130
1/14/2011	SUDAFED PE COLD/CGH DT/NT CAP 10+10	300450115201	BAC015
1/14/2011	MS BENADRYL SEV ALLRGY SNSHDACH CPLT 60	300450175601	ASM375
1/14/2011	MS BENADRYL SEV ALLRGY SNSHDACH CPLT 60	300450175601	BAM206
1/14/2011	MS BENADRYL SEV ALLRGY SNSHDACH CPLT 60	300450175601	BBM198
1/14/2011	TYLENOL CLD HDCGN CAP 2500X2 CLBRST	300450261021	GS07972
1/14/2011	TYLENOL CLD HDCGN SEVERE CPLT 24 CLBRST	300450261243	AFM359
1/14/2011	TYLENOL CLD HDCGN SEVERE CPLT 24 CLBRST	300450261243	AHM397
1/14/2011	TYLENOL CLD HDCGN SEVERE CPLT 24 CLBRST	300450261243	ALM328
1/14/2011	TYLENOL CLD HDCGN SEVERE CPLT 24 CLBRST	300450261243	ALM381
1/14/2011	TYLENOL CLD HDCGN SEVERE CPLT 24 CLBRST	300450261243	AMM377
1/14/2011	TYLENOL CLD HDCGN SEVERE CPLT 24 CLBRST	300450261243	AMM388
1/14/2011	TYL CLD HDCGN SEV CPLT 50X2 CLBRST	300450261502	GS07907
1/14/2011	TYL CLD HDCGN SEV CPLT 50X2 CLBRST	300450261502	GS07971
1/14/2011	TYL CLD HDCGN SEV CPLT 50X2 CLBRST	300450261502	GS08039
1/14/2011	TYL CLD HDCGN SEV CPLT 50X2 CLBRST	300450261502	GS08255
1/14/2011	TYLENOL SNS CG/PN CAP 2500X2 CLBRST	300450262028	GS07732
1/14/2011	TYLENOL SNS CG/PN CAP 2500X2 CLBRST	300450262028	GS07736
1/14/2011	TYLENOL SNS CG/PN CAP 2500X2 CLBRST	300450262028	GS07795
1/14/2011	TYLENOL SNS CG/PN CAP 2500X2 CLBRST	300450262028	GS07900
1/14/2011	TYLENOL SNS CG/PN CAP 2500X2 CLBRST	300450262028	GS07910
1/14/2011	TYLENOL CLD HDCGN SEV CPLT CLBRST 48 CLUB	300450261229	AFM359
1/14/2011	TYLENOL CLD HDCGN SEV CPLT CLBRST 48 CLUB	300450261229	AHM397
1/14/2011	TYLENOL SINUS PAIN/EXP CAPLET 24	300450262240	AFM030
1/14/2011	TYLENOL SINUS PAIN/EXP CAPLET 24	300450262240	AFM354
1/14/2011	TYLENOL SINUS PAIN/EXP CAPLET 24	300450262240	AHM395
1/14/2011	TYLENOL SINUS PAIN/EXP CAPLET 24	300450262240	ALM367
1/14/2011	TYLENOL SINUS PAIN/EXP CAPLET 24	300450262240	BBM213
1/14/2011	TYLENOL SINUS PAIN/EXP CAPLET 24	300450262240	BCM156
1/14/2011	TYLENOL SNS CG/PN SEV CAP 48 CLBRST	300450262486	AFM353
1/14/2011	TYLENOL SNS CG/PN SEV CAP 48 CLBRST	300450262486	AJM339
1/14/2011	TYLENOL SNS CG/PN SEV CAP 48 CLBRST	300450262486	ALM464
1/14/2011	TYLENOL SNS CG/PN SEV CAP 48 CLBRST	300450262486	APM422
1/14/2011	TYLENOL SNS CG/PN SEV CAP 48 CLBRST	300450262486	BBM177
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07679
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07688
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07737
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07789
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07790
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07909
1/14/2011	TYL SNS CG/PN SEV CPLT 50X2 CLBRST	300450262509	GS07954
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	ABM048
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	ACM059

Recall Date	Product Name	UPC	Lot
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	AHM323
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	AHM427
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	ALM383
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	AMM441
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	APM424
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	ASM385
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	BAM257
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	BAM290
1/14/2011	TYLENOL SNS CG/PN NT CPLT 24 CLBRST	300450264244	BCM132
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	AJF011
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	AJF055
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	APF018
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	BAF001
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	BAF019
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	BAF048
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	BCF058
1/14/2011	TYLENOL SNS CG/PN DT/NT CPLT 20 CLBRST	300450266200	BCF059
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	AHM370
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	AHM428
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	AJM325
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	ALM396
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	AMM369
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	AMM440
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	APM379
1/14/2011	TYLENOL CLD MLSYM SEV CAP 24 CLBRST	300450270245	BAM265
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	ACM046
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	ACM049
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	ACM101
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	AHM373
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	AJM359
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	ALM347
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	AMM380
1/14/2011	TYLENOL CLD MLSYM DT CPLT 24 CLBRST	300450271242	ASM303
1/14/2011	TYLENOL SNS/ALLRGY CPLT 2500X2 CLBRST	300450273024	GS07582
1/14/2011	TYLENOL SNS/ALLRGY CPLT 2500X2 CLBRST	300450273024	GS07670
1/14/2011	TYLENOL SNS/ALLRGY CPLT 2500X2 CLBRST	300450273024	GS08022
1/14/2011	TYLENOL ALLRGY MS CAPLET 12 CLBRST	300450273123	AJM360
1/14/2011	TYLENOL ALLRGY MS CAPLET 12 CLBRST	300450273123	BAM283
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	ACM016
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	ACM060
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	AEM006
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	AHM441
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	ASM305
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	BAM233
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	BAM286
1/14/2011	TYLENOL ALLERGY MS CAPLET 24 CLBRST	300450273246	BDM243
1/14/2011	TYLENOL ALLERGY MS CPLT 50X2 CLBRST	300450273505	GS07653
1/14/2011	TYLENOL ALLERGY MS CPLT 50X2 CLBRST	300450273505	GS07743
1/14/2011	TYLENOL ALLERGY MS CPLT 50X2 CLBRST	300450273505	GS08134
1/14/2011	TYLENOL ALLERGY MS CPLT 50X2 CLBRST	300450273505	GS08321
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AAM100
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AEM035
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AEM094
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AFM031
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AHM400
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AJM357
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	ALM459
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	AMM370
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	ASM459
1/14/2011	TYLENOL SNS CG/PN DT CPLT 24 CLBRST	300450275240	BCM152
1/14/2011	TYLENOL CLD HDCGN DT CPLT 24 CLBRST	300450277244	AAM116
1/14/2011	TYLENOL CLD HDCGN DT CPLT 24 CLBRST	300450277244	AJM341
1/14/2011	TYLENOL CLD HDCGN DT CPLT 24 CLBRST	300450277244	ALM461
1/14/2011	TYLENOL CLD HDCGN DT CPLT 24 CLBRST	300450277244	APM432
1/14/2011	TYLENOL CLD HDCGN NT CPLT 24 CLBRST	300450278241	AHM426

Recall Date	Product Name	UPC	Lot
1/14/2011	TYLENOL CLD HDCGN NT CPLT 24 CLBRST	300450278241	AMM384
1/14/2011	TYLENOL CLD HDCGN NT CPLT 24 CLBRST	300450278241	APM343
1/14/2011	TYLENOL CLD HDCGN NT CPLT 24 CLBRST	300450278241	ASM377
1/14/2011	TYLENOL CLD HDCGN DT/NT CPLT 20 CLBRST	300450282200	AHF021
1/14/2011	TYLENOL CLD HDCGN DT/NT CPLT 20 CLBRST	300450282200	APF042
1/14/2011	TYLENOL CLD HDCGN DT/NT CPLT 20 CLBRST	300450282200	ASF018
1/14/2011	TYLENOL CLD HDCGN DT/NT CPLT 20 CLBRST	300450282200	ASF028
1/14/2011	TYLENOL CLD HDCGN DT/NT CPLT 20 CLBRST	300450282200	ASF035
1/14/2011	TYLENOL ALLERGY MS NT CAP 12 CLBRST	300450283122	AJM362
1/14/2011	TYLENOL ALLERGY MS NT CAP 12 CLBRST	300450283122	BBM187
1/14/2011	TYLENOL ALLRGY MS NT CPLT 24 CLBRST	300450283245	APM344
1/14/2011	TYL ALRGY MS MLSYM/NT CAP 24 CLBRST	300450284242	ALF057
1/14/2011	TYL ALRGY MS MLSYM/NT CAP 24 CLBRST	300450284242	BDF014
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	08HMC067
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	08HMC068
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	08JMC100
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	08JMC106
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	08KMC135
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	09AMC015
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	09BMC033
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	09HMC106
1/14/2011	TYLENOL ARTHRITIS GELCAP 20	300450292209	ASM348
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	08GMC054
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	08GMC056
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	08HMC069
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	08JMC101
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	08JMC104
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	08JMC105
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09AMC011
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09BMC030
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09CMC044
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09DMC058
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09HMC103
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09KMC135
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09LMC139
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09XMC111
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	09XMC117
1/14/2011	TYLENOL ARTHRITIS GELCAP 40	300450292407	ASM349
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	AAM066
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	ACM012
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	ADM051
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	AEM059
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	AHM378
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	AJM334
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SCM025
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SCM061
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SEM006
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SJM069
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SJM072
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SLM094
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SMM091
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SMM126
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SMM140
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SPM078
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SSM049
1/14/2011	TYLENOL ARTHRITIS GELCAP 80	300450292803	SSM092
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07521
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07522
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07523
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07524
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07525
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07590
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H07730
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H08125
1/14/2011	TYLENOL 8 HOUR CAPLET 2X2500	300450297044	H08188

Recall Date	Product Name	UPC	Lot
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07521A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07523A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07524A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07525A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07590A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07590B
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07730A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H07730B
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H08125
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H08188A
1/14/2011	TYLENOL 8 HOUR CAPLET 3 X 2	300450297068	H08188B
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	ADM034
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SDM023
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SDM108
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SFM018
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SLM004
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SLM122
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SMM090
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SMM093
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SMM141
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SSM022
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SSM085
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297105	SSM086
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297112	ADM005
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297112	ADM073
1/14/2011	TYLENOL 8 HOUR CAPLET 100	300450297112	AEM052
1/14/2011	TYLENOL 8 HOUR CAPLET 150	300450297150	SHM003
1/14/2011	TYLENOL 8 HOUR CAPLET 150	300450297150	SMM142
1/14/2011	TYLENOL 8 HOUR CAPLET 100+10	300450297174	AAM065
1/14/2011	TYLENOL 8 HOUR CAPLET 100+10	300450297174	SJM108
1/14/2011	TYLENOL 8 HOUR CAPLET 100+10	300450297174	SLM066
1/14/2011	TYLENOL 8 HOUR CAPLET 100+10	300450297174	SPM101
1/14/2011	TYLENOL 8 HOUR CAPLET 100+10	300450297174	SSM089
1/14/2011	TYLENOL 8 HOUR CAPLET 150	300450297181	ADM014
1/14/2011	TYLENOL 8 HOUR CAPLET 150	300450297181	ADM033
1/14/2011	TYLENOL 8 HOUR CAPLET 150	300450297181	ADM074
1/14/2011	TYLENOL 8 HOUR CAPLET 150	300450297181	AEM034
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	AAM044
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	ABM003
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SCM055
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SDM050
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SEM005
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SEM104
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SFM015
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SFM047
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SJM070
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SJM119
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SLM064
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SLM123
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SMM143
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SMM144
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297242	SSM113
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297266	ACM070
1/14/2011	TYLENOL 8 HOUR CAPLET 24	300450297075	ACM070
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	ABM002
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	SDM025
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	SDM052
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	SEM004
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	SJM074
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	SMM125
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297501	SPM086
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297518	ABM069
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297518	ADM054
1/14/2011	TYLENOL 8 HOUR CAPLET 50	300450297518	AEM049
1/14/2011	TYLENOL 8 HOUR CAPLET 50 BOGO	300450297532	SDM025

Recall Date	Product Name	UPC	Lot
1/14/2011	TYLENOL 8 HOUR CAPLET 50 BOGO	300450297532	SDM052
1/14/2011	TYLENOL 8 HOUR CAPLET 50 BOGO	300450297532	SEM004
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	AEM106
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	AFM028
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	AHM437
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	AHM445
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	AJM303
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	AJM422
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	ALM319
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	ALM320
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	ALM384
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	ASM306
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	ASM353
1/14/2011	SUDAFED PE TRPL ACTN CAPLET 24	300450526243	BAM269
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07457
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07575
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07583
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07584
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07655
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07802
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07901
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS07921
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS08228
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS08234
1/14/2011	TYLENOL ARTHRITIS CAPLET 34X2	300450838025	GS08237
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	AEM032
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	AEM108
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	AFM358
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	AHM326
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	AHM401
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	ALM421
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	AMM359
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	ASM406
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	BAM256
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	BAM271
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	BCM134
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	BCM177
1/14/2011	BENADRYL SVR ALRGY/SNS/HEADACH CP20	312547175845	BDM237
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 10S	312547227308	AJM418
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 20S	312547227315	AJM350
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 20S	312547227315	AJM351
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 20S	312547227315	AJM363
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 20S	312547227315	AMM302
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 20S	312547227315	APM347
1/14/2011	SUDAFED PE COLD & COUGH CAPLET 20S	312547227315	ASM351
1/14/2011	SUDAFED PE NON-DRY SINUS CAPLET 24S	312547227322	ALM329
1/14/2011	SUDAFED PE NON-DRY SINUS CAPLET 24S	312547227322	ALM462
1/14/2011	SUDAFED PE NON-DRY SINUS CAPLET 24S	312547227322	BAM200
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	AEM075
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	AHM430
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	ALM392
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	AMM329
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	AMM425
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	ASM356
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 12S	312547227339	BBM200
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	AFM061
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	AHM429
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	AHM442
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	AMM358
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	AMM423
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	APM426
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	ASM453
1/14/2011	SUDAFED PE SEVERE COLD CAPLET 24S	312547227346	BCM136
1/14/2011	SUDAFED PE 5MG NIGHT/COLD CAP 20S	312547227360	ALM428
1/14/2011	SUDAFED PE 5MG NIGHT/COLD CAP 20S	312547227360	ASM355

Recall Date	Product Name	UPC	Lot
1/14/2011	SUDAFED PE 5MG NIGHT/COLD CAP 20S	312547227360	BAM262
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	ABM043
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	ACM041
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	ACM055
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	ACM061
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	AEM089
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	AHM371
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	AHM377
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	AJM349
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	AJM361
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	ALM460
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	APM385
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	APM423
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	BAM267
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	BCM138
1/14/2011	SUDAFED PE SINUS HEADACHE CAPLET24S	312547227384	BCM178
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET48S	312547227391	AEM088
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET48S	312547227391	ALM391
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET48S	312547227391	APM354
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET48S	312547227391	BAM266
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET48S	312547227391	BCM137
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	ABM043
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	ACM041
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	ACM055
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	ACM061
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	AEM089
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	AHM371
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	AHM377
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	AJM361
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	APM423
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	BAM267
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	BCM138
1/14/2011	SUDAFED PE SINUS/HEADACHE CAPLET72S CLUB	300450227157	BCM178
1/14/2011	SINUTAB MSWD CAP 24S	312547364751	AEM060
1/14/2011	SINUTAB MSWD CAP 24S	312547364751	AMM417
1/14/2011	SINUTAB MSWD CAP 24S	312547364751	BAM251
1/14/2011	SINUTAB MSWD CAP 24S	312547364751	BCM173
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090087
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090088
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090089
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090090
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090091
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090299
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090300
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090301
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090302
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090303
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090304
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090547
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 100 count	312547654579	V090548
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	0134TA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	9056TA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	9349TB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	9356TA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	9356TB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	9357TA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	9357TB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	V090097
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	V090098
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 10 count	312547654616	V090099
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0028PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0028PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0032PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0033PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0034PA

Recall Date	Product Name	UPC	Lot
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0078PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0078PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0079PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0079PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0079PC
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0080PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0080PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0081PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	0081PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9049PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9049PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9050PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9051PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9051PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9052PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9052PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9055PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9056PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9056PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9057PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9057PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9307PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9310PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9351PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9351PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9352PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9352PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9352PC
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9355PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9355PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9356PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9356PB
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	9357PA
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090092
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090093
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090094
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090095
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090096
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090294
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090295
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090296
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090297
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090298
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090549
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090550
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090551
1/14/2011	ROLAIDS® Multi-Symptom Tablet Berry 3 pack 30 count	312547654654	V090974
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1004651
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1004652
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1005870
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1005874
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1008467
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1008468
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1009532
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1010850
2/25/2011	Sudafed 24 Hr 10 ct	300819600270	1013065
3/29/2011	TYLENOL ARTHRITIS GELTABS 20 ct	300450292209	09BMC031
3/29/2011	TYLENOL ARTHRITIS GELTABS 20 ct	300450292209	09DMC064
3/29/2011	TYLENOL ARTHRITIS GELTABS 40 ct	300450292407	09AMC012
3/29/2011	TYLENOL ARTHRITIS GELTABS 40 ct	300450292407	09HMC104
3/29/2011	TYLENOL ARTHRITIS GELTABS 40 ct	300450292407	09JMC120
3/29/2011	BENADRYL ALLERGY PLUS SINUS HEADACHE KAPGELS 24 ct	300450107244	BAC009
3/29/2011	BENADRYL ALLERGY PLUS SINUS HEADACHE KAPGELS 48 ct	300450107480	BAC008
3/29/2011	SUDAFED PE COLD & COUGH CAPLET 10 ct	312547227308	APM346
3/29/2011	TYLENOL SINUS CONGESTION/PAIN Daytime/Nighttime 20 ct	300450266200	ASF026

Recall Date	Product Name	UPC	Lot
3/29/2011	TYLENOL 8 HOUR CAPLET 3 pouches of 2 ct	300450297068	BDC014
3/29/2011	Tylenol 8 HOUR CAPLET 150ct	300450297181	ADM074
6/28/2011	Tylenol Extra Strength Caplet 225 ct	300450444271	ABA619
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	AMA277
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	APA059
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	APA162
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	ASA025
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	APA237
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	ASA072
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	ASA208
8/15/2011	Tylenol Cold Multi-Symptom Nighttime RRG 24 ct	300450395245	BAA008
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 12+8 ct	300450396204	AMF034
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 12+8 ct	300450396204	BAF005
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 12+8 ct	300450396204	BAF027
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 12+8 ct	300450396204	BCF080
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 36+24 ct	300450396600	BBF001
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 36+24 ct	300450396600	BCF060
8/15/2011	Tylenol Cold Multi-Symptom RRG DAY/NIGHT 36+24 ct	300450396600	BCF079
12/21/2011	MOTRIN® IB 24 COUNT COATED TABLETS	300450463029	ADA069
12/21/2011	MOTRIN® IB 24 COUNT COATED TABLETS	300450463029	ALA168
12/21/2011	MOTRIN® IB 24 COUNT COATED TABLETS	300450463029	ALA244
12/21/2011	MOTRIN® IB 24 COUNT COATED TABLETS	300450463029	AMA286
12/21/2011	MOTRIN® IB 24 COUNT COATED TABLETS	300450463029	APA001
12/21/2011	MOTRIN® IB 24 COUNT COATED TABLETS	300450463029	ASA001
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ACA310
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ACA460
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ADA407
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	AEA262
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	AFA226
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	AJA170
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ALA037
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ALA163
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	AMA012
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	AMA331
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	AMA342
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	APA035
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ASA082
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ASA123
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	ASA285
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BDA238
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BDA260
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BDA383
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BEA065
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BEA148
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BEA269
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BEA277
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BFA064
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BFA144
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BFA244
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BHA078
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BHA147
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BHA167
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BHA198
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BJA164
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BJA221
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BMA144
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BMA215
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BMA271
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BSA022
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	BSA056
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CBA063
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CBA107
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CCA028
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CDA003
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CFA065

Recall Date	Product Name	UPC	Lot
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CFA100
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CHA012
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CHA044
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CHA066
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CHA080
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CMA028
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CMA035
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CMA057
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CMA102
12/21/2011	MOTRIN® IB 24 COUNT COATED CAPLETS	300450481030	CMA108
12/21/2011	MOTRIN® IB 24 +6 COUNT COATED CAPLETS	300450481641	ACA761
12/21/2011	MOTRIN® IB 24 +6 COUNT COATED CAPLETS	300450481641	ALA265

STATE OF VERMONT
WASHINGTON SUPERIOR COURT

IN RE: JPay Inc.	)	CIVIL DIVISION
	)	334-6-17 Wncv
	)	

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General Thomas J. Donovan, Jr. ("the Attorney General") and JPay, Inc. ("Respondent") hereby agree to this Assurance of Discontinuance ("Assurance") pursuant to 9 V.S.A. § 2459.

REGULATORY FRAMEWORK

1. Vermont's Consumer Protection Act prohibits "unfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce." 9 V.S.A. § 2453.

2. The Vermont Attorney General's Consumer Protection Rule 109.01 states that it shall be an unfair and deceptive trade act and practice in commerce under 9 V.S.A. § 2453 "for any person to solicit any other person to engage in any kind of a game of skill, contest, sweepstakes, give-away or other promotion which…requires any kind of entry fee, service charge, purchase or similar consideration in order to enter or to continue to remain eligible…" CP Rule 109.

BACKGROUND

3. Respondent JPay Inc. ("JPay") is a corporation incorporated under the laws of Delaware, with its mailing address at 12864 Biscayne Blvd., Suite 243, Miami, FL 33181. JPay provides payment, communication and media services for correctional agencies.

4. Respondent is registered with the Vermont Secretary of State to conduct business in Vermont.

5. At least as early as April 17, 2017, JPay solicited Vermont consumers to participate in its "JPay Day" promotion, scheduled for April 20, 2017.

6. The solicitations for these promotions advised consumers that for each eligible transaction they conducted on April 20, 2017, consumers would be given an entry into a drawing for a $1,000 prize.

7. Vermont consumers were solicited to participate in the JPay Day promotion through emails, posts on the JPay website, and posts on JPay's public Twitter and Facebook pages.

8. The promotion did not provide any way for a consumer to enter the contest without making a purchase from JPay.

9. The Attorney General alleges that the above conduct constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453 and CP Rule 109.

CONTESTS AND PRIZES

10. JPay shall comply with all provisions of Vermont and federal law, including the Vermont Consumer Protection Act, 9 V.S.A. chapter 63 and the Vermont Attorney General's Consumer Protection Rule 109 in all future solicitations it sends to Vermont consumers.

RESTITUTION

11. Within 30 days of signing this Assurance, JPay shall refund all service fees it charged to Vermont consumers for eligible transactions that took place on April 20, 2017, in an amount totaling $409.25.

12. JPay shall process the refunds by issuing automatic credits to the credit card or bank account used by the consumer for the transaction. For any transactions which JPay is unable to refund automatically, JPay shall mail checks or money orders payable to each consumer in the

amount of their refund. All checks or money orders shall be valid for no less than 60 days and shall state the length of validity on the face of the check or money order.

13. JPay shall send to all consumers receiving payment under this provision a notice explaining that the consumer is receiving a refund as a result of JPay not properly following all promotion requirements under Vermont law in connection with its JPay Day promotion conducted on April 20, 2017.

14. No later than 120 days after both Parties execute this Assurance, JPay shall mail the total of all uncashed and returned checks to James Layman, Assistant Attorney General, Office of the Vermont Attorney General, 109 State Street, Montpelier, VT 05609:

a. a single check payable to "Vermont State Treasurer," and indicating the company's federal tax identification number, of the total dollar amount of all refunds that were returned or, in the case of checks, that went uncashed, to be treated as unclaimed funds;

b. a list, in electronic Excel format on a compact disc or via electronic mail, of the consumers whose refunds were returned or, in the case of checks, were not cashed (which list shall set out the first and last names of the consumers in distinct fields or columns), and for each such consumer, the last known address and dollar amount due; and

c. the company's corporate address.

PENALTIES

15. JPay shall pay civil penalties of seven thousand three hundred eighty dollars ($7,380) to the State of Vermont by June 13, 2017. JPay shall make payment to the "State of

Vermont" and send payment to: James Layman, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

OTHER TERMS

16. JPay agrees that this Assurance shall be binding on JPay, and its successors and assigns.

17. Agreeing to the terms of this Assurance does not constitute an admission by JPay to a violation of any law, rule or regulation. Acceptance of this Assurance shall not be deemed approval by the Attorney General of any practices or procedures of JPay not required by this Assurance, and JPay shall make no representation to the contrary.

18. The Attorney General hereby releases and discharges any and all claims arising under the Consumer Protection Act, 9 V.S.A. chapter 63 and the Vermont Attorney General's Consumer Protection Rule 109 that it may have against JPay for the conduct described in the Background section during April 2017.

19. The Superior Court of the State of Vermont, Washington Unit, shall have jurisdiction over this Assurance and the parties hereto for the purpose of enabling the Attorney General to apply to this Court at any time for orders and directions as may be necessary or appropriate to enforce compliance with or to punish violations of this Assurance.

20. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondent to be in violation of this Assurance, the Attorney General may pursue any remedies available under 9 V.S.A. chapter 63.

SIGNATURE

In lieu of instituting an action or proceeding against JPay, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance. By signing below, Respondent voluntarily agrees with and submits to the terms of this Assurance.

DATED at Miramar, FL, this 26th day of May, 2017.

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 2nd day of June, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By:
James Layman
Assistant Attorney General

STATE OF VERMONT

SUPERIOR COURT
Washington Unit

CIVIL DIVISION
Docket No. 505-9-17Wncv

STATE OF VERMONT
Plaintiff

v.

LENOVO (UNITED STATES) INC.
Defendant

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the people of the State of Vermont by Thomas J. Donovan, Jr., Attorney General of the State of Vermont, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 *et seq.* (the "Consumer Protection Act"), alleging Defendant, Lenovo (United States) Inc. ("Defendant" or "Lenovo," as defined in Part III of this Final Judgment and Consent Decree below), committed violations of the Consumer Protection Act.

Plaintiff and Lenovo have agreed to the Court's entry of this Final Judgment and Consent Decree ("Final Judgment and Consent Decree") without trial or adjudication of any issue of fact or law or finding of wrongdoing or liability of any kind, and that Lenovo does not admit any violation of law or any wrongdoing. This Final Judgment and Consent Decree is for settlement purposes only, and it is the intent of the parties that, to the fullest extent permitted by law, neither the fact of, nor any provision contained in, this Final Judgment and Consent Decree, nor any action taken hereunder, shall constitute, be construed as, or be admissible in evidence as any admission of the validity of any claim or any fact alleged in any other pending or subsequently filed action or of any wrongdoing, fault, violation of law, or liability of any

kind on the part of Lenovo or admission by Lenovo of the validity or lack thereof of any claim, allegation, or defense asserted in any other action. Nothing in this Final Judgment and Consent Decree shall be construed to affect Lenovo's right to take legal or factual positions in defense of litigation or other legal proceedings to which Vermont is not a party.

I. PARTIES

A. Plaintiff is the State of Vermont, by Thomas J. Donovan, Jr., Attorney General of the State of Vermont ("Plaintiff"). Plaintiff is charged with, among other things, enforcement of the Consumer Protection Act.

B. Lenovo is a Delaware corporation with its principal place of business at 1009 Think Place, Morrisville, North Carolina 27560-9002.

II. FINDINGS

A. The Court has jurisdiction over the subject matter of the Complaint filed herein and, solely for the purposes of this matter, over the parties to this Final Judgment and Consent Decree. Jurisdiction is retained by this Court for the purpose of enabling Plaintiff to apply to this Court for such further orders and directions as may be necessary or appropriate for the construction, modification, or execution of this Final Judgment and Consent Decree, including the enforcement of compliance therewith and penalties for violation thereof.

B. At all times relevant to this matter, Lenovo was engaged in trade and commerce affecting consumers in the State of Vermont in that Lenovo manufactures personal computers that are sold in retail stores in the State of Vermont. Lenovo also maintains a website through which consumers can purchase Lenovo products and ship those products to consumers residing in the State of Vermont.

NOW THEREFORE, on the basis of these findings, and for the purpose of effecting this Final Judgment and Consent Decree, IT IS HEREBY ORDERED AND DECREED AS FOLLOWS:

III. DEFINITIONS

For purposes of this Final Judgment and Consent Decree, the following definitions apply:

A. "Affirmative Express Consent" means that:

i. Prior to the initial operation of any Covered Software, it shall be Clearly and Conspicuously disclosed, separate and apart from any "end user license agreement," "privacy policy," "terms of use" page or similar document, the following:

1. For any Covered Software that displays advertising,

a. The fact that the Covered Software will display advertisements, including any pop-up advertisements; and

b. The frequency and circumstances under which such advertisements are displayed to the consumer; and

2. For any Covered Software that transmits, or causes to be transmitted, Covered Information to a person or entity other than the consumer,

a. The fact that the software will transmit, or cause to be transmitted, the Covered Information to a person or entity other than the consumer;

b. The types of Covered Information that will be transmitted to a person or entity other than the consumer;

c. The types of Covered Information that the receiving person or entity will share with third parties, which does not include an entity with a common corporate ownership and branding of Defendant or the Software Provider, a Third Party Service Provider, or any person or entity otherwise excluded by the Proviso in Part IV.B of this Final Judgment and Consent Decree;

d. The identity or specific categories of such third parties; and

e. The purposes for sharing such Covered Information.

ii. At the time this disclosure is made, a Clear and Conspicuous mechanism shall be provided for a consumer to indicate assent to the operation of the Covered Software by taking affirmative action authorizing its operation.

B. "Application Software" means any computer program designed for and used by consumers (e.g., database programs, word processing programs, games, Internet browsers or browser add-ons) that Defendant preinstalls or causes to be preinstalled onto a Covered Product. Application Software does not include device drivers; system software designed to configure, optimize or maintain a computer; operating systems; software bundled, integrated or included with operating systems; or software otherwise provided to Defendant for preinstallation on a Covered Product by an operating system provider.

C. "Clear(ly) and Conspicuous(ly)" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by consumers, including in all of the following ways:

i. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the

communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("Triggering Representation") is made through only one means.

ii. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

iii. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for consumers to easily hear and understand it.

iv. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

v. On a product label, the disclosure must be presented on the principal display panel.

vi. The disclosure must use diction and syntax understandable to consumers and must appear in each language in which the Triggering Representation appears.

vii. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

viii. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

D. "Covered Information" means the following information from or about an individual consumer that is input into, stored on, accessed or transmitted through Application Software: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) login credentials and passwords; (e) a telephone number; (f) a Social Security number; (g) a driver's license or other government-issued identification number; (h) a financial institution account number; (i) credit or debit card information; (j) any portion of the content of a consumer's communications; (k) any portion of the content of a consumer's files (e.g., documents, photos or videos); and (l) precise geolocation information sufficient to identify a street name and name of a city or town.

E. "Covered Product" means any personal computer (i.e., desktop computers, laptops, laptops that convert into tablets or vice versa, and notebooks) that is manufactured by or on behalf of Defendant and is sold to U.S. consumers. Covered Products do not include servers and server peripherals, mobile handsets or smartphones, or tablets or similar devices that are sold without an integrated or detachable physical keyboard. Covered Products also do not include the actual personal computers specifically sold to enterprise customers with over 1,000 employees.

F. "Covered Software" means: (a) Application Software that injects advertisements into a consumer's Internet browsing session, including pop-up advertisements or (b) Application Software that transmits, or causes to be transmitted, Covered Information to a person or entity other than the consumer, except when

i. the Covered Information is used only in an aggregated and/or de-identified form that does not disclose, report, or otherwise share any individually identifiable information; or

ii. the Covered Information is transmitted or used solely for one or more of the following purposes:

1. being reasonably necessary for the software to perform a function or service that the consumer requests or otherwise interacts with;
2. authenticating the consumer;
3. configuring or setting up the software; or
4. assessing or analyzing the software's performance (e.g., to find or fix problems in the software, assess how consumers are using the software, or to make improvements to the software).

Covered Software does not include Internet browsers, antivirus software, parental control software, or other computer security software.

G. "Effective Date" of this Final Judgment and Consent Decree is the later of the date that the Court enters an Order, Judgment or Decree approving the terms of this document, or the effective date of the Order in the FTC Action.

H. "Executive Committee" refers to the following Attorneys General Offices: California, Connecticut, Illinois and Pennsylvania.

I. "Feature" means one or more of the following attributes of Covered Software: (a) the Covered Software's benefits, efficacy, or features; (b) the fact that it will display advertising, including pop-up advertisements; (c) the frequency and circumstances under which the Covered Software will display advertising; and (d) the fact of and extent to which the

Covered Software will transmit, or cause to be transmitted, Covered Information to a person or entity other than the consumer.

J. "FTC Action" means the Federal Trade Commission matter entitled In re Matter of Lenovo (United States) Inc., File No. 152 3134.

K. "Lenovo" or "Defendant" means Lenovo (United States) Inc. and its successors and assigns.

L. "Participating States" or "States" refers to the states and commonwealths listed in Exhibit A.

M. "Software Provider" means any person or entity other than Defendant that sells, leases, licenses, or otherwise provides Application Software.

N. "Third Party Service Provider" means any person or entity that is contractually required by Defendant or a Software Provider to: (a) use or receive Covered Information collected by or on behalf of Defendant or the Software Provider for and at the direction of Defendant or Software Provider, and for no other individual or entity; (b) not disclose the Covered Information, or any individually identifiable information derived from it, to any individual or entity other than Defendant or Software Provider; and (c) not use the Covered Information for any other purpose.

IV. INJUNCTIVE RELIEF

A. Prohibited Misleading Representations

It is ordered that Defendant, its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Final Judgment and Consent Decree, whether acting directly or indirectly, in connection with the advertising, promotion, offering for sale, sale, or distribution of Covered Software shall not

make a misrepresentation, in any manner, expressly or by implication, about any Feature of the Covered Software.

B. Affirmative Express Consent Provision

It is further ordered that, commencing no later than 120 days after the Effective Date of this Final Judgment and Consent Decree, Defendant, its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Final Judgment and Consent Decree, whether acting directly or indirectly, shall not preinstall or cause to be preinstalled any Covered Software unless Defendant or the Software Provider:

i. Will obtain the consumer's Affirmative Express Consent;

ii. Provides instructions for how the consumer may revoke consent to the Covered Software's operation, which can include uninstalling the Covered Software; and

iii. Provides a reasonable and effective means for consumers to opt out, disable or remove all of the Covered Software's operations, which can include uninstalling the Covered Software.

Provided, however, that Affirmative Express Consent will not be required if sharing the Covered Information is reasonably necessary to comply with applicable law, regulation or legal process.

C. Mandated Software Security Program

It is further ordered that Defendant must, no later than the Effective Date of this Final Judgment and Consent Decree, establish and implement, and thereafter maintain a comprehensive software security program that is reasonably designed to (1) address software

security risks related to the development and management of new and existing Application Software, and (2) protect the security, confidentiality, and integrity of Covered Information. The content, implementation and maintenance of the software security program must be fully documented in writing. The software security program must contain administrative, technical, and physical safeguards appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, the nature of the Application Software, the security policies and practices of the Software Provider, and the sensitivity of the Covered Information, including:

i. The designation of an employee or employees to coordinate and be responsible for the software security program;

ii. The identification of internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment must include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) Application Software design, including the processing, storage, transmission and disposal of Covered Information by the Application Software; and (3) the prevention, detection, and response to attacks, intrusions, or other vulnerabilities;

iii. The design and implementation of reasonable safeguards to control these risks, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

iv. The development and use of reasonable steps to select and retain software or service providers capable of maintaining security practices consistent with this Final Judgment and Consent Decree, and requiring software and service providers, by contract, to implement and maintain appropriate safeguards; and

v. The evaluation and adjustment of the software security program in light of the results of the testing and monitoring required by sub-provision iii above, any changes to Defendant's operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have an impact on the effectiveness of the software security program.

D. Software Security Assessments by a Third Party

It is further ordered that, in connection with compliance with the provision of this Final Judgment and Consent Decree titled Mandated Software Security Program, Defendant must obtain initial and biennial assessments ("Assessments"):

i. The Assessments must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with professional experience with secure Internet-accessible, consumer-grade devices; an individual qualified as a Certified Information Systems Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA) with

professional experience with secure Internet-accessible consumer-grade devices; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, as ordered in the FTC Action.

ii. The reporting period for the Assessments must cover: (1) the first 180 days after the Effective Date for the initial Assessment, and (2) each 2-year period thereafter for 20 years for the biennial Assessments.

iii. Each Assessment must:

1. Set forth the specific administrative, technical, and physical safeguards that Defendant has implemented and maintained during the reporting period;
2. Explain how such safeguards are appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, the nature of the Application Software, the security policies and practices of the Application Software provider and the sensitivity of the Covered Information;
3. Explain how the safeguards that have been implemented meet or exceed the protections required by the Provision of this Final Judgment and Consent Decree titled Mandated Software Security Program; and
4. Certify that the Mandated Software Security Program is operating with sufficient effectiveness to provide reasonable assurance that the security of the Application Software preinstalled on Covered

Products and the security, confidentiality, and integrity of Covered Information is protected, and that the Mandated Software Security Program has so operated throughout the reporting period.

iv. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies as set forth in Part IV of the Order in the FTC Action.

E. The obligations and other provisions set forth in this Section IV shall expire 20 years after the Effective Date of this Final Judgment and Consent Decree. Nothing in this paragraph should be construed or applied to excuse Lenovo from its obligations to comply with all applicable state and federal laws, regulations and rules.

V. COMPLIANCE MONITORING

Defendant is required to monitor its compliance with this Final Judgment and Consent Decree in the same manner as it is required to monitor its compliance with the Order in the FTC Action, all as detailed in Part VI of the Order in the FTC Action. Upon request by any Participating State, Lenovo shall provide a copy of any Assessment or other submission made to the FTC pursuant to the FTC Action within 10 days of the request.

VI. ACKNOWLEDGMENTS OF THE FINAL JUDGMENT AND CONSENT DECREE

For 5 years after the Effective Date of this Final Judgment and Consent Decree, Defendant must deliver a copy of this Final Judgment and Consent Decree to all individuals and entities listed in Part V of the Order in the FTC Action.

VII. PAYMENT TO THE STATES

Within 30 days of the Effective Date of this Final Judgment and Consent Decree, Lenovo shall pay the sum of Three Million Five Hundred Thousand Dollars ($3,500,000) to the

Participating States. Payment of Fifty-Two Thousand, Six Hundred Nineteen Dollars and Eighty-Four Cents ($52,619.84) shall be made to the "State of Vermont" and sent to: Ryan Kriger, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609. The money is to be allocated among the Attorneys General[1] of the Participating States as determined solely by the Executive Committee. Said payment shall be used by the Attorneys General for such purposes that may include, but are not limited to, civil penalties, attorneys' fees and other costs of investigation, or to be placed in, or applied to, the consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation, or local consumer aid fund or revolving fund used to defray costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the Attorneys General.

VIII. RELEASE

Following full payment of the amounts due under this Final Judgment and Consent Decree, the Vermont Attorney General shall release and discharge Lenovo and its affiliates, subsidiaries and divisions from all civil claims that the Vermont Attorney General could have brought under the Consumer Protection Act based on Lenovo's conduct alleged in the Complaint filed in this matter prior to the Effective Date of this Final Judgment and Consent Decree. Nothing contained in this paragraph shall be construed to limit the ability of the Vermont Attorney General to enforce the obligations that Lenovo has under this Final

[1] Hawaii is represented in this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity purposes, the entire group will be referred to as the "Attorneys General" and the designation as it pertains to Hawaii, shall refer to the Executive Director of the State of Hawaii's Office of Consumer Protection.

Judgment and Consent Decree. Further, nothing in this Final Judgment and Consent Decree shall be construed to create, waive, or limit any private right of action.

IX. GENERAL PROVISIONS

A. The Parties understand and agree that this Final Judgment and Consent Decree shall not be construed as an approval or a sanction by the Vermont Attorney General of Lenovo's business practices, nor shall Lenovo represent that this Final Judgment and Consent Decree constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Vermont Attorney General to take any action in response to any information submitted pursuant to this Final Judgment and Consent Decree shall not be construed as an approval, waiver, or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date, except as provided by the Release herein.

B. Nothing in this Final Judgment and Consent Decree shall be construed as relieving Lenovo of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Final Judgment and Consent Decree be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

C. Nothing contained in this Final Judgment and Consent Decree shall be construed to waive or limit any right of action by any consumer, person or entity, or by any local, state, federal or other governmental entity, except as provided by the Release herein.

D. Nothing in this Final Judgment and Consent Decree shall prevent or restrict the use of this Final Judgment and Consent Decree by Vermont in any action against Lenovo for contempt or failure to comply with any of its provisions, or in the event that Lenovo is in default of any of its terms and conditions. A default on the part of Lenovo shall include any material breach by Defendant of any of the terms or requirements of this Final Judgment and

Consent Decree. Nothing in this Final Judgment and Consent Decree shall be construed to (i) exonerate any contempt or failure to comply with any of its provisions after the Effective Date of this Final Judgment and Decree, (ii) compromise or limit the authority of Vermont to initiate a proceeding for any contempt or other sanctions for failure to comply, or (iii) compromise the authority of the Court or any other court of competent jurisdiction to punish as contempt any violation of this Final Judgment and Consent Decree.

E. Those signing for Lenovo below hereby state that they each are authorized to enter into and execute this Final Judgment and Consent Decree by and on behalf of Lenovo.

F. Lenovo further agrees to execute and deliver all authorizations, documents and instruments which are necessary to carry out the terms and conditions of this Final Judgment and Consent Decree, whether required prior to, contemporaneous with or subsequent to the Effective Date of this Final Judgment and Consent Decree, as defined herein.

G. To the extent that there are any, Lenovo agrees to pay all court costs associated with the filing of this Final Judgment and Consent Decree. No court costs, if any, shall be taxed against the Vermont Attorney General.

H. Lenovo shall not, directly or indirectly, participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part in Vermont that are prohibited by this Final Judgment and Consent Decree or for any other purpose that would otherwise circumvent any term of this Final Judgment and Consent Decree. Lenovo shall not cause, knowingly permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Final Judgment and Consent Decree.

I. This Final Judgment and Consent Decree may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall

constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Final Judgment and Consent Decree may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

J. This Final Judgment and Consent Decree sets forth all of the promises, covenants, agreements, conditions and understandings between the parties, and supersedes all prior and contemporaneous agreements, understandings, inducements or conditions, express or implied. There are no representations, arrangements, or understandings, oral or written, between the parties relating to the subject matter of this Final Judgment and Consent Decree that are not fully expressed herein or attached hereto. Each party specifically warrants that this Final Judgment and Consent Decree is executed without reliance upon any statement or representation by any other party hereto, except as expressly stated herein.

K. Lenovo agrees that this Final Judgment and Consent Decree does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and Lenovo further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

L. This Final Judgment and Consent Decree shall not be construed to waive any claims of sovereign immunity Vermont may have in any action or proceeding.

M. Except as otherwise provided under law, this Final Judgment and Consent Decree may only be enforced by Vermont, Lenovo, and this Court. The Parties to this action may agree, in writing, through counsel, to an extension of any time period in this Final Judgment and Consent Decree without a Court order.

X. SEVERABILITY

If any clause, provision, or section of this Final Judgment and Consent Decree shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Final Judgment and Consent Decree and this Final Judgment and Consent Decree shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

XI. NOTICE/DELIVERY OF DOCUMENTS

Whenever Lenovo shall submit documents or provide notice to the Vermont Attorney General under this Final Judgment and Consent Decree, that requirement shall be satisfied by sending notice to: Designated Contacts on behalf of the Attorneys General listed in Exhibit A. Any notices or other documents sent to Lenovo pursuant to this Final Judgment and Consent Decree shall be sent to the following address: (1) Lenovo (United States) Inc., ATTN: General Counsel, 1009 Think Place, Morrisville, North Carolina 27560-900 and (2) Rebecca S. Engrav, Esq., Perkins Coie, 1201 Third Avenue, Suite 4900, Seattle, WA 98101-3099. All notices or other documents to be provided under this Final Judgment and Consent Decree shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its address by sending written notice to the other party.

SIGNATURE

In lieu of further litigation against Defendant, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Judgment. By signing below, Defendant voluntarily agrees with and submits to the terms of this Final Judgment and Consent Decree.

DATED at Morrisville, NC, this 23rd day of August, 2017.

DEFENDANT, LENOVO (UNITED STATES) INC.

By: _____
Christian Teismann
Senior Vice President and General Manager,
Lenovo North America Sales (Interim)

By: _____
Christopher J. Valente (Vermont #5449)
christopher.valente@klgates.com
K&L GATES LLP
State Street Financial Center
One Lincoln Street
Boston, MA 02111
T. 617.261.3100
F. 617.261.3175

Rebecca S. Engrav
rengrav@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
T. 206.359.6168
F. 206.359.7168

Attorneys for Lenovo (United States) Inc.

ACCEPTED on behalf of the Attorney General:

DATED at ~~Burlington,~~ Montpelier Vermont this 5th day of September, 2017.

STATE OF VERMONT
THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____
Ryan G. Kriger
Assistant Attorney General

SIGNATURE

In lieu of further litigation against Defendant, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Judgment. By signing below, Defendant voluntarily agrees with and submits to the terms of this Final Judgment and Consent Decree.

DATED at _____, this ____ day of _____, 2017.

DEFENDANT, LENOVO (UNITED STATES) INC.

By: _____
Christian Teismann
Senior Vice President and General Manager,
Lenovo North America Sales (Interim)

By: _____
Christopher J. Valente (#5449)
christopher.valente@klgates.com
K&L GATES LLP
State Street Financial Center
One Lincoln Street
Boston, MA 02111
T. 617.261.3100
F. 617.261.3175

Rebecca S. Engrav
rengrav@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
T. 206.359.6168
F. 206.359.7168

Attorneys for Lenovo (United States) Inc.

ACCEPTED on behalf of the Attorney General:

DATED at ~~Burlington~~ Montpelier, Vermont this 5th day of September, 2017.

STATE OF VERMONT
THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____
Ryan G. Kriger
Assistant Attorney General

DECREE, ORDER AND FINAL JUDGMENT

This Consent Decree is accepted and entered as a Decree, Order and Final Judgment of this Court in the matter of: *State of Vermont v. Lenovo (United States) Inc.*, Docket No. _____ Wncv.

SO ORDERED.

DATED at Montpelier, Vermont this_____day of _____, 2017.

_____
Washington Superior Court Judge

STATE OF VERMONT

SUPERIOR COURT
Chittenden Unit

CIVIL DIVISION
Docket No. 822-9-16 Cncv

State of Vermont,
Plaintiff,

v.

Literati Creative Group, Inc.
and Krista Washburn,
Defendants.

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the State of Vermont having filed a Complaint (the "Complaint") against Literati Creative Group, Inc. and Krista Washburn (hereinafter collectively referred to as "Defendants"), for injunctive and other relief pursuant to 9 V.S.A. § 2453, alleging that the Defendants committed violations of the aforementioned Act. Plaintiff, by its counsel, and the Defendants have agreed to the entry of this Final Judgment and Consent Decree ("Judgment" or "Consent Decree") by this Court without trial or adjudication of any issue of fact or law.

PARTIES

1. The State of Vermont is the Plaintiff in this case and is represented by the Attorney General of the State of Vermont.

2. Defendant Literati Creative Group, Inc. ("LCG") was, at all times relevant to the subject of the Complaint, a Vermont domestic corporation. Its business purpose included publication of Vermont Vows and Well Wed Magazines ("magazines"). LCG's corporate status was terminated on June 18, 2016.

3. Defendant Krista Washburn was a principal of Literati Creative Group, Inc. Washburn had knowledge and control over the day-to-day operations of LCG.

4. At all times relevant hereto, LCG engaged in trade affecting consumers, within the meaning of the Vermont Consumer Protection Act, 9 V.S.A. § 2451 *et seq.,* in the State of Vermont including, but not limited to, Chittenden County.

DEFINITIONS

5. "Consumers" shall mean purchasers of goods or services as defined in 9 V.S.A. § 2451a(a).

6. "Covered Conduct" shall mean Defendants' publication of Vermont Vows and Well Wed magazines through the Effective Date of the Judgment.

7. "Effective Date" shall mean shall mean the date on which a copy of this Judgment, duly executed by the Parties, is approved by and becomes a Judgment of the Court.

8. "Parties" shall mean the State of Vermont, LCG and Krista Washburn.

9. "Vermont Consumer Protection Act" shall mean 9 V.S.A. § 2451 *et seq.*

FINDINGS

10. This Court has jurisdiction over the subject matter of this lawsuit and over the Parties.

11. The terms of this Judgment shall be governed by the laws of the State of Vermont.

12. Entry of this Judgment is in the public interest and reflects a negotiated agreement among the Parties.

13. The Parties have agreed to resolve the issues resulting from the Covered Conduct by entering into this Judgment.

14. The parties have consented to the entry of this Judgment solely for the purpose

of settlement and agree that it does not constitute an admission of the violation of law, rule, or regulation, or of any other matter of fact or law. Defendants have not admitted any violation of Vermont law. This Judgment is made without trial or adjudication of any issue of fact or law or finding of liability of any kind. No part of this Judgment shall create a private cause of action or confer any right to any third party for violation of state statute except that the State may file an action to enforce the terms of this Judgment. The statements and commitments contained in this Judgment are not for use by any third party for any purpose.

15. This Judgment does not create a waiver or limit Defendants' legal rights, remedies, or defenses in any other action by the Vermont Attorney General, except with respect to enforcement of this Judgment by the Attorney General, and does not waive or limit Defendants' right to defend themselves from, or make argument in, any other matter, claim, or suit, including, but not limited to any investigation or litigation relating to the subject matter or terms of this Judgment. Nothing in this Judgment shall waive, release or otherwise affect any claims, defenses, or positions Defendants may have in connection with any investigations, claims, or other matters the State is not releasing hereunder. Notwithstanding the foregoing, the State may file an action to enforce the terms of this Judgment.

REMEDIES

Defendants are enjoined and restrained as follows:

16. Defendants will not recommence publication of either Vermont Vows or Well Wed magazine or of any other magazine serving the wedding industry or for persons interested in wedding industry services.

17. For a period of five (5) years from the Effective Date, Defendant Washburn

may not have publication authority for any other print publication unless she provides sixty (60) days' written notice to the Consumer Protection Unit of the Vermont Attorney General's Office of her intention to do so along with a Fifty Thousand Dollars ($50,000) bond to be held by the Attorney General's Office. The bond shall be held for a period of five (5) years for the benefit of any businesses that may purchase advertisements in the new publication in the event publication does not take place as represented.

18. Except as set forth below, within ten (10) days after the Effective Date of this Judgment, Defendants shall pay a total of Seventeen Thousand Dollars ($17,000) to the State of Vermont, in care of the Attorney General's Office, for the purpose of paying restitution to Consumers pursuant to this Consent Decree.

19. Upon submission and review of tax returns for the years 2013, 2014, and 2015, credit report from three credit reporting agencies, banking statements for the past year, and a current statement of assets and liabilities, it has been determined by the Office of the Attorney General that Defendants are unable to pay the restitution set forth in paragraph 18, above. Based on Defendants' demonstrated inability to pay, Defendants are not required to pay such restitution, subject to the conditions set forth below.

20. No later than November 1 of each calendar year beginning in 2017 and ending in 2021, Defendant Washburn shall submit to the Vermont Attorney General's Office accurate copies of her income tax returns for each of the calendar years 2016 through 2020, respectively, along with sworn and accurate statements of her then-current assets and liabilities.

21. In the event an income tax return or statement of assets and liabilities required

by paragraph 20, above, shows that Defendant Washburn has pre-tax income exceeding Sixty-Five Thousand Dollars ($65,000), and/or net assets exceeding Ninety Thousand Dollars ($90,000), Defendant Washburn shall, no later than December 1 of that year, pay to the State of Vermont, in care of the Attorney General's Office, an amount equal to Twenty Percent (20%) of any pre-tax income exceeding Sixty-Five Thousand Dollars ($65,000), plus an amount equal to Twenty Percent (20%) of any net assets exceeding Ninety Thousand Dollars ($90,000), provided that once she has paid a total of Seventeen Thousand Dollars ($17,000) pursuant to this paragraph, she shall have no further liability or further obligation to report to the Attorney General's Office. Following submission of her 2020 tax return, if it is determined that Defendant Washburn does not have pre-tax income exceeding Sixty-Five Thousand Dollars ($65,000) and/or net assets exceeding Ninety Thousand Dollars ($90,000), then she shall have no further liability or further obligation to report to the Attorney General's Office.

22. Any pre-tax income or net assets described in paragraph 21, shall exclude the income and assets Defendant Washburn's spouse or partner. The income and assets of Defendant's spouse or partner shall not be subject to this Consent Decree. Any attempt by Defendant to contravene this Judgment by placing income or assets under the control of any spouse or partner shall be considered a violation of this Consent Decree.

23. The Attorney General at his discretion may waive the interest on the amount described in paragraphs 19-22, depending on the particular circumstances of Defendant in a given year and following submission of her tax return for that year.

OTHER TERMS

24. The Attorney General hereby releases and discharges any and all claims arising under the Consumer Protection Act, 9 V.S.A. §§ 2451-2480, that it may have against Defendants for the conduct described in the Complaint.

25. The Superior Court of the State of Vermont, Chittenden Unit, shall have jurisdiction over this matter and the parties hereto for the purpose of enabling the Attorney General to apply to this Court at any time for orders and directions as may be necessary or appropriate to enforce compliance with or to punish violations of this Consent Decree.

26. Defendants shall be subject to a tax off-set through the Vermont Department of Taxes if any amounts ordered are unpaid as per 32 V.S.A. § 5933.

STIPULATED PENALTIES

27. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondent to be in violation of this Consent Decree, then the parties agree that penalties to be assessed by the Court for each act in violation of this Consent Decree shall be $10,000.

SIGNATURE

In lieu of further litigation against Defendants, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Judgment. By signing below, Defendants voluntarily agree with and submit to the terms of this Consent Decree.

DATED at _____, this 30th day of June, 2017.

Krista Washburn – individually

Krista Washburn on behalf of Literati Creative Group, Inc.

ACCEPTED on behalf of the Attorney General:

DATED at ~~Burlington,~~ Montpelier Vermont this 29th day of June, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____

Ryan G. Kriger
Assistant Attorney General

DECREE, ORDER AND FINAL JUDGMENT

This Consent Decree is accepted and entered as a Decree, Order and Final Judgment of this Court in the matter of: *State of Vermont v. Literati Creative Group, Inc., and Krista Washburn,* Docket No. 822-9-16 Cncv.

SO ORDERED.

DATED at Burlington, Vermont this 10th day of July, 2017.

Chittenden Superior Court Judge

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

In re: Nationwide Mutual Insurance Company)
and)
Allied Property & Casualty Insurance Company)

Civil Division

Docket No. 455-8-17 Wncv

ASSURANCE OF DISCONTINUANCE

In Re:

NATIONWIDE MUTUAL INSURANCE COMPANY

and

ALLIED PROPERTY & CASUALTY INSURANCE COMPANY

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance (the "Assurance")[1] is between Nationwide Mutual Insurance Company, an Ohio corporation ("Nationwide"), acting for itself and its wholly-owned subsidiary Allied Property & Casualty Insurance Company ("Allied") (referred to collectively as "Nationwide/Allied"), and the Attorneys General of Alaska, Arizona, Arkansas, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, and the District of Columbia (referred to collectively as the "Attorneys General").[2]

PARTIES

1. The Attorneys General have defined jurisdiction under the laws, or assert jurisdiction under the common law, of their respective States for the enforcement of state laws and regulations, which may include state Consumer Protection Acts and state Personal Information Protection Acts.

---

[1] This Assurance of Voluntary Compliance shall, for all necessary purposes, also be considered an Assurance of Discontinuance.

[2] For simplicity purposes, the entire group will be referred to as the "Attorneys General," or individually as "Attorney General." Such designations, however, as they pertain to Hawaii shall mean the State of Hawaii, including the Executive Director of the State of Hawaii, Office of Consumer Protection and as they pertain to Connecticut, shall include the Commissioner of Consumer Protection.

2. Nationwide Mutual Insurance Company is an Ohio corporation with its principal place of business at One Nationwide Plaza, Columbus, OH 43215. Nationwide is a property and casualty insurer doing business throughout the United States, including in the States.

3. Allied Property & Casualty Insurance Company is an Iowa corporation with its principal place of business at 1100 Locust Street, Des Moines, IA 50391. In 1998, Nationwide acquired Allied as a wholly-owned subsidiary.

DEFINITIONS

For the purposes of this Assurance, the following definitions shall apply:

4. "**Effective date**" shall be August 9, 2017.

5. "**Common vulnerabilities and exposures**" or "**CVE**" shall mean a specific numbered vulnerability that has at the time in question been published as a "Common Vulnerability and Exposure" by MITRE Corporation or appears in the U.S. Government's "National Vulnerability Database" (e.g., "CVE-20XX-XXXX"), or if both of the two foregoing vulnerability lists are no longer in existence, any substantially equivalent successor publication jointly selected by Nationwide/Allied and the States.

6. "**Consumer Protection Acts**" shall mean the statutes listed in Section A of the attached Appendix to Assurance of Voluntary Compliance ("Appendix").

7. "**Covered systems**" shall mean all routers, switches, firewalls, servers, common operating systems, and applications within Nationwide/Allied's datacenter network that are used to collect, process, and store personal information.

8. "**Personal information**" shall have the same definition as set forth in the Personal Information Protection Acts. In the absence of any such statutory definition, "personal information" shall mean any record of Nationwide/Allied (unless encrypted) containing the

following information about an individual collected in connection with receiving an insurance price quote: any individual's first name or first initial and last name, in combination with one or more of the following: (i) social security number; (ii) driver's license number or state identification card number; or (iii) account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial account, and does not include information that is lawfully made available to the general public from federal, state or local government records or widely distributed media or is otherwise lawfully available from publicly available information.

9. "**Personal Information Protection Acts**" shall mean the statutes listed in Section B of the attached Appendix.

10. "**Security information and event management**" shall mean a system that correlates data to identify potential information technology security events and/or security incidents.

11. "**States**" when used herein shall refer to the States of Alaska, Arizona, Arkansas, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, and Washington, as well as the District of Columbia.

THE ATTORNEYS GENERAL'S ALLEGATIONS

12. In order to provide consumers with insurance quotes, Nationwide/Allied collected information from consumers residing in the States, including all or a portion of the following: (a) full name; (b) sex; (c) occupation; (d) employer name and address; (e) driver's license number

and state of issuance; (f) Social Security number; (g) marital status; (h) date of birth; and (i) a Nationwide internal credit-related score.

13. On October 3, 2012, Nationwide/Allied experienced a criminal data breach ("the Intrusion") that Nationwide/Allied believes may have resulted in the loss of data containing some or all of the above listed consumer information for 1.27 million consumers, including consumers residing in the States.

14. The data breach occurred when hackers exploited a vulnerability in Nationwide/Allied's web application hosting software. After data were exfiltrated, Nationwide/Allied addressed the software vulnerability by applying a software patch that was not previously applied.

NATIONWIDE/ALLIED'S DENIALS

15. Nationwide/Allied admits it experienced a criminal data breach, but denies any liability or wrongdoing relating thereto, as more fully set forth in paragraph 50, *infra*, and further denies the Attorneys General have jurisdiction over the matters addressed in this Assurance.

REQUIREMENTS

16. Nationwide/Allied shall maintain an online disclosure that personal information it collects from individuals, even if they do not become insureds, is retained while the individual's account is active or to provide services, and as required or permitted by law.

17. Nationwide/Allied shall appoint an individual (referred to herein as the "Patch Policy Supervisor") who shall be at least an elected information technology officer and, for a period of three (3) years from the effective date of this Assurance, shall be responsible for

maintaining the process by which Nationwide/Allied's security policies as to software and application security updates and security patch management are regularly reviewed and by which revisions are made. Such policies shall (during this time frame) address the application of security updates or security patches to covered systems in a reasonable fashion and time frame, taking into account (without limitation) the currency of the software to which the update or patch relates, the sensitivity and nature of the data that the software stores, processes or transmits, the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue as reasonably determined by Nationwide/Allied in the context of its overall network, any compensating controls and its ongoing business and network operations, and the scope of the resources required to address the issue.

18. Nationwide/Allied shall appoint an individual (referred to herein as the "Patch Supervisor") who shall be at least an elected information technology officer and shall be responsible for (a) monitoring and managing software and application security updates and security patch management; (b) supervising, evaluating, and coordinating the maintenance, management, and application of all security patches and software and application security updates, including monitoring for notifications of patches identified by applicable software providers; and (c) supervising, evaluating and coordinating any system patch management tool(s) such as those identified in paragraphs 22(d) and (e).

19. Nationwide/Allied shall, for a period of three (3) years from the effective date of this Assurance, under the direction and/or coordination of the Patch Supervisor, maintain and, on at least a semi-annual basis, update, an inventory of all covered systems they utilize. The inventory required under this paragraph shall include: (a) name; (b) version; and (c) a list of any software and application security updates and security patches applied or installed during the

preceding period. During this time frame, Nationwide/Allied shall use this inventory in its regular operations to assist in reviewing whether new security updates or security patches are available for any covered system, and for each new security update and security patch under consideration, Nationwide/Allied shall assign a priority level and schedule any related action that may reasonably be determined to be pursued with respect to the covered systems, taking into consideration risk levels identified by software and application providers, and shall address any security updates and security patches, consistent with the policies set forth in paragraph 17, supra, and maintain for a period of at least three (3) years a written exception stating the basis for exceptions therefrom.

20. Nationwide/Allied shall, for a period of three (3) years from the effective date of this Assurance, regularly review and update its Incident Management Policy and Procedures by which it commences and manages its response and review of information security incidents, and reporting to a security manager, in relation to the circumstances of the incident. Information, security incident and investigation records maintained within the Event Management System shall have a retention period of three (3) years. No waiver of any applicable legal protection or privilege as to such matters is intended or effected hereby.

21. Nationwide/Allied shall, for a period of three (3) years from the effective date of this Assurance, deploy (to the extent it has not already done so) and maintain a system management tool (or contract with a vendor) to provide such service, the purpose of which shall be to:

(a) provide Nationwide/Allied with near real-time updates regarding known CVEs for any vendor-purchased software applications in use within its covered systems;

(b) identify, confirm and enhance discovery of covered systems that may be subject to CVE events and/or incidents; and

(c) scan covered systems for CVEs.

22. Nationwide/Allied shall, for a period of three (3) years from the effective date of this Assurance, further (to the extent it has not already done so):

(a) implement processes and procedures for Nationwide/Allied's covered systems that provide for notification of CVEs to the teams responsible for currency and patch management of the technology impacted;

(b) implement processes and procedures for Nationwide/Allied's covered systems to evaluate the relative severity of identified CVEs in the context of the technology and network area impacted and, based on Nationwide/Allied's evaluation, prioritize any mitigation actions in response;

(c) document in writing the risk severity attached to each CVE evaluated under subparagraph (b) and mitigation or exception actions taken in response thereto;

(d) purchase and install, as to Nationwide/Allied's covered systems, an automated CVE feed from a solution provider, to Nationwide/Allied's intrusion detection system/intrusion protection system; and

(e) purchase and install, as to Nationwide/Allied's covered systems, an automated CVE feed from a solution provider to Nationwide/Allied's security information and event management technology.

23. On at least a semi-annual basis, for a period of three (3) years from the effective date of this Assurance, Nationwide/Allied shall perform an internal patch management

assessment of the covered systems. This assessment shall identify known CVEs rated by Nationwide/Allied as critical, high, and medium risk and confirm appropriate patches have been applied or that any exceptions were noted. The assessment and any exceptions will be formally identified, documented and reviewed by the Patch Supervisor.

24. On at least an annual basis, for a period of three (3) years from the effective date of this Assurance, Nationwide/Allied shall hire an outside, independent provider to perform a patch management audit of Nationwide/Allied's covered systems. This audit will identify known CVEs rated as critical, high, and medium risk and confirm that appropriate patches have been applied or that any exceptions have been formally documented. A formal executive summary shall be available to the Attorneys General for review upon request.

25. One (1) year after the effective date of this Assurance, Nationwide/Allied shall provide the Attorneys General with a certification of its compliance with this "Requirements" section of the Assurance (the "Compliance Certification") to date. The Compliance Certification shall describe each of the policies or practices that Nationwide/Allied have implemented, or that remain in place, that establish Nationwide/Allied's compliance with the Requirements section of this Assurance. The Attorneys General shall maintain the Compliance Certification they receive consistent with the requirements of paragraph 27.

26. The written policies, inventories, assessments, and audits referenced under the "Requirements" section of this Assurance that are in effect or created during the three (3) year period following the effective date of this Assurance shall be available to the Attorneys General during that period or for one year after creation, whichever is longer, upon reasonable request.

27. The Attorneys General shall treat all information (including without limitation any documents) they receive under this Assurance as exempt from disclosure under the relevant

public records laws to the fullest extent they are able to do such under such laws and agree to reasonably secure such information. Nationwide/Allied contends all such documents contain sensitive information about the current state of Nationwide/Allied's security infrastructure and mechanisms, which could be harmful to Nationwide/Allied's ability to secure data if disclosed. In the event that an Attorney General receives any request from the public to inspect any Compliance Certification or other documentation of compliance and that Attorney General believes such document is subject to disclosure under any public record law, that Attorney General agrees to provide Nationwide/Allied with at least twenty (20) days advance notice before producing documents in response to such a request, to the extent permitted by state law (and with any required lesser advance notice), so that Nationwide/Allied may take appropriate action to defend against the disclosure of such documents. The notice required under this paragraph shall be provided consistent with the notice requirements contained in paragraph 43.

PAYMENT TO THE ATTORNEYS GENERAL

28. Within thirty (30) days of the effective date of this Assurance, Nationwide/Allied shall pay Five Million, Five Hundred Thousand Dollars ($5,500,000.00) to the Attorneys General, to be distributed as agreed by the Attorneys General. The money received by the Attorneys General pursuant to this paragraph may be used for purposes that may include, but are not limited to, attorneys' fees and costs of investigation and litigation, placed in, or applied to, any consumer protection law enforcement fund including future consumer protection or privacy enforcement, consumer education, litigation, local consumer aid or revolving funds, used to defray the costs of the inquiry leading to this Assurance, or for other uses permitted by state law,

and all at the sole discretion of the Attorneys General. [3]

ENFORCEMENT

29. The parties agree that this Assurance constitutes a legally enforceable agreement. This Assurance and the rights and obligations of the parties hereunder shall be governed within each of the respective States by the laws of such States in which any enforcement of this Assurance or any action to determine the rights and obligations hereunder is attempted.

30. This Assurance may be enforced only by the parties hereto. Nothing in this Assurance shall provide any rights to or permit any person or entity not a party hereto, including any State or Attorney General not a party hereto, to enforce any provision of this Assurance. No person or entity not a signatory hereto is a third-party beneficiary of this Assurance. Nothing in this Assurance shall be construed to create, affect, limit, alter, or assist any private right of action, including without limitation any private right of action that a consumer or other third-party may hold against Nationwide/Allied.

31. This Assurance shall be binding on the parties. Notwithstanding any other provision in this Assurance, the obligations herein shall not apply to any act or omission within any state that has not signed this Assurance.

---

[3] By agreement of the Missouri Office of Attorney General and Nationwide, payment to the State of Missouri shall be paid into the Merchandising Practices Revolving Fund pursuant to Section 407.010, RSMo. The Washington Attorney General shall use the funds for recovery of the costs and attorneys' fees incurred in investigating this matter, future monitoring and enforcement of this Assurance, future enforcement of RCW 19.86, or for any lawful purpose in the discharge of the Attorney General's duties at the sole discretion of the Attorney General. No part of this payment shall be deemed a civil penalty. The money received by the State of Indiana pursuant to this paragraph may be used for any purpose allowable under state law, including to protect the privacy and security of Indiana residents' personal information. The remainder of this footnote refers only to New Mexico's use of the monetary amount it receives and in no way refers to conduct by Nationwide. With that understanding, the settlement portion allocated to New Mexico shall be expended, in the sole discretion of the New Mexico Attorney General, to enhance the Office's law enforcement efforts to prevent and prosecute unfair or deceptive acts or practices and to investigate, enforce and prosecute any illegal conduct related to financial services or consumer protection laws.

32. This Assurance may be modified or amended solely in writing by the Attorneys General and Nationwide/Allied, subject to any limitations contained in paragraph 35 below. If Nationwide/Allied believes that any modification or amendment of this Assurance becomes warranted or appropriate for any reason, including, but not limited to, changes in the risks to the security, confidentiality, and integrity of personal information or to the relevant security procedures, practices, or tools used to protect against those risks, Nationwide/Allied may submit to the Attorneys General the proposed written modification or amendment.

33. Nothing in this Assurance shall be construed as preventing or exempting Nationwide/Allied from complying with any law, rule, or regulation, nor shall any of the provisions of this Assurance be deemed to authorize or require Nationwide/Allied to engage in any acts or practices prohibited by any law, rule, or regulation.

34. If Nationwide/Allied believes that any provision in this Assurance conflicts in whole or in part with any law, rule, or regulation as modified, enacted, promulgated, or interpreted by the state or federal governments or any state or federal agency, including the state departments of insurance, then, subject to the limitations contained in paragraph 35, Nationwide/Allied may provide a written proposal to the Attorneys General relative to the believed conflict, identifying the nature of the conflict and the manner in which Nationwide/Allied proposes to proceed in light of the purported conflict.

35. To the extent this Assurance is filed in any court, such court retains jurisdiction over this Assurance and the parties hereto for the purpose of enforcing and modifying this Assurance and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Assurance shall be valid or binding unless made in writing, signed by the parties, and approved by any court in which the Assurance is

filed, and then only to the extent specifically set forth in such a court's order. The parties may agree in writing, through counsel, to an extension of any time period in this Assurance without a court order.

RELEASE

36. Effective immediately upon full payment of the amounts due under this Assurance, this Assurance constitutes a full and final settlement and release by the Attorneys General that are parties to this Assurance from any and all civil, regulatory and administrative proceedings, claims, and causes of action against Nationwide Mutual Insurance Company, Allied Property & Casualty Insurance Company and their affiliates, subsidiaries, successors and assigns, including any of their officers, agents, directors, attorneys and employees, arising out of or relating to the Intrusion, or the subject matter of the Attorneys General's investigation set forth in paragraphs 12 through 14, or Nationwide/Allied's conduct in relation thereto, which the Attorneys General have, or could have asserted or brought prior to the effective date of this Assurance, under the Consumer Protection Acts (however denominated in the respective states in Section A of the attached Appendix), or Personal Information Protection Acts (however denominated in the respective states in Section B of the attached Appendix), or other state laws regarding the safeguarding of consumers' personal information. Nothing contained in this paragraph shall be construed to limit the ability of the Attorneys General to enforce the obligations that Nationwide/Allied has under this Assurance.

37. Notwithstanding any term of this Assurance, any and all of the following forms of liability are specifically reserved and excluded from the release in paragraph 36 as to any entity or person, including Nationwide/Allied:

(a) Any criminal liability that any person or entity, including Nationwide/Allied, have or may have to the Attorneys General.

(b) Any civil or administrative liability that any person or entity, including Nationwide/Allied, have or may have to the States under any statute, regulation or rule not covered by the release in paragraph 36 above, including but not limited to, any rule giving rise to any and all of the following claims:

(i) State or federal antitrust violations;

(ii) State or federal securities violations; or

(iii) State or federal tax claims.

GENERAL PROVISIONS

38. Nationwide/Allied shall not knowingly cause or encourage third parties acting on its behalf, nor knowingly permit third parties acting on its behalf, to engage in practices from which Nationwide/Allied are prohibited by this Assurance.

39. Nationwide/Allied shall not, directly or indirectly, form a separate entity or corporation for the purpose of engaging in acts prohibited by this Assurance or for the purpose of circumventing this Assurance.

40. This Assurance represents the full and complete terms of the settlement entered by the parties.

41. All parties participated in the drafting of this Assurance.

42. This Assurance may be executed in counterparts, and a facsimile or .pdf signature shall be deemed to be, and shall have the same force and effect as, an original signature.

43. All notices under this Assurance shall be provided via electronic and/or overnight

mail to the following persons, unless a different address is specified in writing by the party changing such address:

For Nationwide Mutual Insurance Company and
Allied Property & Casualty Insurance Company

Kirk Herath
VP, Chief Privacy Officer, Associate General Counsel
Nationwide
One Nationwide Plaza, 1-32-304
Columbus, OH 43215
614-249-4420
herathk@nationwide.com

For the Attorneys General, please see the persons listed in Section C of the attached Appendix.

44. Any failure by any party to this Assurance to insist upon the strict performance by any other party of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions of this Assurance, and such party, notwithstanding such failure, shall have the right thereafter to insist upon the specific performance of any and all of the provisions of this Assurance. For the Attorneys General, this shall be without prejudice to the imposition of any applicable remedies, including but not limited to contempt, civil penalties and/or the payment of attorneys' fees to any Attorney General, and any other remedies under applicable state law.

45. Except for the release in paragraph 36, if any clause, provision or section of this Assurance shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision or section of this Assurance and this Assurance shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section or other provision had not been contained herein.

46. Nothing in this Assurance shall be construed as relieving Nationwide/Allied of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of

the provisions of this Assurance be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

47. Nothing in this Assurance limits Nationwide/Allied's right, at its sole discretion, to take measures in connection with the maintenance and safeguarding of personal information in addition to what is required in this Assurance.

48. The parties understand and agree that this Assurance shall not be construed as an approval or a sanction by Attorneys General of the business practices of Nationwide/Allied, and Nationwide/Allied shall not represent that this Assurance constitutes an approval or sanction of its business practices. The parties further understand and agree that any failure by any Attorney General to take any action in response to any information submitted pursuant to this Assurance shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.

49. Nationwide/Allied shall deliver a copy of this Assurance to, or otherwise fully apprise, its executive management having decision-making authority with respect to the subject matter of this Assurance within thirty (30) days of the effective date of this Assurance.

50. This Assurance (including without limitation any and all legal and factual statements herein) is not intended to be and shall not in any event be construed or deemed to be, or represented or caused to be represented as, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Nationwide/Allied or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind. Nationwide/Allied believes that its conduct has been lawful and has not violated any consumer protection or other laws or the common law of the States and enters into this Assurance for settlement purposes only.

Without limitation of the terms of paragraph 35, supra, Nationwide/Allied's agreement to undertake the obligations described in this Assurance shall not be construed as an admission of any kind or type including as to jurisdiction.

51. This Assurance shall not be construed or used as a waiver or any limitation of any defense otherwise available to Nationwide/Allied in any pending or future legal or administrative action or proceeding relating to its conduct prior to the effective date of this Assurance or of Nationwide/Allied's right to defend itself from, or make any arguments in, any individual or class claims or suits relating to the existence, subject matter, or terms of this Assurance.

52. For purposes of enforcement by the Iowa Attorney General, a violation of this Assurance, if established by the Iowa Attorney General by a preponderance of the evidence in an action by the Iowa Attorney General against Nationwide/Allied, shall be deemed a violation of Iowa Code § 714.16. This Assurance creates no right of action under Iowa Code § 714H.

53. The settlement negotiations resulting in this Assurance have been undertaken by Nationwide/Allied and the Attorneys General in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Assurance, or this Assurance itself, shall be offered or received in evidence in any action or proceeding for any purpose.

54. Nothing contained in this Assurance, and no act to be performed hereunder, including, but not limited to, the Compliance Certification, the provision of any documentation of Nationwide/Allied's compliance with this Assurance, or the provision of information and/or material, shall require Nationwide/Allied to waive (a) any attorney-client privilege, work-product protection, or common interest/joint defense privilege, or (b) confidential, proprietary, or trade secret exception under the States' public records laws.

55. To the extent there are any, Nationwide/Allied agrees to pay all court costs associated with the filing (if legally required) of this Assurance. No court costs, if any, shall be taxed against the Attorneys General.

SIGNATURE

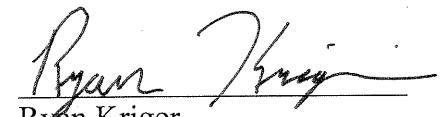
In lieu of instituting an action or proceeding against Respondents, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, Respondent voluntarily agrees with and submits to the terms of this Assurance of Discontinuance.

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 24th day of July, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: 

Ryan Kriger
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
802-828-3170

NATIONWIDE MUTUAL INSURANCE COMPANY

and

ALLIED PROPERTY AND CASUALTY INSURANCE COMPANY

By: _____

Kirk Herath
VP, Chief Privacy Officer, Associate General Counsel
Nationwide

Date: 8-3-17

APPENDIX: SECTION A

STATE	CONSUMER PROTECTION ACTS
Alaska	Alaska Unfair Trade Practices and Consumer Protection Act, AS 45.50. 471, *et seq.*
Arizona	Arizona Consumer Fraud Act, A.R.S. §§ 44-1521 – 44-1534
Arkansas	Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101, *et seq.*
Connecticut	Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110a, *et seq.*
D. Columbia	Consumer Protection Procedures Act, D.C. Code § 28-3901, *et seq.*
Florida	Florida Deceptive and Unfair Trade Practices Act, § 501.201, *et. seq.*, Fla. Stat.
Hawaii	Uniform Deceptive Trade Practice Act- Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Sect. 480-2
Illinois	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*
Indiana	Deceptive Consumer Sales Act, Indiana Code chapter 24-5-0.5
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16
Kentucky	Kentucky Consumer Protection Act, Ky. Rev. Stat. 367.110-.300
Louisiana	Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. 51:1401, *et seq.*
Maine	5 M.R.S. § 205-A, *et seq.*
Maryland	Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101, *et seq.* (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Massachusetts Consumer Protection Act (Mass. Gen. Laws ch. 93A)
Mississippi	Mississippi Consumer Protection Act Miss. Code Ann. § 75-24-1, *et seq.*
Missouri	Missouri Merchandising Practices Act, Chapter 407, RSMo.
Montana	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-101, *et seq.*
Nebraska	Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601 et seq., and Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301, *et seq.*
Nevada	Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903-.0999
New Mexico	Unfair Practices Act NMSA 1978 §57-12-1, *et seq.*
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1, *et seq.*
New York	Executive Law 63(12) and General Business Law 349/350
North Carolina	North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, *et seq.*
North Dakota	N.D.C.C. ch. 51-15 (Unlawful Sales or Advertising Practices)
Oregon	Oregon Unlawful Trade Practices Act, Oregon Revised Statutes (ORS) 646.605 *et seq.*
Pennsylvania	Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq.*
Rhode Island	Rhode Island General Laws, § 6-13.1-1, et seq., known as the Rhode Island Deceptive Trade Practices Act
South Dakota	SDCL Chapter 37-24
Tennessee	Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-108
Texas	Texas Deceptive Trade Practices Act, Tex. Bus. & Com. Code Ann. § 17.41 (West 2011)
Vermont	Vermont Consumer Protection Act, § 9 V.S.A. 2451, *et seq.*
Washington	Consumer Protection Act, RCW 19.86.020

APPENDIX: SECTION B

STATE	PERSONAL INFORMATION PROTECTION ACTS
Alaska	Alaska Personal Information Protection Act, AS 45.48.010 et seq., including, without limitation, Alaska Breach of Security Involving Personal Information statutes, AS 45. 48.0 10-45.48.090
Arizona	Notification of Breach of Security System, A.R. S. § 18-545 (formerly Ariz. Rev. Stat. § 44-7501. (effective December 31, 2006 through April 5, 2016))
Arkansas	Arkansas Personal Information Protection Act. Ark. Code Ann. § 4-110-101 et seq., including, without limitation, Disclosure of Security Breaches, Ark. Code Ann. § 4-110-105
Connecticut	Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471; Breach of Security re Computerized Data Containing Personal Information, Conn. Gen. Stat. § 36a-701b
D. Columbia	Security Notification Act, D. C. Code§ 28-3851, *et seq.*
Florida	Florida Information Protection Act, Fla. Stat. § 501.171 (effective July 1, 2014); Fla. Stat. § 817.5681 (effective July 1, 2005 through June 30, 2014)
Hawaii	Personal Information Protection- Haw. Rev. Stat. Chpt. 487J; Security Breach of Personal Information- Haw. Rev. Stat. Chpt. 487N
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*
Indiana	Disclosure of Security Breach Act, Indiana Code article 24-4.9, including, without limitation Indiana Code section 24-4.9-3-3.5(c) (see 2017 Ind. Legis. Serv. P.L. 76-2017 (S.E.A. 549) (WEST))
Iowa	Iowa Personal Information Security Breach Protection Act, Iowa Code § 715C
Kentucky	Ky. Rev. Stat. 365.732
Louisiana	Database Security Breach Notification Law, La. Rev. Stat. 51:3071, *et seq.*; and Reporting Requirements, La. Admin. Code tit. 16, pt. 3, §701
Maine	Maine Notice of Risk to Personal Data Act, 10 M.R. S. § 1346, *et seq.*
Maryland	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501, *et seq.* (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Mass. Gen. Laws ch. 93H, §§ 1, *et seq.* and Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 C.M.R. 17.00 et seq.)
Mississippi	Notice of Breach of Security Miss. Code Ann.§ 75-24-29
Missouri	Missouri Merchandising Practices Act, Section 407.1500, RSMo., including, without limitation, Missouri Merchandising Practices Act, § 407.1500.1(9), RSMo.
Montana	Montana Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1701 et seq., including, without limitation, Mont. Code Ann. § 30- 14-1704
Nebraska	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801, *et seq.*
Nevada	Nevada Security of Personal Information Act; Nev. Rev. Stat. §§ 603A.010, et seq., including, without limitation, Nev. Rev. Stat. § 603A.220 (located within the Nevada Security of Personal Information Act)
New Mexico	Data Breach Notification Act, NMSA 1978 Section 57-12(C)-1 et seq.
New Jersey	Identity Theft Prevention Act, N.J.S.A. 56:8-161, *et seq.*
New York	NYS Information Security Breach and Notification Act (General Business Law 899-aa) (as to the New York Attorney General, when this agreement uses the term "personal information," it shall have the meaning set forth for "private information" in the NYS Information Security Breach and Notification Act)
North Carolina	North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-60, *et seq.*, including, without limitation, N.C. Gen. Stat. § 75-65
North Dakota	N.D.C.C. ch. 51-30 (Notice of Security Breach for Personal Information)
Oregon	Oregon Consumer Identity Theft Protection Act, ORS 646A.600 to 646A.628.
Pennsylvania	Breach of Personal Information Notification Act, 73 P.S. §§ 2301, et *seq.*
Rhode Island	Rhode Island General Laws, § 11-49.3-1, *et seq.*, known as the Rhode Island Identity Theft Protection Act, including, without limitation, R.I. Gen. Laws§ 11-49.3-4
Tennessee	Identity Theft Deterrence, Tenn. Code Ann. § 47-18-2101 et seq., including, without limitation, Tenn. Code Ann. § 47-18-2107
Texas	Texas Identify Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. Ch. 521 (West 2015)
Vermont	Vermont Security Breach Notice Act, § 9 V.S.A. 2435
Washington	Data Breach Notification Law, RCW 19.255.010

APPENDIX: SECTION C

STATE	ATTORNEYS GENERAL CONTACTS
Alaska	Davyn Williams, Assistant Attorney General, 1031 W 4th Ave., Suite 200, Anchorage, AK 99501, 907-269-5200, davyn.williams@alaska.gov
Arizona	Taren Ellis Langford, Chief Counsel, Consumer Litigation Unit, Office of the Arizona Attorney General, Consumer Protection & Advocacy Section, 400 W. Congress, Suite S-315, Tucson, AZ 85701, 520-628-6504, Taren.Langford@azag.gov
Arkansas	Peggy Johnson, Assistant Attorney General, 323 Center Street Suite 500, Little Rock, AR, 72201, 501-682-8062, Peggy.johnson@arkansasag.gov
Connecticut	Matthew F. Fitzsimmons, Assistant Attorney General, Department, Head Privacy and Data Security Department, Office of the Attorney General, 110 Sherman Street, Hartford CT 06105, 860-808-5440, Matthew.Fitzsimmons@ct.gov
D. Columbia	Philip D. Ziperman, Director, Office of Consumer Protection, Office of the Attorney General for the District of Columbia, 442 4th Street, N.W., 6th Floor, Washington, D.C. 20001, 202-442-9886, philip.ziperman@dc.gov
Florida	Patrice Malloy, Chief, 110 S.E. 6th Street, Fort Lauderdale, FL, 33301, 954-712-4669, Patrice.Malloy@myfloridalegal.com
Hawaii	Lisa P. Tong, State of Hawaii Office of Consumer Protection, 235 S. Beretania Street #801, Honolulu, Hawaii 96813, 808-586-2636, ltong@dcca.hawaii.gov
Illinois	Matthew W. Van Hise, CIPP/US, Assistant Attorney General, Consumer Privacy Counsel, Consumer Fraud Bureau, Illinois Attorney General's Office, 500 South Second Street, Springfield, IL 62706, 217-782-9024, mvanhise@atg.state.il.us
Indiana	Ernâni Magalhães, Deputy Attorney General, Consumer Protection Division, Office of Attorney General Curtis Hill, 302 West Washington Street, IGCS-5th Floor, Indianapolis, IN 46204, 317-234-6681, ernani.magalhaes@atg.in.gov
Iowa	Nathan Blake, Deputy Attorney General, Office of the Iowa Attorney General, 1305 E. Walnut St. Des Moines, IA 50314, 515-281-4325, nathan.blake@iowa.gov
Kentucky	Kevin R. Winstead, Assistant Attorney General, 1024 Capital Center Dr., #200, Frankfort, KY 40601, 502-696-5379, kevin.winstead@ky.gov
Louisiana	L. Christopher Styron, Assistant Attorney General, 1885 N. Third Street, Baton Rouge, LA 70802, 225-326-6468, styronl@ag.louisiana.gov
Maine	Christina Moylan, Assistant Attorney General, Office of the Maine Attorney General, 6 State House Station, Augusta, Maine, 04333-0006, 207-626-8838, christina.moylan@maine.gov
Maryland	Richard Trumka Jr., Assistant Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 410-576-6957, rtrumka@oag.state.md.us
Massachusetts	Sara Cable, Assistant Attorney General, Director of Data Privacy & Security, Consumer Protection Division, Office of the Massachusetts Attorney, One Ashburton Place, Boston, MA 02108, (617) 727-2200, sara.cable@state.ma.us
Mississippi	Crystal Utley Secoy, Special Assistant Attorney General, Consumer Protection Division, Mississippi Attorney General's Office, Post Office Box 22947, Jackson, Mississippi 39225, 601-359-4213, cutle@ago.state.ms.us
Missouri	Joyce Yeager, Assistant Attorney General, Consumer Protection Section, Office of the Missouri Attorney General, PO Box 899, Jefferson City, MO 65102, 573-751-6733, joyce.yeager@ago.mo.gov
Montana	Kelley L. Hubbard, Assistant Attorney General, PO Box 200151, Helena, MT 59620-0151, 406-444-2026, khubbard@mt.gov
Nebraska	Dan Birdsall, Assistant Attorney General, 2115 State Capitol, Lincoln, NE 68509-8920, 402-471-3840, dan.birdsall@nebraska.gov
Nevada	Lucas J. Tucker, Senior Deputy Attorney General, Bureau of Consumer Protection, 10791 W. Twain Ave., Suite 100, Las Vegas, Nevada 89135, 702-486-3256, LTucker@ag.nv.gov
New Mexico	Cholla Khoury, Director, Consumer and Environmental Protection Division, 408 Galisteo St., Santa Fe, NM 87504, 505-231-3483, ckhoury@nmag.gov
New Jersey	Patricia Schiripo, Deputy Attorney General/ Assistant Chief, 124 Halsey Street, 5th Floor, Newark, NJ 07101 973-648-7819, patricia.schiripo@law.njoag.gov
New York	Clark P. Russell, Deputy Bureau Chief, Bureau of Internet and Technology, New York State Office of the Attorney General , 120 Broadway, New York, NY 10271-0332, 212-416-8422, clark.russell@ag.ny.gov
North Carolina	Kim D'Arruda, Special Deputy Attorney General, NC Department of Justice, Consumer Protection Division, 114 West Edenton St, Raleigh, NC 27603, 919-716-6013, Kdarruda@ncdoj.gov
North Dakota	Brian Card, Assistant Attorney General, Gateway Professional Center, 1050 E. Interstate Ave., Suite 200, Bismarck, ND 58503-5574, 701-328-5570, bmcard@nd.gov
Oregon	Andrew Shull, Senior Assistant Attorney General, 1162 Court Street, NE, Salem, OR 97301-4096, 503-934-4400, andrew.shull@doj.state.or.us
Pennsylvania	John Abel, Senior Deputy Attorney General, Bureau of Consumer Protection, Office of the Attorney General, 15th Floor, Strawberry Square, Harrisburg, Pennsylvania 17120, 717-787-9707, jabel@attorneygeneral.gov
Rhode Island	Edmund F. Murray, Jr., Special Assistant Attorney General, Rhode Island Department of Attorney General, 150 South Main Street, Providence, RI 02903, 401-274-4400 ext. 2401, emurray@riag.ri.gov
South Dakota	Phil Carlson, Assistant Attorney General, Consumer Protection Division, South Dakota Attorney General, 1302 E. Hwy. 14, Ste 1, Pierre, SD 57501-8501, 605-773-3215, Phil.Carlson@state.sd.us
Tennessee	Jeff Hill, Deputy Attorney General, Office of the Tennessee Attorney General, Consumer Protection and

	Advocate Division, UBS Tower, 315 Deaderick Street, Nashville, TN 37243, (615) 741-1671, Jeff.hill@ag.tn.gov
Texas	D. Esther Chavez, Senior Assistant Attorney General, Office of the Attorney General, Consumer Protection Division, P.O. Box 12548, Austin, Texas 78711, 512-475-4628, Esther.Chavez@oag.texas.gov
Vermont	Ryan Kriger, Assistant Attorney General, 109 State St., Montpelier, VT 05609, 802-828-3170, ryan.kriger@vermont.gov
Washington	Andrea M. Alegrett, Assistant Attorney General, 800 Fifth Avenue, Suite 2000, Seattle, WA 98104, 206-389-3813, andreaa1@atg.wa.gov

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

In Re: ROGER DEMAR	)	CIVIL DIVISION
D&R FAMILY PROPERTIES, LLC	)	Docket No. 643-11-17 Wncv
	)	

ASSURANCE OF DISCONTINUANCE

The State of Vermont, by and through Vermont Attorney General Thomas J. Donovan, Jr., and Roger Demar and D&R Family Properties, LLC ("Respondents"), hereby enter into this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

Regulatory Framework

1. Lead-based paint in housing, the focus of the Vermont lead law, is a leading cause of childhood lead poisoning, which can result in adverse health effects, including decreases in IQ.
2. All paint in pre-1978 housing is presumed to be lead-based unless a certified inspector has determined that it is not lead-based. 18 V.S.A. § 1759(a).
3. All paint in rental target housing is "presumed to be lead-based unless a lead inspector or lead risk assessor has determined that it is not lead-based." 18 V.S.A. § 1760(a).
4. The lead law requires that essential maintenance practices ("EMPs") specified in 18 V.S.A. § 1759 be performed at all pre-1978 rental housing.
5. EMPs include, but are not limited to, installing window well inserts, visually inspecting properties at least annually for deteriorated paint, restoring surfaces to be free of deteriorated paint within 30 days after such paint has been visually identified

or reported to the owner, and posting lead-based paint hazard information in a prominent place. 18 V.S.A. § 1759(a) (2), (4) and (7).

6. The EMP requirements also mandate that an owner of rental target housing file affidavits or compliance statements attesting to EMP performance with the Vermont Department of Health and with the owner's insurance carrier. 18 V.S.A. § 1759(b).
7. A violation of the lead law requirements may result in a maximum civil penalty of $10,000.00. 18 V.S.A. § 130(b)(6). Each day that a violation continues is a separate violation. 18 V.S.A. § 130(b)(6).
8. The Vermont Consumer Protection Act, 9 V.S.A Chapter 63, prohibits unfair and deceptive acts and practices, which includes the offering for rent, or the renting of, target housing that is noncompliant with the lead law.
9. Violations of the Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1). Each day that a violation continues is a separate violation.

Respondents' Rental Housing and Lead Compliance Practices

10. Respondents own sixteen rental properties located at: 35 East High Street (Morrisville); 612 VT Route 15 W (Morristown); 630 VT Route 15 W (Morristown); 2317 VT Route 15 (Hardwick); 40 Granite Street (Hardwick); 106 Church Street (Hardwick); 43 Glenside Avenue (Hardwick); 115 Glenside Avenue (Hardwick); 245 Lower Main Street (Johnson); 53 Gihon Lane (Johnson); 42 Upper French Hill Road (Johnson); 2681 Hogback Road (Johnson); 55 Gihon Lane (Johnson); 103 Gihon Lane (Johnson); 48 Granite Street (Hardwick); and 726 Route 100C (Johnson) all located in Vermont (collectively, "the Properties").

11. The Properties were all constructed prior to 1978, and therefore, are pre-1978 "rental target housing" within the meaning of the Vermont lead law, 18 V.S.A. § 1751(23), and are all subject to the requirements of 18 V.S.A. Chapter 38.

12. Respondents have in the past and continue presently to rent and offer for rent units in the Properties.

13. On January 5, 2017 and February 15, 2017, the Vermont Department of Health sent a "Notice of Non-Compliance" indicating that Respondents had not filed an "EMP Rental Property Compliance Statement" for several of the Properties. The Department allowed for 30 days for Respondents to file the necessary statements.

14. Respondents did not respond to the 30-day Notice, and did not file EMP compliance statements within 30 days.

15. On August 30, 2017, Respondents confirmed that nine rental properties were EMP compliant, but seven properties did not have not current EMP compliance statements. Respondents submitted a compliance plan to bring the seven properties into compliance and file EMP statements.

16. Respondents admit the facts described in ¶¶ 10-15.

The State's Allegations

17. The Vermont Attorney General's Office alleges the following violations of the Consumer Protection Act and Lead Law:

    a. Failing to file EMP compliance statements for rental properties.

18. The State of Vermont alleges that the above behavior constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

Assurances and Relief

In lieu of instituting an action or proceeding against Respondents, the Attorney General and Respondents are willing to accept this AOD pursuant to 9 V.S.A. § 2459. Accordingly, the parties agree as follows:

19. Respondents shall fully and timely comply with the requirements of the Vermont lead law, 18 V.S.A., Chapter 38, as long as they maintain any ownership or property management interest in the Properties and in any other pre-1978 rental housing in which they currently have, or later acquire, an ownership or property management interest.

20. Respondents shall complete all EMP inspections and work of the Properties (as specified in 18 V.S.A. § 1759) as described in Respondents' August 30, 2017 compliance plan, giving priority to the Properties where a child age 6 or under is residing. Pursuant to 18 V.S.A. § 1759(a)(3), exterior work of the Properties may be postponed until June 1, 2018, so long as access to exterior surfaces and components of the Properties with lead hazards and areas directly below the deteriorated surfaces are clearly restricted. All interior work must be completed promptly. If Respondents require additional time to complete the work, Respondents will contact the Attorney General's Office and provide a detailed justification for any extension.

21. Within one week of completion of the EMP work at the Properties described in the paragraph above, Respondents will file with the Vermont Department of Health, Respondents' insurance carrier and with the Office of the Attorney General, a completed EMP compliance statement for all Properties, and will give a copy of the compliance statement to an adult in each rented unit of all Properties. The copy for

the Office of the Attorney General shall be sent to: *Justin Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.*

22. In the event Respondents wish to rent a unit which becomes vacant in any of Respondents' pre-1978 rental housing before such housing is made EMP compliant, Respondents shall provide advance written notice of the intent to rent to the Office of the Attorney General at the address listed above. Respondents' advance written notice shall also: (1) verify that the interior of the specific unit to be rented is EMP compliant; (2) provide an update as to any remaining EMP work to be performed at the property, including the date by which the entire property will be EMP compliant. Otherwise, Respondents shall not rent, or offer for rent, any unit which becomes vacant in any of property owned or managed by Respondents that is not EMP compliant until such time as the EMP work is complete and the EMP compliance statement is distributed as described above.

23. Respondents shall pay the sum of $10,000 in civil penalties and costs for the failure to file EMP compliance statements, as follows:

    a. Respondents shall expend at least seven thousand dollars ($7,000), including the actual cost of materials and labor, on lead hazard reduction improvements at any or all of the Properties described herein;

    b. Respondents shall pay three thousand dollars ($3,000) by November 15, 2017, by a single check payable to "the State of Vermont" and sent to the following address: *Justin E. Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.*

24. Respondent shall pay the costs of any follow-up compliance inspections as determined by the Attorney General's Office.

Other Terms

25. This AOD is binding on Respondents, however, sale of any pre-1978 rental property may not occur unless Respondents have complied with all obligations under this AOD, or this AOD is amended in writing to transfer to the buyer or other transferee all remaining obligations.
26. Transfer of ownership of any of Respondents' pre-1978 rental properties shall be consistent with Vermont law, including the provisions of 18 V.S.A. § 1767 specifically relating to the transfer of ownership of pre-1978 rental housing.
27. This AOD shall not affect marketability of title.
28. Nothing in this AOD in any way affects Respondents' other obligations under state, local, or federal law.
29. In addition to any other penalties or relief which might be appropriate under Vermont law, any future failure by Respondents to comply with the terms of this AOD shall be subject to a liquidated civil penalty paid to the State of Vermont in the amount of at least $5,000 and not more than $10,000.

SIGNATURES APPEAR ON NEXT PAGE

DATED at Montpelier, Vermont this 2nd day of ~~October~~ November, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____

Justin E. Kolber
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-5620
justin.kolber@vermont.gov

DATED at Stowe, Vermont this 27 day of October, 2017.

ROGER DEMAR

By: _____

Roger Demar

DATED at Stowe, Vermont this 27 day of October, 2017.

D&R FAMILY PROPERTIES, LLC

By: _____

Roger Demar, authorized agent

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE: SAMANAGE SECURITY BREACH) CIVIL DIVISION
) Docket No. 555-9-17 Wncv.
)

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General Thomas J. Donovan, Jr. ("the Attorney General") and SAManage LTD. ("Respondent") hereby agree to this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

REGULATORY FRAMEWORK

1. Vermont's Consumer Protection Act prohibits "[u]nfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce." 9 V.S.A. § 2453.

2. Vermont's Security Breach Notice Act requires notice of security breaches to consumers and to the Attorney General, and requires contractors that maintain other businesses data to notify the business of data breaches affecting that data. 9 V.S.A. § 2435.

BACKGROUND

3. Respondent SAManage USA, Inc. ("Samanage") is a corporation incorporated under the laws of Israel and doing business as SAManage USA, Inc., incorporated under the laws of Delaware, with its principal place of business located at 117 Edinburgh South, Suite 100 Cary, NC 27511. Samanage provides business-support information technology ("IT") products and services.

4. Samanage provides a cloud-based IT support system which was used by WEX Health, Inc. ("WEX Health"), formerly Bennaissance, a contractor to the State of Vermont, for managing its IT help desk and maintenance tasks.

5. On June 2, 2016, a WEX Health employee attached a Microsoft Excel spreadsheet containing the names and social security numbers of 660 Vermonters (the "Spreadsheet") to a job ticket that was part of Samanage's cloud-based IT Support system.

6. The IT Support system communicated job tickets via a unique URL generated by a hash algorithm. Samanage did not authenticate the entity requesting information via the URL (by, for example, requesting a username and password). Anyone, anywhere, could theoretically guess the URL and type it into a standard web browser, and have access to the document.

7. In June or July 2016, a Microsoft Bing webcrawler discovered the URL and posted it to its search results. The Bing search results revealed not only the link to the spreadsheet, but previewed the contents of the spreadsheet. The search results themselves displayed the names and social security numbers of some of the Vermonters in the spreadsheet. This means that it was possible to view exposed social security numbers without clicking the link for the spreadsheet, making it impossible to know how many people actually saw the exposed data.

8. Vermont's Security Breach Notice Act defines "Personally Identifiable Information" ("PII") to include an individual's name combined with a social security number.
9 V.S.A. § 2430(5).

9. Vermont's Security Breach Notice Act defines "Security Breach" as "unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the data collector." 9 V.S.A. § 2430(8).

10. The exposure of the spreadsheet including the names and social security numbers of 660 Vermonters constituted a security breach.

11. In late July 2016, a Vermonter, while searching for her own name, came across this search result. The URL contained "AWS," indicating that it was on the Amazon Web Services platform. The Vermonter contacted Amazon and the Attorney General.

12. The Attorney General contacted Amazon to try to determine how the spreadsheet got posted and to assure it was taken down.

13. On July 25, 2016, Amazon emailed an engineer at Samanage to inform Samanage that PII that it had stored on its services was publicly accessible, and asking them to remove it. The engineer did not inform the appropriate personnel at Samanage that a security breach had occurred.

14. This notification triggered Samanage's duty to immediately investigate the breach, remediate it, and notify the owner of the data, WEX Health.

15. Samanage remediated the breach by changing the Spreadsheet's security settings to require authentication.

16. However, Samanage did not:

a. immediately require authentication of documents generally; or

b. notify WEX Health that its PII had been exposed.

17. Samanage is a "Data Collector" under Vermont's Security Breach Notice Act. The act distinguishes between Data Collectors who "own or license" and those who "maintain or possess" Personally Identifiable Information ("PII"). The former have a duty to notify the Attorney General within 14 days of notice or discovery of a breach, and consumers within 45 days of notice or discovery. The latter have a duty to notify the owner or licensor of the data "of the information of any security breach immediately following discovery of the breach." 9 V.S.A. § 2435(b)(2).

18. Samanage did not notify WEX Health of the security breach until late September 2016, shortly after the Attorney General, having obtained the information from Amazon, contacted Samanage about the breach.

19. WEX Health promptly issued notice to consumers and the Attorney General, in compliance with the law.

20. Absent intervention by the Attorney General, there is no indication that Samanage planned to inform anyone of the breach.

21. Samanage's delay caused Vermont consumers to learn that their social security numbers had been exposed almost two months later than they should have.

22. Respondent admits the truth of all facts set forth in the Background section.

23. Respondent complied with the Attorney General's investigative demands and inquiries in a timely manner, and worked with the Attorney General to efficiently resolve its enforcement action.

24. The Attorney General alleges that the above conduct constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453 and violations of the Security Breach Notice Act under 9 V.S.A § 2435.

INJUNCTIVE RELIEF

Information Security Program

25. **General Provisions:** Samanage shall implement and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Personally Identifiable Information, by no later than sixty (60) days after the date that this Assurance is filed with the court ("Effective Date"). Such program's content and implementation shall be fully documented and shall contain administrative, technical, and physical safeguards appropriate to the size and complexity of Samanage's operations, the nature

and scope of Samanage's activities, and the sensitivity of the Personally Identifiable Information Respondent collects, including:

a. The designation of an employee or employees to coordinate and be accountable for the Information Security Program.

b. The identification of material internal and external risks to the security, confidentiality, and integrity of Personally Identifiable Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (i) employee training and management; (ii) information systems, including network and software design, information processing, storage, transmission, and disposal; and (iii) prevention, detection, and response to attacks, intrusions, or other systems failures.

c. The design and implementation of reasonable safeguards to control the risks identified through risk assessment and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

d. The implementation and evaluation of any modification to Samanage's Information Security Program, in light of the results of the testing and monitoring of any material changes to Samanage's operations or business arrangements, or any other change in circumstances that Samanage knows or has reason to know may have a material impact on the effectiveness of its Information Security Program.

26. **Specific Provisions**: Without any party admitting that the following provisions alone amount to reasonable actions to protect Personally Identifiable Information in the future, Samanage shall, to the extent it has not already done so:

a. Segment appropriately those network-based portions of the Samanage's computer system that store, process, or transmit Personally Identifiable Information by firewalls, access controls, or other appropriate measures.

b. Implement security patching protocol for Samanage's computer system.

c. Use Virtual Private Networks ("VPNs") or other methods at least as secure as VPNs for transmission of Personally Identifiable Information across open, public networks.

d. Install and maintain appropriately configured and up-to-date anti-malware software on the Samanage's computer system.

e. Implement and maintain security monitoring tools, such as intrusion detection systems or other devices to track and monitor unauthorized access to the Samanage's computer system. Conduct quarterly testing and continual monitoring of the Samanage's computer system.

f. Implement access control measures for the portions of Samanage's computer system that store, process, and transmit Personally Identifiable Information. Access control measures include: (a) limiting physical and electronic access to Personally Identifiable Information on a need-to-know basis; (b) assigning unique user IDs to persons with access to Personally Identifiable Information; and (c) generating logs or other inventories of the user accounts on the portions

of Samanage's computer system used to store, process, or transmit Personally Identifiable Information.

g. Retain logs for at least 90 days online and one additional year offline.

h. Implement user authentication for all aspects of Samanage's systems that could be exposed to public access and that could possibly store or transmit Personally Identifiable Information.

Legal Compliance Program

27. Within 120 days of both Parties signing this AOD, Samanage shall engage in a full audit of its Legal Compliance Program to ensure that it is complying with all Vermont laws, including but not limited to 9 V.S.A. Chapters 62 and 63.

28. Samanage shall implement policies and procedures to ensure continued compliance with Vermont law.

29. This Legal Compliance Program shall include training as appropriate of all officers, managers, and employees of Samanage of their roles and responsibilities in ensuring that Samanage complies with the law.

30. All officers and managers of Samanage shall be provided with a copy of this Assurance of Discontinuance and be required to read the AOD as part of the Legal Compliance Program.

31. Samanage shall comply with all provisions of Vermont law, including but not limited to provisions of 9 V.S.A. Chapters 62 and 63.

PENALTIES

32. Respondents shall pay civil penalties of Two-Hundred and Sixty-Four Thousand Dollars ($264,000) within ten days of both Parties signing this AOD. Respondent shall make payment to the "State of Vermont" and send payment to: Ryan Kriger, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

33. Respondents shall be jointly responsible for the payment of the civil penalties.

REPORTING

34. To determine or secure compliance with this Assurance of Discontinuance, on reasonable notice given to Respondent, subject to any lawful privilege:

a. The Attorney General may request electronic copies of any correspondence, memoranda and other documents and records in the possession, custody, or control of Respondent that relate to the violations described in this Assurance of Discontinuance, and such documents shall be delivered to the Attorney General within 30 days or at a mutually agreed to time.

b. Respondent shall submit written reports, under oath if requested, with respect to any matters contained in this Assurance of Discontinuance.

OTHER TERMS

35. Respondents agree that this Assurance of Discontinuance shall be binding on Respondents, and their successors and assigns.

36. The Attorney General hereby releases and discharges any and all claims arising under the Security Breach Notice Act, 9 V.S.A. §§ 2430-35, and the Consumer Protection Act, 9 V.S.A. §§ 2451-2480, that it may have against Respondents for the conduct described in the Background section between the dates of January 1, 2016 and the Effective Date.

37. The Superior Court of the State of Vermont, Washington Unit, shall have jurisdiction over this Assurance and the parties hereto for the purpose of enabling the Attorney General to apply to this Court at any time for orders and directions as may be necessary or appropriate to enforce compliance with or to punish violations of this Assurance of Discontinuance.

38. Acceptance of this AOD by the Vermont Attorney General's Office shall not be deemed approval by the Attorney General of any practices or procedures of Respondent not required by this AOD, and Respondent shall make no representation to the contrary.

STIPULATED PENALTIES

39. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondent to be in violation of this Assurance of Discontinuance, then the parties agree that penalties to be assessed by the Court for each act in violation of this Assurance of Discontinuance shall be $10,000.

NOTICE

40. Respondents may be located at:

117 Edinburgh South

Suite 100

Cary, NC 27511

41. Respondents shall notify the Attorney General of any change of business name or address within 20 business days.

SIGNATURE

In lieu of instituting an action or proceeding against Respondents, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, Respondent voluntarily agrees with and submits to the terms of this Assurance of Discontinuance.

DATED at Cary, NC, this 25 day of September, 2017.

Samanage, Ltd.

By: _____

Itay Link
Chief Financial Officer

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 27 day of SEPTEMBER, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____

Ryan Kriger
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
802-828-3170

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE: KEVIN SPILLANE;)
LOWELL SPILLANE;)
SHIP SEVIN, LLC; and)
SHIP SEVIN II, LLC;)

CIVIL DIVISION
Docket No. 383-6-17 Wncv

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General Thomas J. Donovan Jr. ("the Attorney General") and Kevin Spillane; Lowell Spillane; Ship Sevin, LLC; and Ship Sevin II, LLC ("Respondents") hereby agree to this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

REGULATORY FRAMEWORK

1. The Vermont Consumer Protection Act prohibits "unfair or deceptive acts or practices in commerce." 9 V.S.A. § 2453(a).

2. The Vermont Consumer Protection Act authorizes the Attorney General to take actions to restrain unfair and deceptive acts in commerce. 9 V.S.A. §§ 2453, 2458.

3. Pursuant to 10 V.S.A. § 6205(a), "a mobile home park owner who violates or fails to comply with a provision of [Vermont's Mobile Home Parks law] violates 9 V.S.A. § 2453." Vermont's Mobile Home Parks law applies to both mobile home rentals and mobile home lot rentals. *See* 10 V.S.A. § 6201(5) (defining "'[l]easeholder'" as "a resident lawfully occupying a mobile home owned by the park owner or the owner of a mobile home sited on a mobile home lot in a mobile home park").

4. Similarly, landlord-tenant transactions governed by Vermont's Residential Rental Agreements Act, 9 V.S.A. chapter 137, are subject to the Vermont Consumer Protection Act. *See, e.g., Bisson v. Ward*, 160 Vt. 343, 348-50, 628 A.2d 1256, 1260-61 (Vt. 1993). Vermont's

Residential Rental Agreements Act applies to mobile home rentals to the extent that Act is consistent with Vermont's Mobile Home Parks law. 10 V.S.A. § 6204(c). Vermont's Residential Rental Agreements Act does not apply to mobile home lot rentals. 9 V.S.A. § 4452(6).

5. In relevant part, Vermont's Mobile Home Parks law provides that:

> (a) All terms governing the use and occupancy of a mobile home lot shall be contained in a written lease. Mobile home park owners shall promulgate reasonable and fair lease terms governing the use and occupancy of a mobile home lot and shall furnish an initial copy of the lease to leaseholders. . . . Any lease term which is not uniformly applied to all leaseholders of the same or a similar category shall be unenforceable. . . .
>
> (c) Prospective leaseholders shall be furnished with a copy of the proposed lease prior to any agreement to use or occupy a mobile home lot, and upon acceptance of the lease terms the lease shall be signed by the lessor and the lessee. . . .
>
> (e)(1) All mobile home lot leases shall contain . . . [r]ental and utility charges and other reasonable incidental service charges, if any. No charges other than properly disclosed charges for rent, utilities, or other reasonable incidental services may be imposed or collected. . . .
>
> (f) A copy of all new lease terms shall be furnished to all leaseholders at least 30 days prior to the effective date of any amendment, addition, or deletion of the existing lease terms. Upon request, the park owner shall provide to any leaseholder a copy of the current lease for his or her lot.

10 V.S.A § 6236(a), (c), (e)(1), and (f).

6. A corresponding agency rule provides that:

> 4.7(a) All mobile home park lot leases shall contain . . . [the] [a]mount and schedule for rental and utility charges and other reasonable incidental service charges, if any. Failure to include such charges in the lease shall prohibit a park owner from imposing or collecting the same. . . .
>
> 4.8 Any proposed new lease, lease amendment, addition to, or deletion from the lease shall be provided in writing to all residents at least thirty days in advance of the effective date of such change, and shall be signed by the park owner and leaseholder. If the leaseholder does not object in writing by the effective date, the leaseholder shall be deemed to have accepted the

> new or changed lease terms or new lease. Lot leases automatically renew unless superseded or replaced, or voided due to a termination or expiration of tenancy.

Agency of Commerce Community Development, Department of Economic, Housing and Community Development, Housing Division Rules, Part I: Mobile Home Parks ("Mobile Home Parks Rule"), §§ 4.7(a) and 4.8.

7. Pursuant to 9 V.S.A. § 4456a, which applies to mobile home rentals, "[a] landlord or a landlord's agent shall not charge an application fee to any individual in order to apply to enter into a rental agreement for a residential dwelling unit."

8. Similarly, pursuant to 10 V.S.A. § 6238(a), "[a] prospective leaseholder or other person may not be charged an entrance fee for the privilege of leasing or occupying a mobile home lot."

9. A corresponding agency rule provides that "[n]o park owner shall charge an entrance fee to a leaseholder or prospective leaseholder for the privilege of leasing or occupying a mobile home park lot." *Mobile Home Parks Rule, § 5.1.*

10. Violations of the Vermont Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1).

RESPONDENTS

11. Respondents Kevin Spillane and Lowell Spillane are Vermont residents.

12. Respondent Ship Sevin, LLC is a limited liability company incorporated under the laws of Vermont, with a Business ID of 0003706. Ship Sevin, LLC leases mobile homes, mobile home lots, and residential rental properties in Bennington, Caledonia, Chittenden, Lamoille, Rutland, and Washington Counties.

13. Respondent Ship Sevin II, LLC is a limited liability company incorporated under the laws of Vermont, with a Business ID of 0305584. Ship Sevin II, LLC leases mobile homes, mobile home

lots, and residential rental properties in Bennington, Caledonia, Chittenden, Lamoille, Rutland, and Washington Counties.

14. Respondents Lowell Spillane and Kevin Spillane are principals of Ship Sevin, LLC and Ship Sevin II, LLC.

BACKGROUND

15. Since January 1, 2011, Respondents Ship Sevin, LLC and Ship Sevin II, LLC have leased mobile homes, mobile home lots,[1] and other residential rental properties to at least 362 tenants.[2]

16. At the time Respondents purchased the mobile homes parks now owned by them, the previous owners assigned all existing mobile home leases to Respondents and provided them with copies of all existing leases except for at least four; however, the previous owners were unable to locate copies of every existing lease. Respondents mailed a new lease to all tenants shortly after purchasing the mobile home parks. Several tenants did not sign the new lease.

17. Despite the requirement that all reasonable incidental service charges be contained in the written lease, the following tenants were charged fees that were not properly disclosed in a written lease: (1) some tenants with unexpired leases with the previous owners that were assigned to Respondents, (2) some tenants without written leases associated with their tenancy, and (3) some tenants that signed the new lease provided to them by Respondents.

18. For example, Respondents charged numerous tenants without a written lease associated with their tenancy various fees, including late fees, administrative fees,[3] and legal fees. Additionally, Respondents charged at least 12 tenants with a written lease late fees of varying

---

[1] All references to "mobile home leases" or variations thereof include leases for the mobile home and mobile home lot, as well as leases for the mobile home lot only.

[2] This number encompasses many more individuals, as a single "tenant" may include multiple individuals living in the same property.

[3] Respondents provided the Attorney General with a letter stating that "administrative fees" consisted of the "handl[ing of] certain correspondence between Ship Sevin and various branches of the Vermont Superior Court along with various local Sheriff's Departments."

amounts, and at least 46 tenants with a written lease administrative fees of $100, none of which were disclosed by the tenants' respective written leases.

19. The 12 tenants referenced above were charged late fees of varying amounts despite the requirement that all lease terms be applied uniformly with respect to all leaseholders of the same or similar category.

20. Respondents also charged tenants leasing both mobile homes and other residential rental properties fees for lease violations that were neither reasonable nor fair. For example, Respondents charged tenants late fees that were not justified by the actual cost incurred by them.[4]

21. Additionally, the administrative fees charged by Respondents were unlawful because they were, in fact, legal fees charged to tenants prior to a court judgment. All legal fees charged to tenants prior to a court judgment, including service fees and attorney's fees, no matter how labeled, are prohibited by law.

22. Furthermore, since January 1, 2011, at least 75 tenants have been parties to mobile home leases or other residential rental property agreements with Respondents containing unlawful subtenant application fee or entrance fee provisions; such provisions are unlawful despite the fact that Respondents maintain that they never charged any such fees.

23. Respondents agree not to contest the truth of any facts set forth in the sections on Respondents and Background.

24. The Attorney General alleges that the above conduct constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

---

[4] Fees for lease violations, or "liquidated damages," must be reasonably related to the actual costs incurred by the landlord as a result of the lease violation. *Highgate Associates, Ltd. v. Merryfield*, 157 Vt. 313 (1991).

THIRD-PARTY ADMINISTRATOR

25. Respondents shall retain at their own expense an independent administrator to manage and oversee compliance with this AOD. The independent administrator shall not be a current or former employee of Ship Sevin, LLC; Ship Sevin II, LLC; or any other entity affiliated with any of the Respondents.

26. Within fifteen days of the effective date[5] of this AOD, Respondents shall submit to the Attorney General for approval the name, address, telephone number, email address, and resume of at least one proposed administrator who is willing to act as such, as well as three references for each proposed administrator.

27. Upon approval by the Attorney General, the administrator shall be responsible for administering the injunctive relief required by paragraphs 35-43, 45, and 48-50, as well as administering restitution, as described in paragraphs 51-53.

28. Respondents shall cooperate with the Administrator by giving him or her unfettered access to Respondents' paper and electronic files, computer system(s), and any other document or device necessary for the Administrator to carry out his or her duties. Respondents shall also not impede in any way the Administrator's ability to interview current or former tenants.

29. The Administrator shall submit to the Attorney General monthly reports on the fifth day of each month beginning 30 days after the effective date of this AOD, describing in detail (including names, dates, and dollar amounts, etc.) all actions that have been taken in the previous month to ensure compliance with this AOD, as well as certifying that Respondents have completed the actions required by paragraphs 35-39, 41-42, and 48-53. The Attorney General will work with the Administrator to develop a system of reporting that is as efficient as possible

[5] The "effective date" of this AOD is the date on which all parties, including the Attorney General, have signed on the signatures lines below.

for the Administrator.

INJUNCTIVE RELIEF

Violations of Vermont Law Prohibited

30. Respondents shall comply with all provisions of Vermont law, including the Vermont Consumer Protection Act, 9 V.S.A. chapter 63; the Vermont Mobile Home Parks law, 10 V.S.A. chapter 153; the Vermont Residential Rental Agreements Act, 9 V.S.A. chapter 137; and Part I of the Agency of Commerce and Community Development Housing Division Rules on Mobile Home Parks.

31. Respondents shall only impose or collect charges for rent, utilities, or other reasonable incidental services which are properly disclosed in a written mobile home lease.

32. All fees for lease violations charged to tenants leasing mobile homes, mobile home lots, and other residential rental properties shall be reasonably related to the actual cost that would be incurred by Respondents as a result of a violation of the lease.

33. Respondents shall not impose or collect charges for application fees or entrance fees from any current or prospective tenant, including subtenants.

34. Respondents shall also not impose or collect legal fees, including service fees and attorney's fees, no matter how labeled, from tenants prior to a court judgment.[6]

35. Within 20 days of the effective date of this AOD, Respondents shall provide all tenants currently leasing mobile homes or mobile home lots from Respondents with a copy of a proposed written lease that (1) complies with Vermont law; (2) discloses to tenants that legal fees, including service fees and attorney's fees, will not be imposed or collected prior to a court judgment; and (3) does not alter the material terms of the tenant's existing unexpired lease. The

[6] The requirement set forth in paragraph 34 is subject to changes in the law made by statute or the Vermont Supreme Court.

material terms of the tenant's existing unexpired lease include, but are not limited to, the lease term, the rental amount, and any term governing the tenant's ownership interest or potential ownership interest in the mobile home or mobile home lot. Lease terms relating to fees for "reasonable incidental services," such as late fees, are not material lease terms and shall be altered to comply with Vermont law.

36. The leases required by paragraph 35 shall be the same for all tenants of the same or a similar category in a given park.

37. Along with a copy of the proposed written lease, Respondents shall also provide all tenants referenced in paragraph 35 with a copy of a form letter, described in paragraph 46, stating that the tenant shall have 30 days from the date on which Respondents provide the tenant with a copy of the proposed written lease to accept its terms, and that if the tenant does not sign the proposed written lease within the 30-day period, Respondents may proceed according to the lease terms.

38. Respondents shall immediately void, waive, and/or rescind all unpaid fees charged to tenants except for any fees that (1) are lawful, (2) were justified by actual costs incurred by Respondents, and (3) were properly disclosed in the tenants' respective written leases.

Dismissal of Court Actions and Vacating of Court Judgments

39. For every pending eviction proceeding or other lawsuit filed against current or former tenants leasing mobile homes or mobile home lots in which Respondents are attempting to collect prohibited fees, Respondents shall file a motion to dismiss within 30 days of the effective date of this AOD.

40. The first report from the Administrator shall include the following information for each lawsuit described in paragraph 39:

a. the caption (name of the case) and the docket number; and

b. whether a motion to dismiss was filed, and if so, the date the motion to dismiss was filed.

41. Respondents shall file motions to vacate all court judgments, or portions of court judgments, entered against current or former tenants leasing mobile homes unless Respondents can prove, for each lawsuit, that the judgment was not based on any prohibited fees. The deadlines for filing all such motions to vacate are as follows:

a. within 30 days of the effective date of this AOD for any court judgment entered in 2016 or 2017;

b. within 60 days of the effective date of this AOD for any court judgment entered in 2015;

c. within 90 days of the effective date of this AOD for any court judgment entered in 2014; and

d. within 120 days of the effective date of this AOD for any court judgment entered in 2013 or earlier.

42. If a court judgment is vacated as a result of it being based on prohibited fees, Respondents shall, within 30 days of the court order vacating the judgment:

a. reimburse the tenant for all documented costs of the court action paid by the tenant to Respondents, including but not limited to attorney's fees and service or process fees;

b. take the necessary steps to remove any liens placed on the tenant's property;

c. reimburse the tenant for any portion of the vacated judgment that Respondents have collected, except for any amounts collected for delinquent rent;

d. if applicable, provide written notice of the vacated judgment to (1) the Vermont State Housing Authority, or (2) any other Public Housing Authority that Respondents accepted Section 8 Housing Choice Voucher payments from on behalf of a tenant; and

e. provide written notice to the tenant of the vacated judgment, and, if applicable, advising the tenant to contact their local Public Housing Authority to inquire about voucher or subsidy reinstatement.

43. Starting with the first report from the Administrator, each monthly report shall include the following information for each lawsuit in which a court has entered a judgment:

a. the caption (name of the case) and the docket number;

b. whether a motion to vacate was filed, and if so, the date the motion to vacate was filed;

c. if a motion to vacate was not filed within the timeframe set out in paragraph 40, a brief explanation of why the judgment was not based on any prohibited fees; and

d. whether no action has yet been taken by Respondents.

44. Upon request of the Attorney General, Respondents shall provide the documentary proof justifying the explanation required by paragraph 43 that no motion to vacate is required.

45. The monthly reports from the Administrator shall indicate all court rulings on any motion to dismiss or vacate, and the date of the ruling.

Form Letters

46. Within ten days of the effective date of this AOD, Respondents shall submit to the Attorney General for approval a form letter providing written notice to all tenants referenced in paragraph 35 informing them that they shall have 30 days to accept the terms of the leases

referenced in paragraph 35.

47. Within 30 days of the effective date of this AOD, Respondents shall submit to the Attorney General for approval the following form letters:

a. a form letter providing written notice to the major credit reporting agencies (Experian, TransUnion, and Equifax) of a vacated judgment, requesting that any negative reports be removed, and requesting verification to Respondents and the tenant that any negative reports have been removed;

b. a form letter directed to any collection agency, to which Respondents referred a court judgment, providing written notice of the vacated judgment, requesting that the collection agency not pursue the debt, and requesting verification to Respondents and the tenant of all amounts paid by the tenant to the collection agency and that the collection agency will not pursue the debt further;

c. a form letter directed to any credit reporting agency, to which Respondents submitted a negative report with respect to an unpaid fee that is prohibited by law, requesting that the negative report be removed, and requesting verification to Respondents and the tenant that any negative reports have been removed; and

d. a form letter directed to any collection agency, to which Respondents referred an unpaid fee that is prohibited by law, requesting that the collection agency not pursue the debt, and requesting verification to Respondents and the tenant that the collection agency will not pursue the debt further.

48. If a court judgment is vacated as a result of inclusion of prohibited fees, Respondents shall, within 30 days of the court order vacating the judgment, send via certified mail a separate form letter for each tenant to all applicable credit reporting agencies and collection agencies, and

copy the respective tenant on all such letters.

49. If any unpaid fee is voided, waived, and/or rescinded based on it being prohibited by law, Respondents shall, within 10 days of receiving approval by the Attorney General of the form letters referenced in paragraph 48 above, send via certified mail a separate form letter for each tenant to all applicable credit reporting agencies and collection agencies, and copy the respective tenant on all such letters.

Other Injunctive Relief

50. If Respondents referred any unpaid fee that is prohibited by law to a collection agency, Respondents shall reimburse the tenant for any documented amount paid to that collection agency by the tenant within 30 days of the effective date of this AOD.

RESTITUTION

51. Within 60 days of signing this AOD, Respondents shall refund by check all prohibited fees, with interest, including, but not limited to, legal fees, administrative fees, application or entrance fees, late fees in excess of $25, and any other fee not properly disclosed in a written lease, that were paid to Respondents by all current and former tenants. Notwithstanding the foregoing, Respondents may refund the amounts owed to tenants by crediting such amounts toward delinquent rent owed by such tenants; however, in any case where the amount (including interest) of delinquent rent credit exceeds the amount of delinquent rent owed, Respondents shall refund by check the excess amount of prohibited fees with applicable interest.

52. Interest shall be calculated based on the Federal Deposit Insurance Corporation's weekly national interest checking rate for non-jumbo deposits as of the effective date of this AOD. The independent administrator shall be responsible for determining all refund amounts. Payment shall be mailed to the tenant's last known address in an envelope provided by the Attorney

General's Office, along with an explanatory letter contained in Exhibit A. All checks shall be valid for 60 days.

53. On a monthly basis for all checks required by paragraph 51 above that were not cashed by the tenant or were returned to the Respondents at least 120 days prior to the end of the reporting period, the Administrator shall mail to Shannon Salembier, Assistant Attorney General, Office of the Vermont Attorney General, 109 State Street, Montpelier, VT 05609 the following:

a. a single check, payable to "Vermont State Treasurer" in the total dollar amount of all outstanding amounts and all checks that were returned as undeliverable or that went uncashed, to be treated as unclaimed funds;

b. a list, in electronic Excel format, of the tenants whose checks were returned or were not cashed (which list shall set out the first and last names of the tenants in distinct fields or columns), and for each such tenant, the last known address and dollar amount due; and

c. Ship Sevin, LLC and Ship Sevin II, LLC's corporate address and federal tax identification numbers.

PENALTIES

54. Respondents shall pay civil penalties of thirty thousand dollars ($30,000) within the following timeframe: twenty thousand dollars ($20,000) within 60 days of all Parties signing this AOD and the remaining ten thousand dollars ($10,000) within 120 days of all Parties signing this AOD. Respondents shall make payment to the "State of Vermont" and send payment to: Shannon Salembier, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

OTHER TERMS

55. Respondents agree that this AOD shall be binding on them, all of their affiliate companies engaged in the rental of mobile homes, mobile home lots, and other residential properties, their officers, directors, owners, managers, successors and assigns.

56. The Attorney General hereby releases and discharges any and all claims arising under the Consumer Protection Act, 9 V.S.A. chapter 63; the Vermont Mobile Home Parks law, 10 V.S.A. chapter 153; and the Vermont Residential Rental Agreements Act, 9 V.S.A. chapter 137, that it may have against Respondents and their agents, officers, and members for the conduct described in the Background section prior to the date of this AOD.

57. The Superior Court of the State of Vermont, Washington Unit, shall have jurisdiction over this AOD and the parties hereto for the purpose of enabling the Attorney General to apply to this Court at any time for orders and directions as may be necessary or appropriate to enforce compliance with, or to punish violations of, this AOD.

58. Respondents shall, upon request by the Attorney General, provide all documentation and information necessary for the Attorney General to confirm compliance with, and assist in implementation of, this AOD.

59. Respondents shall maintain in an electronic format all records created or utilized by the Administrator in carrying out his or her duties under this AOD for at least six years after all actions required by this AOD have been completed.

60. Acceptance of this AOD by the Attorney General shall not be deemed approval by the Attorney General of any practices or procedures of Respondents not required by this AOD, and Respondents shall make no representation to the contrary.

61. The requirement that Respondents refund all late fees charged to tenants in excess of $25 is for settlement purposes only and in lieu of requiring Respondents to determine the actual

administrative costs associated with every late fee charged by them. The Attorney General makes no representation as to what a reasonable late fee may be since that may vary depending on the individual facts and circumstances of a particular matter.

62. This AOD may be made effective in counterparts, and a facsimile or .pdf signature shall have the same force and effect as an original signature.

63. The undersigned authorized agent(s) of Respondents shall promptly take reasonable steps to ensure that copies of this document are provided to all relevant officers, directors, owners and managers of the company, and all of its affiliated companies engaged in the rental of mobile homes, mobile home lots, and other residential properties.

STIPULATED PENALTIES

64. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondents to be in violation of this AOD, then the parties agree that penalties to be assessed by the Court for each act in violation of this AOD shall be $5,000. This Section shall only apply if Respondents commit five or more separate violations of this AOD within one year.

NOTICE

65. All notices related to this AOD shall be given to:

a. Respondents at:

Ship Sevin, LLC
1700 Williston Road
South Burlington, VT 05403
802-651-3000

b. The Attorney General at:

Shannon Salembier
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609

802-828-5621
shannon.salembier@vermont.gov

66. Respondents shall notify the Attorney General of any change of business name, address or ownership or control within 20 business days.

67. In the event that any Respondent purchases a mobile home park or residential rental property after the execution date of this AOD, the Respondent shall within 20 business days notify the Attorney General of the address and provide a brief description of the property.

SIGNATURE

68. In lieu of instituting an action or proceeding against Kevin Spillane; Lowell Spillane; Ship Sevin, LLC; and Ship Sevin II, LLC, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, Respondents voluntarily agree with and submit to the terms of this Assurance of Discontinuance.

DATED at Montpelier, this 23rd day of June, 2017.

By: _____
Kevin Spillane

DATED at Montpelier, this 23rd day of June, 2017

By: _____
Lowell Spillane

DATED at Montpelier, this 23rd day of June, 2017

By: _____
Lowell Spillane, as Authorized Agent of Ship Sevin, LLC

DATED at Montpelier, this 23 day of June, 2017.

By: _____
Lowell Spillane, as Authorized Agent of Ship Sevin II, LLC

DATED at Montpelier, this 23rd day of June, 2017.

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 29th day of June, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN JR.
ATTORNEY GENERAL

By: _____

Shannon Salembier
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
shannon.salembier@vermont.gov
802-828-5621

Exhibit A

[DATE]

Re: Ship Sevin, LLC and Ship Sevin II, LLC settlement

Dear Vermont consumer:

You have been identified as a tenant of Ship Sevin, LLC or Ship Sevin II, LLC ("Ship Sevin") who was charged fees that are prohibited by Vermont law. As a result of a settlement with the Attorney General's Office, Ship Sevin is providing the enclosed payment to refund all fees and any interest that you paid.

For more information on the Vermont consumer protection rules or the terms of this settlement, please visit the Attorney General's Office website at ago.vermont.gov or call the Consumer Assistance Program at 800-649-2424 or 802-656-3183.

Sincerely,

Thomas J. Donovan Jr.
Attorney General

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE: TARGET CORPORATION SECURITY BREACH	))))	CIVIL DIVISION Docket No. 317-5-17 Wncv

ASSURANCE OF DISCONTINUANCE

This Assurance of Discontinuance is entered into by the Attorneys General of Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii[1], Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington and West Virginia, as well as the District of Columbia (referred to collectively as the "Attorneys General") and Target Corporation to resolve the Attorneys General's investigation into the security incident announced by Target on December 19, 2013 (collectively, the "Parties").[2]

[1] Hawaii is represented on this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity purposes, the entire group will be referred to as the "Attorneys General" or individually as "Attorney General" and the designations, as they pertain to Hawaii, refer to the Executive Director of the State of Hawaii's Office of Consumer Protection.

[2] The State of California is simultaneously negotiating a settlement in a form consistent with the requirements of California law. That settlement would incorporate the substantive terms of this Assurance of Voluntary Compliance; to the extent there are differences, the differences will be related to and/or arise from the differences in the form. Payment to the State of California pursuant to its settlement with TARGET will be a portion of the total paid to the Attorneys General as recited in paragraph 29.

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

I. INTRODUCTION

This Assurance constitutes a good faith settlement and release between TARGET and the Attorneys General of claims related to a data breach, publically announced by TARGET on December 19, 2013 and January 10, 2014, in which a person or persons gained unauthorized access to portions of TARGET'S computer systems that process payment card transactions at TARGET'S retail stores and to portions of TARGET'S computer systems that store TARGET customer contact information (such intrusion referred to as the "Intrusion").

II. DEFINITIONS

1. For the purposes of this Assurance, the following definitions shall apply:

   A. "Cardholder Data Environment" shall mean TARGET's technologies that store, process, or transmit payment card authentication data, consistent with the Payment Card Industry Data Security Standard ("PCI DSS").

   B. "Consumer" shall mean any individual who initiates a purchase of or purchases goods from a TARGET retail location; any individual who returns merchandise to a TARGET retail location; or any individual who otherwise provides Personal Information to TARGET in connection with any other retail transaction at a TARGET retail location.

   C. "Consumer Protection Acts" shall mean the State citation(s) listed in Appendix A.

D. "Effective Date" shall be the date on which TARGET receives a copy of this Assurance duly executed in full by TARGET and by each of the Attorneys General.

E. "Personal Information" shall mean the following:

i. For a Consumer that is a resident of a State that is a Party to this Assurance and that has a Consumer Protection Statute or Personal Information Protection Act, the data elements in the definitions of personal information as set forth in those Acts;

ii. For a Consumer that is a resident of a State that is a Party to this Assurance and that does not have a Consumer Protection Statute or Personal Information Protection Act, the Consumer's first name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number; (c) state-issued identification card number; or (d) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the Consumer's financial account; and

iii. For purposes of Paragraph 15, the first name or first initial and last name of a Consumer who is a resident of a State that is a Party to this Assurance in combination with any one or more of the following data elements that relate to such individual: (a) Social

Security number; (b) driver's license number; (c) state-issued identification card number; or (d) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the Consumer's financial account.

F. "Personal Information Protection Acts" shall mean the State citations listed in Appendix B.

G. "Security Breach Notification Acts" shall mean the State citations listed in Appendix C.

H. "TARGET" shall mean Target Corporation, its affiliates, subsidiaries and divisions, successors and assigns doing business in the United States.

I. "Security Event" shall mean any potential compromise to the confidentiality, integrity, or availability of a TARGET information asset that includes Personal Information.

III. APPLICATION

2. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to TARGET, its affiliates, subsidiaries, successors and assigns, and its officers and employees.

IV. ASSURANCES

3. TARGET shall comply with the Consumer Protection Statutes and the Personal Information Protection Acts in connection with its collection, maintenance, and safeguarding of Personal Information.

4. TARGET shall not misrepresent the extent to which TARGET maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information collected from or about Consumers.

5. TARGET shall comply with the Security Breach Notification Acts. For any future breach of security involving the unauthorized access to or acquisition of Personal Information identified in Paragraph 1(E)(ii) and relating to a Consumer who is a resident of New Mexico or South Dakota, TARGET shall provide notice to such Consumer and the New Mexico and/or South Dakota Attorney General's Office, as relevant, except that notice shall not be required if TARGET reasonably determines that there is not a reasonable likelihood that harm to the Consumer will result from the incident. To the extent that New Mexico or South Dakota enact a security breach notification law following the Effective Date, TARGET shall comply with such law in lieu of the requirement of the preceding sentence.

A. INFORMATION SECURITY PROGRAM

6. TARGET shall, within one hundred and eighty (180) days after the Effective Date of this Assurance, develop, implement, and maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information it collects or obtains from Consumers.

7. TARGET's Information Security Program shall be written and shall contain administrative, technical, and physical safeguards appropriate to:

A. The size and complexity of TARGET's operations;

B. The nature and scope of TARGET's activities; and

C. The sensitivity of the Personal Information that TARGET maintains.

8. TARGET may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Assurance through review, maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that such existing information security program and existing safeguards meet the requirements set forth herein.

9. TARGET shall employ an executive or officer with appropriate background or experience in information security who shall be responsible for implementing and maintaining the Information Security Program.

10. TARGET shall ensure that the role of the designated executive or officer, referenced in Paragraph 9, includes advising the Chief Executive Officer and the Board of Directors of TARGET'S security posture, security risks faced by TARGET, and security implications of TARGET'S decisions.

11. TARGET shall ensure that its Information Security Program receives the resources and support reasonably necessary to ensure that the Information Security Program functions as intended by this Assurance.

B. ADMINISTRATIVE SAFEGUARDS

12. TARGET shall develop, implement, and revise as necessary written, risk-based policies and procedures for auditing vendor compliance with TARGET's Information Security Program.

13. TARGET's Information Security Program shall be designed and implemented to ensure the appropriate handling and investigation of Security Events involving Personal Information.

14. TARGET shall make reasonable efforts to maintain and support the software on its networks, taking into consideration the impact an update will have on data security in the context of TARGET's overall network and its ongoing business and network operations, and the scope of the resources required to address an end-of-life software issue.

15. TARGET shall maintain encryption protocols and related policies that are reasonably designed to encrypt Personal Information identified in Paragraph 1(E)(iii) that TARGET stores on desktops located within the Cardholder Data Environment, and shall encrypt the data elements of Personal Information identified in Paragraph 1(E)(iii), as well as any other data elements required by state law to be so encrypted, that are:

A. Stored on laptops or other portable devices; or

B. Transmitted wirelessly or across public networks.

16. TARGET shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") with respect to its Cardholder Data Environment, as defined in this Assurance, and any TARGET system component the compromise of which TARGET should reasonably believe would impact the security of the Cardholder Data Environment.

C. SPECIFIC SAFEGUARDS

17. Segmentation:

A. TARGET shall take reasonable, risk-based steps to scan and map the connections between its Cardholder Data Environment and the rest of its computer network in order to determine avenues of traffic to the Cardholder Data Environment and to identify and assess potential penetration vulnerabilities to the Cardholder Data Environment.

B. TARGET's Cardholder Data Environment shall be segmented from the rest of the TARGET computer network.

C. TARGET shall develop and implement a risk-based penetration testing program reasonably designed to identify, assess, and remediate penetration vulnerabilities within TARGET's computer network.

18. Access Control and Management:

A. TARGET shall implement and maintain appropriate risk-based controls to manage access to, and use of, TARGET's individual accounts, TARGET's service accounts, and vendor accounts, including strong passwords and password-rotation policies.

B. TARGET shall evaluate, and as appropriate, restrict and/or disable all unnecessary network programs that provide access to TARGET's Cardholder Data Environment and/or to any TARGET system component the compromise of which TARGET reasonably believes would also impact the security of the Cardholder Data Environment.

C. TARGET shall adopt a reasonable and risk-based approach to integrate two-factor authentication into TARGET's individual accounts, TARGET's administrator accounts, and vendor accounts.

19. File Integrity Monitoring: TARGET shall deploy and maintain controls, including, but not limited to, a file integrity monitoring solution, designed to notify personnel of unauthorized modifications to critical applications or operating system files within the Cardholder Data Environment.

20. Whitelisting: TARGET shall deploy and maintain controls, such as, for example, an application whitelisting solution, designed to detect and/or prevent the execution of unauthorized applications within its point-of-sale terminals and in-store point-of-sale servers.

21. Logging and Monitoring:

A. TARGET shall, to the extent technically feasible, implement reasonable controls to manage the access of any device attempting to connect to the Cardholder Data Environment, through hardware or software tools such as firewalls, authentication credentials, or other such access restricting mechanisms.

B. TARGET shall maintain an appropriate system to collect logs and monitor network activity, such as through the use of a security information and event management tool.

22. Change Control: TARGET shall develop and maintain policies and procedures with respect to managing and documenting changes to network systems.

23. Development: TARGET shall take steps reasonably designed to appropriately maintain the separation of development and production environments.

24. Payment Card Security: TARGET shall implement where appropriate steps designed to reasonably manage the review and, where reasonable and appropriate, the adoption of improved, industry-accepted payment card security technologies relevant to TARGET'S business and Cardholder Data Environment, such as chip and PIN technology.

25. Devalue Payment Card Information: TARGET shall make reasonable efforts to devalue payment card information, including, but not limited to, encrypting payment card information throughout the course of a retail transaction at a TARGET retail location.

V. SETTLEMENT COMPLIANCE ASSESSMENT

26. TARGET shall obtain an information security assessment and report from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), within one (1) year after the Effective Date of this Assurance. The Third-Party Assessor's report on the Third-Party Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards maintained by TARGET;

B. Explain the extent to which such safeguards are appropriate in light of TARGET's size and complexity, the nature and scope of TARGET's activities, and the sensitivity of the Personal Information maintained by TARGET;

C. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program; and

D. Identify TARGET's Qualified Security Assessor for purposes of PCI DSS compliance.

27. TARGET's Third-Party Assessor shall be: (a) a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and (b) have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

VI. SUBMISSION TO ATTORNEYS GENERAL

28. TARGET shall provide a copy of the Third-Party Assessor's report on the Third-Party Assessment to the Connecticut Attorney General's Office within one hundred and eighty (180) days of the completion of the report.

A. Confidentiality: The Connecticut Attorney General's Office shall treat the Third-Party Assessment report as exempt from disclosure under the relevant public records laws, pursuant to this Assurance or, as necessary, by employing other means to ensure confidentiality.

B. State Access to Report: The Connecticut Attorney General's Office may provide a copy of the report on Third-Party Assessment received from TARGET to any other of the Attorneys General upon request, and each requesting Attorney General shall, to the extent permitted by the laws of the Attorney General's State, treat such report as exempt from disclosure under the relevant public records laws.

VII. PAYMENT TO THE STATES

29. TARGET shall pay Eighteen Million Five Hundred Thousand Dollars ($18,500,000) to the Attorneys General. Said payment shall be divided and paid by TARGET directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to TARGET by the Illinois Attorney General and Connecticut Attorney General. Each of the Attorneys General agrees that the Illinois Attorney General and Connecticut Attorney General have the authority to designate such amount to be paid by TARGET to each Attorney General and to provide TARGET with instructions for the payments to be distributed

under this Paragraph. Payment shall be made no later than thirty (30) days after the Effective Date of this Assurance and receipt of such payment instructions by TARGET from the Illinois Attorney General and Connecticut Attorney General, except that where state law requires judicial or other approval of the Assurance, payment shall be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

30. Said payment shall be used by the Attorneys General for such purposes that may include, but are not limited to, attorneys' fees and other costs of investigation, or to be placed in, or applied to, the consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the Attorneys General.

VIII. RELEASE AND EXPIRATION

31. Following full payment of the amounts due under this Assurance, the Attorneys General shall release and discharge TARGET from all civil claims that the Attorneys General could have brought under the Consumer Protection Acts, the Personal Information Protection Acts, and the Security Breach Notification Acts based on TARGET's conduct related to the Intrusion. Nothing contained in this paragraph shall be construed to limit the ability of the Attorneys General to enforce the obligations that TARGET has under this Assurance. Further, nothing in this Assurance shall be construed to create, waive, or limit any private right of action.

32. The obligations and other provisions of this Assurance set forth in paragraphs 9, 10, 15, 16, 17.A., 17.B., 18, 19, 20, and 23 shall expire at the conclusion of the five (5) year

period after the Effective Date of this Assurance, unless they have expired at an earlier date pursuant to their specific terms. Provided, however, that nothing in this paragraph should be construed or applied to excuse TARGET from its obligation to comply with all applicable state and federal laws, regulations, and rules.

IX. MEET AND CONFER

33. If any Attorney General determines that TARGET has failed to comply with any of the terms of this Assurance, and if in the Attorney General's sole discretion the failure to comply does not threaten the health or safety of the citizens of the Attorney General's State and/or does not create an emergency requiring immediate action, the Attorney General will notify TARGET in writing of such failure to comply and TARGET shall have thirty (30) days from receipt of such written notice to provide a good faith written response to the Attorney General's determination. The response shall include: (A) a statement explaining why TARGET believes it is in full compliance with this Assurance; or (B) a detailed explanation of how the alleged violation(s) occurred, and (i) a statement that the alleged violation has been addressed and how, or (ii) a statement that the alleged violation cannot be reasonably addressed within thirty (30) days from receipt of the notice, but (a) TARGET has begun to take corrective action(s) to address the alleged violation, (b) TARGET is pursuing such corrective action(s) with reasonable diligence, and (c) TARGET has provided the Attorney General with a reasonable timetable for addressing the alleged violation.

34. Nothing herein shall prevent an Attorney General from agreeing in writing to provide TARGET with additional time beyond the thirty (30) day period to respond to the notice provided under Paragraph 33.

35. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Assurance after the Effective Date, or to compromise the authority of an Attorney General to initiate a proceeding for any failure to comply with this Assurance.

X. PRESERVATION OF AUTHORITY

36. Nothing in this Assurance shall be construed to limit the authority or ability of an Attorney General to protect the interests of his/her State or the people of his/her State. This Assurance shall not bar the Attorney General or any other governmental entity from enforcing laws, regulations, or rules against TARGET for conduct subsequent to or otherwise not covered by this Assurance. Further, nothing in this Assurance shall be construed to limit the ability of the Attorney General to enforce the obligations that TARGET has under this Assurance.

XI. GENERAL PROVISIONS

37. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Attorneys General of TARGET's business practices, nor shall TARGET represent that this Assurance constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Attorneys General to take any action in response to any information submitted pursuant to this Assurance shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.

38. Nothing in this Assurance shall be construed as relieving TARGET of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Assurance be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

39. TARGET shall deliver a copy of this Assurance to, or otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, the executive or officer of Paragraph 9, and General Counsel, and its Board of Directors within ninety (90) days of the Effective Date. TARGET shall deliver a copy of this Assurance to, or otherwise fully apprise, any new Chief Executive Officer, new Chief Information Officer, new Chief Information Security Officer, new executive or officer of Paragraph 9, and new General Counsel, and each new member of its Board of Directors, within ninety (90) days from which such person assumes his/her position with TARGET.

40. To the extent that there are any, TARGET agrees to pay all court costs associated with the filing (if legally required) of this Assurance. No court costs, if any, shall be taxed against any Attorney General.

41. TARGET shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Assurance or for any other purpose that would otherwise circumvent any term of this Assurance. TARGET shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Assurance.

42. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

43. TARGET agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and TARGET further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

44. This Assurance shall not be construed to waive any claims of sovereign immunity the States may have in any action or proceeding.

XII. SEVERABILITY

45. If any clause, provision, or section of this Assurance shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Assurance and this Assurance shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

XIII. NOTICE/DELIVERY OF DOCUMENTS

46. Whenever TARGET shall provide notice to the Attorneys General under this Assurance, that requirement shall be satisfied by sending notice to the Designated Contacts on behalf of the Attorneys General listed in Appendix D. Any notices or other documents sent to TARGET pursuant to this Assurance shall be sent to the following address: (1) Target Corporation, ATTN: General Counsel, 1000 Nicollet Mall, Minneapolis, MN 55403; and (2) Nathan Taylor, Morrison & Foerster LLP, 2000 Pennsylvania Ave., NW, Suite 6000, Washington DC 20006. All notices or other documents to be provided under this Assurance shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person

signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its address by sending written notice to the other party.

SIGNATURE

In lieu of instituting an action or proceeding against Respondent, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, Respondent voluntarily agrees with and submits to the terms of this Assurance of Discontinuance.

DATED at Minneapolis, MN, this 15th day of May, 2017.

TARGET CORPORATION

By: _____
Carter Leuty
Vice President, Law
TARGET CORPORATION

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 9 day of May, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____
Ryan Kriger
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
(802) 828-3170

Appendix A.

STATE	CONSUMER PROTECTION ACTS
Alaska	Alaska Unfair Trade Practices and Consumer Protection Act, AS 45.50. 471 et seq.
Arizona	Arizona Consumer Fraud Act, A.R.S. §§ 44-1521 – 44-1534
Arkansas	Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101 et seq.
Colorado	Colorado Consumer Protection Act, C.R.S. § 6-1-101 et seq.
Connecticut	Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110a, et seq.
District of Columbia	Consumer Protection Procedures Act, D.C. Code, § 28-3901, et seq.
Delaware	Consumer Fraud Act, 6 Del.C. § 2511, et al.; Uniform Deceptive Trade Practices Act, 6 Del.C. § 2531, et al.
Florida	Florida Deceptive and Unfair Trade Practices Act, § 501.201 et seq., Fla. Stat.
Georgia	Fair Business Practices Act, O.C.G.A. § 10-1-390 through 408
Hawaii	Uniform Deceptive Trade Practice Act- Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Sect. 480-2
Idaho	Idaho Consumer Protection Act, title 48, chapter 6, Idaho Code
Illinois	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*
Indiana	Deceptive Consumer Sales Act; Indiana Code chapter 24-5-0.5
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16
Kansas	Kansas Consumer Protection Act K.S.A 50-623 et al.
Kentucky	Kentucky Consumer Protection Act, Ky. Rev. Stat. 367.110-.300
Louisiana	Unfair Trade Practices and Consumer Protection Law, LA. Rev. Stat. 51:1401, et seq.
Maine	Maine Unfair Trade Practices Act, 5 M.R.S. § 205-A et seq.
Maryland	Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101, et seq. (2013 Repl. Vol and 2016 Supp.)

Appendix A.

Massachusetts	Massachusetts Consumer Protection Act (Mass. Gen. Laws ch. 93A)
Michigan	Michigan Consumer Protection Act, Mich. Comp. Laws §§ 445.901, *et seq.*
Minnesota	Minnesota Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43-.48; and Minnesota Prevention of Consumer Fraud Act, Minn Stat. § 325F.68-.69 and .70
Mississippi	Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1 *et seq.*
Missouri	Missouri Merchandising Practices Act, Chapter 407, RSMo.
Montana	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-101 et seq.
Nebraska	Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601 et seq., and Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 et seq.
Nevada	Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903-598.0999
New Hampshire	NH RSA 358-A
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq.
New Mexico	Unfair Practices Act (UPA) NMSA 1978 Section 57-12-1 *et seq*
New York	Executive Law 63(12), General Business Law 349 and 350
North Carolina	North Carolina Unfair and Deceptive trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, et seq.
North Dakota	N.D.C.C. ch. 51-15 (§51-15-02); Unlawful Sales or Advertising Practices
Ohio	Consumer Sales Practices Act, R.C. 1345.01 et seq.
Oklahoma	Oklahoma Consumer Protection Act, 15 O.S. §§ 751 *et seq.*
Oregon	Unlawful Trade Practices Act, ORS 646.605 et seq.
Pennsylvania	Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, et seq.
Rhode Island	Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1, *et seq.*
South Carolina	South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-10, et seq.

Appendix A.

South Dakota	South Dakota Codified Laws (SDCL) Chapter 37-24
Tennessee	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 et seq.
Texas	Texas Deceptive Trade Practices Act, Tex. Bus. & Com. Code Ann. § 17.41 (West 2011)
Utah	Utah Consumer Sales Practices Act, Utah Code § 13-11-1 *et seq.*
Vermont	Vermont Consumer Protection Act, 9 V.S.A. § 2453
Virginia	Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207
Washington	Consumer Protection Act, RCW 19.86.020
West Virginia	West Virginia Consumer Credit and Protection Act ("WVCCPA"), W. Va. Code § 46A-1-101, et al.

Appendix B.

STATE	PERSONAL INFORMATION PROTECTION ACTS
Alaska	Alaska Personal Information Protection Act, AS 45.48.010 et seq.
Arkansas	Personal Information Protection Act, Ark. Code Ann. § 4-110-101 et seq.
Colorado	Colorado Consumer Protection Act, C.R.S. § 6-1-101 et sec.; Notification of Security Breach, C.R.S. § 6-1-716
Connecticut	Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
Florida	Florida Information Protection Act, § 501.171, Fla. Stat.
Georgia	Georgia Personal Identity Protection Act, O.C.G.A § 10-1-910 through 915
Hawaii	Personal Information Protection – Haw. Rev. Stat. Chpt. 487J
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.*
Indiana	Disclosure of Security Breach Act; Indiana Code section 24-4.9-3-3.5
Kansas	Wayne Owen Act K.S.A. 50-6,139b
Maryland	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501, et seq. (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 C.M.R. 17.00 et seq.)
Minnesota	Minnesota Use of Social Security Numbers Statute, Minn. Stat. § 325E.59; and Minnesota Access Devices Statute, Minn. Stat. § 325E.64
Missouri	Missouri Merchandising Practices Act, Section 407.1500.1(9)
Montana	Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1701 et seq.
Nevada	Nevada Security of Personal Information Act; Nev. Rev. Stat. §§ 603A.010, et seq.
North Carolina	North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-60, et seq.
North Dakota	N.D.C.C. ch. 51-13: Notice of Security Breach for Personal Information
Oregon	Oregon Consumer Identity Theft Protection Act, ORS 646A.600 et seq.
Rhode Island	Rhode Island Identity Theft Protection Act, R.I. Gen. Laws § 11-49.3-1, *et seq.*

Appendix B.

South Carolina	The Family Privacy Protection Act, S.C. Code Ann. § 30-2-10, *et seq.*
Texas	Texas Identify Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. Ch. 521 (West 2015)
Utah	Protection of Personal Information Act, Utah Code § 13-44-101 *et seq.*
West Virginia	W. Va. Code § 46A-2A-101, et al.

Appendix C.

STATE	SECURITY BREACH NOTIFICATION ACTS
Alaska	Alaska Breach of Security Involving Personal Information statutes, AS 45.48.010-45.48.090
Arizona	Notification of Breach of Security System, A.R.S. § 18-545
Arkansas	Disclosure of Security Breaches, Ark. Code Ann. § 4-110-105
Colorado	Colorado Consumer Protection Act; Notification of Security Breach § 6-1-716
Connecticut	Breach of Security re Computerized Data Containing Personal Information, Conn. Gen. Stat. § 36a-701b
District of Columbia	Security Notification Act, D.C. Code § 28-3851, *et seq.*
Delaware	6 *Del.C.* § 12B-101, *et al.*
Florida	Florida Information Protection Act, § 501.171, Fla. Stat.
Georgia	Georgia Personal Identity Protection Act, O.C.G.A. § 10-1-910 through 915
Hawaii	Security Breach of Personal Information- Haw. Rev. Stat. Chpt. 487N
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.*
Indiana	Disclosure of Security Breach Act; Indiana Code article 24-4.9
Iowa	Iowa Personal Information Security Breach Protection Act, Iowa Code § 715C
Kansas	K.S.A 50-7a01 et al.
Kentucky	Ky. Rev. Stat. 365.732
Louisiana	Database Security Breach Notification Law, La. Rev. Stat. 51:3071, et seq., and Reporting Requirements, La. Admin. Code tit. 16, pt. 3, §701.
Maine	Maine Notice of Risk to Personal Data Act, 10 M.R.S. § 1346, et seq.
Maryland	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501, et seq. (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Massachusetts Security Breach Law (Mass. Gen. Laws ch. 93H)
Michigan	Identity Theft Protection Act, Mich. Comp. Laws §§ 445.61, et *seq.*
Minnesota	Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61

Appendix C.

Mississippi	Notice of Breach of Security, Miss. Code Ann. § 75-24-29
Missouri	Missouri Merchandising Practices Act, Section 407.1500, RSMo.
Montana	Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1704.
Nebraska	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 et seq.
Nevada	Nev. Rev. Stat. § 603A.220 (located within the Nevada Security of Personal Information Act)
New Hampshire	NH RSA 359-C: 19-21
New Jersey	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
New York	The New York State Information Security Breach and Notification Act (General Business Law 899-aa)
North Carolina	North Carolina Identity Theft Protection Act, Protection from security breaches, N.C. Gen. Stat. § 75-65
North Dakota	N.D.C.C. ch. 51-13: Notice of Security Breach for Personal Information
Ohio	"Private disclosure of security breach of computerized personal information data", R.C. 1349.19 et seq.
Oklahoma	Security Breach Notification Act, 24 O.S. §§ 161 *et seq.*
Oregon	Oregon Consumer Identity Theft Protection Act, ORS 646A.600 et seq.
Pennsylvania	Breach of Personal Information Notification Act, 73 P.S. §§ 2301, et seq.
Rhode Island	Rhode Island Identity Theft Protection Act, R.I. Gen. Laws § 11-49.3-4
South Carolina	The South Carolina Identity Fraud and Identity Theft Protection Act, S.C. Code Ann. § 1-11-490, et seq.
Tennessee	Tenn. Code Ann. § 47-18-2107 (this statute is within the Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 et seq.)
Texas	Texas Identify Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. Ch. 521(West 2015)
Utah	Protection of Personal Information Act, Utah Code § 13-44-101 *et seq.*

Appendix C.

Vermont	Vermont Security Breach Notice Act, 9 V.S.A. § 2435
Virginia	Virginia Code § 18.2-186.6
Washington	Data Breach Notification Law, RCW 19.255.010
West Virginia	WVCCPA, Breach of Security of Consumer Information, W. Va. Code § 46A-2A-101, et al.

Appendix D.

STATE	ATTORNEYS GENERAL DESIGNATED CONTACTS
Alaska	Davyn Williams Assistant Attorney General Alaska Office of the Attorney General 1031 W. 4th Ave, Suite 200 Anchorage, AK 99501 davyn.williams@alaska.gov (907) 375-7778
Arizona	Taren Ellis Langford Unit Chief Counsel Arizona Attorney General's Office 400 W. Congress Street, Suite S-315 Tucson, AZ 85701 Taren.Langford@azag.gov (520) 628-6631
Arkansas	Peggy Johnson Assistant Attorney General Office of the Arkansas Attorney General 323 Center Street, Suite 500 Little Rock, Arkansas 72201 peggy.johnson@arkansasag.gov (501) 682-8062
Colorado	Jay Simonson First Assistant Attorney General Colorado Attorney General's Office 1300 Broadway 7th Fl. Denver CO 80203 jay.simonson@coag.gov (720) 508-6205
Connecticut	Matthew F. Fitzsimmons Assistant Attorney General Department Head Privacy and Data Security Department Office of the Attorney General 110 Sherman Street Hartford CT 06105 Matthew.Fitzsimmons@ct.gov (860) 808-5515
District of Columbia	Philip Ziperman Director, Office of Consumer Protection Office of the District of Columbia Attorney General 441 – 4th Street, N.W., 6th Floor Washington, DC 20001 philip.ziperman@dc.gov (202) 442-9886

Appendix D.

Delaware	Stephen McDonald Deputy Attorney General Delaware Department of Justice 820 N. French St., 5th Floor Wilmington, DE 19801 Stephen.McDonald@state.de.us (302) 577-8513
Florida	Patrice Malloy Chief, Multi-State and Privacy Bureau Sr. Assistant Attorney General Office of the Attorney General 110 S.E. 6th Street Fort Lauderdale, FL 33301 Patrice.Malloy@myfloridalegal.com (954) 712-4669
Georgia	Daniel S. Walsh Senior Assistant Attorney General Department of Law State of Georgia 40 Capitol Square, SW Atlanta, Georgia 30334-1300 dwalsh@law.ga.gov (404) 657-2204
Hawaii	Lisa P. Tong Enforcement Attorney State of Hawaii Office of Consumer Protection 235 S. Beretania Street #801 Honolulu, Hawaii 96813 ltong@dcca.hawaii.gov (808) 586-5978
Idaho	Stephanie Guyon Deputy Attorney General Idaho Attorney General's Office Consumer Protection Division 954 W. Jefferson Street, 2nd FL. Boise, ID 83702 stephanie.guyon@ag.idaho.gov (208) 334-4135
Illinois	Matthew W. Van Hise, CIPP/US Assistant Attorney General Consumer Privacy Counsel Consumer Fraud Bureau Illinois Attorney General's Office 500 South Second Street Springfield, IL 62706 mvanhise@atg.state.il.us (217) 782-9024

Appendix D.

Indiana	Ernâni Magalhães Deputy Attorney General Consumer Protection Division Office of Attorney General Curtis Hill 302 West Washington Street IGCS-5th Floor Indianapolis, IN 46204 ernani.magalhaes@atg.in.gov (317) 234-6681
Iowa	Nathan Blake Assistant Attorney General Office of the Attorney General of Iowa 1305 E. Walnut St. Des Moines, IA 50319 nathan.blake@iowa.gov (515) 281-4325
Kansas	Sarah M. Dietz Assistant Attorney General Office of Kansas Attorney General Derek Schmidt 120 SW 10th Avenue, 2nd Floor sarah.dietz@ag.ks.gov (785) 296-3751
Kentucky	Kevin R. Winstead Assistant Attorney General Kentucky Attorney General's Office of Consumer Protection 1024 Capital Center Dr., #200 Frankfort, KY 40601 kevin.winstead@ky.gov (502) 696-5379
Louisiana	L. Christopher Styron Section Chief - Consumer Protection Assistant Attorney General Louisiana Department of Justice 1885 N. Third Street Baton Rouge, Louisiana 70802 styronl@ag.louisiana.gov (225) 326-6468
Maine	Christina Moylan Assistant Attorney General Maine Office of the Attorney General Cross State Office Building, 6th Floor 109 Sewall St. 6 State House Station Augusta, Maine 04333-0006 christina.moylan@maine.gov (207) 626-8838

Appendix D.

Maryland	Richard Trumka Jr. Assistant Attorney General Consumer Protection Division Office of the Attorney General 200 St. Paul Pl. Baltimore, MD 21202 rtrumka@oag.state.md.us (410) 576-6957
Massachusetts	Sara Cable Director, Data Privacy & Security Assistant Attorney General Consumer Protection Division Office of Attorney General Maura Healey Commonwealth of Massachusetts One Ashburton Place Boston MA 02108 sara.cable@state.ma.us (617) 963-2827
Michigan	Mark Gabrielse Assistant Attorney General Michigan Department of Attorney General Corporate Oversight Division P.O. Box 30755 Lansing, MI 48909 gabrielsem@michigan.gov (517) 373-1160
Minnesota	David Cullen Assistant Attorney General Minnesota Attorney General's Office 445 Minnesota Street, Suite 1400 St. Paul, MN 55101 David.Cullen@ag.state.mn.us (651) 757-1221
Mississippi	Crystal Utley Secoy Special Assistant Attorney General Consumer Protection Division Mississippi Attorney General's Office Post Office Box 22947 Jackson, Mississippi 39225 cutle@ago.state.ms.us (601) 359-4213

Appendix D.

Missouri	Joyce Yeager Assistant Attorney General Consumer Protection Section Office of the Missouri Attorney General PO Box 899 Jefferson City, MO 65102 joyce.yeager@ago.mo.gov (573) 751-6733
Montana	Kelley L. Hubbard Assistant Attorney General Montana Office of Consumer Protection 555 Fuller Ave Helena, MT 59601 khubbard@mt.gov (406) 444-5790
Nebraska	Daniel Birdsall Assistant Attorney General Consumer Protection Division Nebraska Attorney General's Office 2115 State Capitol Building Lincoln, NE 68509 dan.birdsall@nebraska.gov (402) 471-3840
Nevada	Lucas J. Tucker Senior Deputy Attorney General Office of the Nevada Attorney General Bureau of Consumer Protection 10791 W. Twain Ave., Suite #100 Las Vegas, NV 89135 ltucker@ag.nv.gov (702) 486-3256
New Hampshire	James T. Boffetti Senior Assistant Attorney General Chief, Consumer Protection and Antitrust Bureau Department of Justice 33 Capitol Street Concord, New Hampshire 03301 James.Boffetti@doj.nh.gov (603) 271-0302

Appendix D.

New Jersey	Elliott M. Siebers Deputy Attorney General Affirmative Civil Enforcement Practice Group Office of the Attorney General State of New Jersey 124 Halsey St. – 5th Floor P.O. Box 45029-5029 Newark, NJ 07101 Elliott.Siebers@dol.lps.state.nj.us (973) 648-4460
New Mexico	Elizabeth K. Korsmo Assistant Attorney General Consumer and Environmental Protection Division New Mexico Office of the Attorney General 408 Galisteo St. Santa Fe, NM 87504 ekorsmo@nmag.gov (505) 660-7593
New York	Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Office of the Attorney General 120 Broadway New York, NY 10271-0332 clark.russell@ag.ny.gov (212) 416-6494
North Carolina	Kim D'Arruda, CIPP/US Special Deputy Attorney General North Carolina Department of Justice Consumer Protection Division 114 West Edenton Street Raleigh, NC 27603 kdarruda@ncdoj.gov (919) 716-6013
North Dakota	Brian M. Card Assistant Attorney General Consumer Protection & Antitrust Division Office of Attorney General of North Dakota 1050 E. Interstate Ave., Suite 200 Bismarck, ND 58503-5574 bmcard@nd.gov (701) 328-5570

Appendix D.

Ohio	Michael Ziegler Principal Assistant Attorney General Office of the Ohio Attorney General - Consumer Protection Section 30 East Broad Street, 14th Floor Columbus, Ohio 43215 michael.ziegler@ohioattorneygeneral.gov (614) 466-3980
Oklahoma	Rachel Irwin Assistant Attorney General Consumer Protection Unit Oklahoma Attorney General's Office 313 NE 21st Street Oklahoma City, OK 73105 Rachel.Irwin@oag.ok.gov (405) 522-1014
Oregon	Eva Novick Assistant Attorney General Financial Fraud/Consumer Protection Section Oregon Department of Justice 100 SW Market Street Portland, OR 97201 eva.h.novick@doj.state.or.us (971) 673-1880
Pennsylvania	Nicole R. DiTomo Deputy Attorney General Pennsylvania Office of Attorney General Bureau of Consumer Protection 15th Floor, Strawberry Square Harrisburg, PA 17120 nditomo@attorneygeneral.gov (717) 705-6559
Rhode Island	Edmund F. Murray, Jr. Special Assistant Attorney General Rhode Island Department of Attorney General 150 South Main Street Providence, Rhode Island 02903 emurray@riag.ri.gov (401) 274-4400 ext. 2401

Appendix D.

South Carolina	Chantelle L. Neese Assistant Attorney General SC Attorney General's Office Consumer Protection & Antitrust Section Rembert C. Dennis Bldg 1000 Assembly St. P. O. Box 11549 Columbia, SC 29211 CNeese@scag.gov (803) 734-2346
South Dakota	Philip D. Carlson Assistant Attorney General Consumer Protection Division South Dakota Attorney General 1302 E. Hwy. 14, Ste. 1 Pierre, SD 57501 Phil.Carlson@state.sd.us (605) 773-3216
Tennessee	Carolyn Smith Senior Counsel Consumer Protection and Advocate Division Tennessee Attorney General's Office P.O. Box 20207 Nashville, TN 37202-0207 carolyn.smith@ag.tn.gov (615) 532-2578
Texas	D. Esther Chavez Senior Assistant Attorney General Office of the Attorney General Consumer Protection Division P.O. Box 12548 Austin, Texas 78711 Esther.Chavez@oag.texas.gov (512) 475-4628
Utah	David N. Sonnenreich Deputy Attorney General Office of the Utah Attorney General 160 East 300 South, 5th Floor P.O. Box 140872 dsonnenreich@agutah.gov (801) 366-0132

Appendix D.

Vermont	Ryan Kriger Assistant Attorney General Vermont Office of the Attorney General Public Protection Division 109 State St. Montpelier, VT 05609 ryan.kriger@vermont.gov (802) 828-3170
Virginia	Stephen John Sovinsky Assistant Attorney General Office of the Attorney General 202 North Ninth Street Richmond, Virginia 23219 ssovinsky@oag.state.va.us (804) 823-6341
Washington	Andrea Alegrett Assistant Attorney General Consumer Protection Division Office of the Washington Attorney General 800 Fifth Avenue, Suite 2000 Seattle, WA 98104 andreaa1@atg.wa.gov (206) 389-3813
West Virginia	Laurel K. Lackey Assistant Attorney General Office of the Attorney General Eastern Panhandle Office 269 Aikens Center Martinsburg, WV 25404 laurel.k.lackey@wvago.gov (304) 267-0239

SETTLEMENT AGREEMENT

Vermont Attorney General Thomas J. Donovan ("the Attorney General") and Valerie Shemeth and Welthy Myers, as former board members of the former nonprofit corporation United Way of Bennington County (collectively, "Respondents"), hereby agree to this voluntary Settlement Agreement ("Agreement").

LEGAL FRAMEWORK

1. The Attorney General has broad authority over the conduct of nonprofit corporations in Vermont and their use of charitable funds. *See generally* 9 V.S.A. § 2479(b); 11B V.S.A. §§ 3.03, 8.10, 14.30; *and* 14A V.S.A. §§ 110, 405, 413, 813.

2. A domestic nonprofit corporation in Vermont must be governed by a board of directors, 11B V.S.A. § 8.01(a), and cannot lawfully operate with fewer than three directors, *id.* § 8.03.

3. A nonprofit director "shall discharge his or her duties as a director . . . : (1) in good faith; (2) with the care an ordinarily prudent person in a like position would exercise under similar circumstances; and (3) in a manner the director reasonably believes to be in the best interests of the corporation." 11B V.S.A. § 8.30(a).

4. Subject to certain exceptions, it is a breach of the duty of good faith, 11B V.S.A. § 8.30(a)(1), and/or the duty of loyalty, *id.* § 8.30(a)(3), for a nonprofit director to improperly engage in a "conflict of interest transaction." *Id.* § 8.31.

5. A "conflict of interest transaction" is a transaction "in which a director of the corporation has a direct or indirect interest." 11B V.S.A. § 8.31(a). A director "has an indirect interest in a transaction if (1) another entity in which the director has a material interest or in which the director is a general partner is a party to the transaction; or (2) another entity of which the director is a director, officer or trustee is a party to the transaction." *Id.* § 8.31(d).

6. Such a transaction "is not voidable or the basis for imposing liability on the director if the transaction was fair at the time it was entered into." 11B V.S.A. § 8.31(a).

7. However, a conflict of interest transaction "may not be authorized, approved, or ratified under [Vermont law] by a single director[,]" regardless of whether the interested director has disclosed the material facts of the conflict in advance of the vote to approve the transaction and the board has voted to approve the transaction. 11B V.S.A. § 8.31(e). Further, the vote of the interested director is not considered for purposes of a quorum to validate the vote. *See id.*

8. Any "director who votes for or assents to a distribution made in violation of [Vermont's nonprofit code] is personally liable to the corporation for the amount of the distribution that exceeds what could have been distributed without violating [Vermont's nonprofit code] if it is established that the director did not perform his or her duties in compliance with section 8.30 of [the nonprofit code]." 11B V.S.A. § 8.33(a).

FACTUAL BACKGROUND

9. Respondent Valerie Shemeth is a resident of Vermont.

10. Respondent Welthy Myers is a resident of Vermont.

11. The United Way of Bennington County ("UWBC") was a Vermont nonprofit corporation and a local affiliate of United Way Worldwide (the "United Way").

12. UWBC's primary purpose, as stated in its filings with the Internal Revenue Service, was to "support local charities" by distributing "fundraising proceeds to charities that have applied for funding."

13. As the local affiliate of the United Way, UWBC was responsible for serving specific communities primarily in Bennington County, Vermont. UWBC was the only United Way affiliate assigned to those communities.

14. Since at least 2009, the bulk of UWBC's fundraising proceeds came from individuals who donated funds through other United Way affiliates in Vermont and around the country and purposefully directed those donations to the communities UWBC served. These funds were routed through the nation-wide United Way network to UWBC's bank account.

15. UWBC was governed by a board of directors (the "UWBC board").

16. Ms. Shemeth joined the UWBC board in the summer of 2010 and served as its president in 2011-13.

17. Ms. Myers joined the UWBC board in 2009 and served as its president in 2010 and vice-president in 2011-13.

18. In October 2010, for reasons immaterial to this matter, the UWBC board terminated the UWBC's executive director. In November 2010, the UWBC board hired a new executive director. However, after one year, for reasons likewise immaterial, the UWBC board elected not to renew the new executive director's contract. By January 2012, with the assistance of a certified public accountant, the UWBC board concluded that there were insufficient funds to continue to support an executive director position.

19. In March 2012, the UWBC board decided to cease operations and dissolve the corporation. Other than Ms. Myers and Ms. Shemeth, the entire UWBC board resigned.

20. On March 22, 2012, Ms. Shemeth sent a letter to the United Way and informed the membership accountability director that, effective May 15, 2012, UWBC would voluntarily withdraw from United Way membership, dissolve, and cease using the United Way name and logo.

21. Following the UWBC Board's resignation, Ms. Myers acted as the treasurer of UWBC and had sole signatory authority on UWBC's bank account.

22. In the summer of 2012, after the UWBC board's resignation and UWBC's formal notice of withdrawal from the United Way, Ms. Shemeth and Ms. Myers realized that, despite UWBC's official closure and withdrawal as a United Way affiliate, money continued to be deposited into UWBC's bank account.

23. Without consulting the United Way or any other former UWBC board members or staff, and without transferring the funds to the United Way affiliate that had taken over responsibility for the communities UWBC had served, Ms. Myers and Ms. Shemeth, alone, decided to distribute $48,397 from UWBC funds to local organizations.

24. Of the total funds distributed by Ms. Shemeth and Ms. Myers, $11,500 went to Gallop to Success, a Vermont nonprofit corporation that Ms. Shemeth founded, incorporated in September 2011, and presided over as President. Ms. Myers served as the organization's vice-president. The organization's principal place of business was Kimberly Farms in North Bennington, Vermont, Ms. Shemeth's for-profit horse farm.

25. Likewise, of the $48,397 distributed, an additional $7000 went directly to Kimberly Farms. Ms. Shemeth served as Kimberly Farms' President. Her husband and daughter served as corporate directors. At no time was Kimberly Farms a charitable organization.

26. In total, in 2012, Ms. Shemeth and Ms. Myers distributed $18,500 of charitable funds to organizations in which Ms. Shemeth had an interest (almost 40% of all the charitable funds they distributed together), including $7000 to Ms. Shemeth's for-profit business with no charitable mission.

27. Following a complaint by the United Way regarding UWBC's continued use of the United Way name and logo, and a subsequent investigation by the Attorney General's Office, in September 2013 Ms. Shemeth and Ms. Myers agreed to cease operating UWBC and transfer all

funds to the United Way of Vermont ("UWVT"), the organization currently serving the Bennington County communities that UWBC had served.

28. The Attorney General finds, based on its investigation:

a. Ms. Myers and Ms. Shemeth acted without proper authority and, as two individuals, were not a properly constituted board of directors when they made decisions on behalf of UWBC after March 2012 regarding the use of charitable funds.

b. Ms. Myers and Ms. Shemeth breached their duties of good faith and loyalty when they gave charitable funds to an organization in which they both had an interest, and gave additional charitable funds to a for-profit corporation in which Ms. Shemeth had a financial interest.

29. Respondents admit the truth of all facts set forth in the Factual Background section above.

CLAIM

The Attorney General alleges that the above conduct constitutes a breach of fiduciary duty, in violation of 11B V.S.A. § 8.30, and an improper conflict of interest transaction, in violation of 11B V.S.A. § 8.33, as to both Ms. Myers and Ms. Shemeth.

TERMS OF SETTLEMENT

As conditions for settling this matter, Respondents agree to the following:

Restitution

A. Within 60 days of signing this agreement, Respondent Valerie Shemeth will repay $7,000.00 to the United Ways of Vermont, PO Box 111, Essex Junction, VT 05453 as restitution for monies improperly distributed to Gallop to Success and Kimberly Farms.

B. Upon making the above payments, or any portion thereof, Ms. Shemeth shall send a copy of the check and any associated correspondence to the Attorney General's Office, 109 State St., Montpelier, Vermont 05609, to the attention of Assistant Attorney General Jamie Renner.

Temporary Prohibition on Nonprofit Board Service

C. Respondents are prohibited from serving on any nonprofit board of directors until they have successfully completed a training course on the fiduciary responsibilities of a nonprofit board member and receive approval from the Attorney General's Office. Such approval shall be promptly given in writing upon presentation of documents demonstrating completion of an appropriate training course, and shall not be unreasonably withheld.

MISCELLANEOUS PROVISIONS

A. Negotiation and Drafting of Document: This Agreement is a document which both Parties have negotiated and drafted; therefore, the general rule of construction interpreting a document against the drafter shall not be applied in any future interpretation of this Agreement.

B. Entire Agreement: This Agreement represents the entire and only Agreement between the parties. All prior agreements, representations, statements, negotiations and understandings shall have no effect.

C. Governing Law: The law of the State of Vermont shall govern any dispute regarding this Agreement.

SIGNATURE

In lieu of instituting an action or proceeding against Respondents, the Office of the Attorney General accepts this Settlement Agreement. By signing below, Respondents voluntarily agrees with and submits to the terms of this Agreement.

DATED at N Bennington, Vermont, this 17th day of July, 2017.

Valerie Shemeth

Valerie Shemeth

Welthy Myers

Welthy Myers

AS TO FORM:

Peter Langrock, Esq.

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont, this 11 day of September, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN
ATTORNEY GENERAL

By: _____

Jamie Renner
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
Jamie.Renner@state.vt.us
(802) 828-5947

In the matter of:
THE WESTERN UNION COMPANY,
a corporation,

Respondent.

ASSURANCE OF DISCONTINUANCE/ASSURANCE OF VOLUNTARY COMPLIANCE

A. PARTIES

1. The signatory to this Assurance of Discontinuance ("Assurance") is The Western Union Company ("Western Union," the "Company," or "Respondent"), and the States and Commonwealths listed in Exhibit A (hereafter "the Participating States" or "the States," and, collectively with Western Union, may be referred to as "the Parties.").

2. The States are represented by the Consumer Protection Divisions of their respective Attorneys General.[1]

3. The Western Union Company is a Delaware corporation with its principal place of business at 12500 East Belford Avenue, Englewood, Colorado 80112.

B. STIPULATIONS

[1] The Utah Division of Consumer Protection is statutorily authorized to enforce all statutes listed in Utah Code 13-2-6, including the Utah Consumer Sales Practices Act, Utah Code 13-11-1, *et seq.* Hawaii is represented by its Office of Consumer Protection, an agency that is not part of the State Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. Massachusetts is represented by the Insurance and Financial Services Division of the State Attorney General's Office which, as part of the State Attorney General's Office, is statutorily authorized to bring consumer protection actions under M.G.L. c. 93A, Section 1 *et seq.*

4. Pursuant to their respective authority under their state consumer protection statutes ("Acts"[2]), the Participating States conducted an investigation of Western Union's anti-fraud compliance efforts.

5. Respondent neither admits nor denies any of the allegations in this Assurance and, only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

6. Respondent waives all rights to appeal or otherwise challenge or contest the validity of this Assurance.

7. This Assurance does not constitute an approval by the Participating States of Respondent's business practices, and Respondent shall make no representation or claim to the contrary.

8. This Assurance sets forth the entire agreement between the Parties.

9. This Assurance may be executed in counterparts, each of which shall be deemed to constitute an original counterpart hereof, and all of which shall together constitute one and the same Assurance.

10. Nothing in this Assurance shall require Respondent to take any action inconsistent with, or in addition to other than as expressly set forth herein, the requirements or prohibitions of the Stipulated Order for Permanent Injunction and Final Judgement entered into in *Federal Trade Commission v. The Western Union Company,* Civil Action No. 1:17-cv-00110-CCC, in the United States District Court for the Middle District of Pennsylvania, or any subsequent modifications thereof.

[2] Exhibit A attached here lists the Participating States and cites the applicable state consumer protection laws of each.

11. The Parties stipulate that the Compliance Provisions of this Assurance are consistent with Western Union's obligations pursuant to the case referenced in the preceding paragraph above.

DEFINITIONS

12. The following definitions shall be used in construing this Assurance:

A. "**Cash-to-cash money transfer**" means the transfer of the value of cash from one person in one location to a recipient (payee) in another location that is received in the form of cash.

B. "**Cash reload money transfer**" means the transfer of the value of cash from one person in one location to a recipient (payee) in another location that is received in a form that makes it possible for a person to convert the cash into an electronic form that can be used to add funds to a general-use prepaid card or an account with a payment intermediary.

C. "**Consumer**" means any person, worldwide, who initiates or sends a money transfer.

D. "**Respondent**" means The Western Union Company.

E. "**Effective Date**" means the date upon which Respondent signs and executes this Assurance.

F. "**Elevated fraud countries**" means any country in which the principal amount of money transfers that are the subject of fraud complaints, received by Respondent from any source, represents one (1) percent or more of the principal amount of fraud complaints worldwide received by Respondent, for either money transfers sent or received in that country, determined on a quarterly basis, *provided that* once a country is determined to be one of the elevated fraud countries, it shall continue to be treated as such for purposes of this Assurance.

G. "**Elevated fraud risk agent location**" means any Western Union agent location that has processed payouts of money transfers associated with:

1. Five (5) or more fraud complaints for such agent location, received by Respondent from any source, during the previous sixty (60) day period, based on a review of complaints on a monthly basis; and fraud complaints, received by Respondent from any source, totaling five (5) percent or more of the total payouts for such agent location in numbers or dollars in a sixty (60) day period, calculated on a monthly basis; or

2. Fifteen (15) or more fraud complaints for such agent location, received by Respondent from any source, during the previous sixty (60) day period, based on a review of complaints on a monthly basis.

H. "**Executive Committee**" refers to the following Attorneys Generals' offices: Illinois, Kentucky, Louisiana, Massachusetts, New Jersey, North Carolina, Ohio, Texas and Vermont.

I. "**Fraud-induced money transfer**" includes any money transfer that was induced by, initiated, or sent as a result of, unfair or deceptive acts or practices and/or deceptive or abusive telemarketing acts or practices.

J. "**Front line associate**" means the employee of the Western Union agent responsible for handling a transaction at the point of sale for a consumer or a recipient (payee) of a money transfer, including by initiating, sending, or paying out the money transfer.

K. "**FTC Action**" refers to the case styled *Federal Trade Commission v. The Western Union Company,* Civil Action No. 1:17-cv-00110-CCC, in the United States District Court for the Middle District of Pennsylvania.

L. "**Money transfer**" means the sending of money (in cash or any other form, unless otherwise stated) between a consumer in one location to a recipient (payee) in another location using Respondent's money transfer service, and shall include transfers initiated or sent in person, online, over the telephone, using a mobile app, or through whatever platform or means made available. The term "money transfer" does not include Respondent's bill or loan payment services, or purchases of foreign currency conversions or options contracts from Respondent.

M. "**Participating States**" or "**States**" refers to the District of Columbia and the states, commonwealths, and territories listed in Exhibit A.[3]

N. "**Person**" includes a natural person, an organization or other legal entity, including a corporation, partnership, sole proprietorship, limited liability company, association, cooperative, or any other group or combination acting as an entity.

O. "**Seller**" means any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services in exchange for consideration.

P. "**Telemarketer**" means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer.

Q. "**Telemarketing**" means any plan, program, or campaign which is conducted to induce the purchase of goods or services by use of one or more telephones, and which involves a telephone call, whether or not covered by the Telemarketing Sales Rule, 16 CFR Part 310.

R. "**Western Union agent**" means any network agent, master agent, representative, authorized delegate, independent agent, super-agent, national account agent, key account agent,

---

[3] With regard to the Commonwealth of Virginia, this document will be titled as an "Agreement." With regard solely to Western Union's agreement with the State of Delaware, the parties agree that this Assurance shall operate as a cease and desist by agreement authorized by 29 Del.C. Section 2525(a).

strategic account agent, sub-representative, subagent, or any location, worldwide, authorized by Respondent to offer or provide any of its money transfer products or services.

COMPLIANCE TERMS

I.

PROHIBITED BUSINESS ACTIVITIES

IT IS AGREED that Respondent, Respondent's officers, agents, and employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Assurance, whether acting directly or indirectly, in connection with promoting, offering for sale, or providing money transfer services, are permanently restrained and enjoined from:

A. Transmitting a money transfer that Respondent knows or reasonably should know is a fraud-induced money transfer, or paying out a money transfer to any person that Respondent knows or reasonably should know is using its system to obtain funds from a consumer, directly or indirectly, as a result of fraud;

B. Providing substantial assistance or support to any seller or telemarketer that Respondent knows or reasonably should know is accepting from a U.S. consumer, directly or indirectly, a money transfer as payment for goods or services offered or sold through telemarketing;

C. Failing to do any of the following in connection with money transfers initiated by consumers:

1. Interdict recipients that have been the subject of any complaints about fraud-induced money transfers based on information provided to, or that becomes known by, Respondent;

2. Identify, prevent, and stop cash-to-cash money transfers and cash reload money transfers initiated or received in the U.S. from being used as a form of payment by sellers or telemarketers, including, but not limited to, by:

   a. Asking all U.S. consumers whether the money transfer is a payment for goods or services offered or sold through telemarketing;

   b. Declining to process money transfers from U.S. consumers where the money transfer is a payment for goods or services offered or sold through telemarketing; and

   c. Interdicting known sellers and telemarketers accepting money transfers as payments for goods or services offered through telemarketing;

3. Provide a clear, concise, conspicuous and uncontradicted consumer fraud warning on the front page of all money transfer forms, paper or electronic, utilized by consumers in elevated fraud countries (based on money transfers sent from those countries) to initiate money transfers using Respondent's system that includes, but is not limited to:

   a. A list of the most common types of scams that utilize Respondent's money transfer system;

   b. A warning that it is illegal for any seller or telemarketer to accept payments from U.S. consumers through money transfers for goods or services offered or sold through telemarketing;

c. A notice to consumers that the money transfer can be paid out to the recipient within a short time, and that after the money is paid out, consumers may not be able to obtain a refund from Respondent, even if the transfer was the result of fraud, except under limited circumstances; and

d. A toll-free or local number and a website for Respondent, subject to the timing requirements set forth in Subsection C.4, that consumers may call or visit to obtain assistance and file a complaint if their money transfer was procured through fraud;

4. Make available in all countries in which Respondent offers money transfer services a website that consumers may visit to obtain assistance and file a complaint if they claim their money transfer was procured through fraud, *provided that* websites that are not yet available shall be made available in accordance with the following schedule: (i) for countries determined to be elevated fraud countries, within six (6) months of entry of the Stipulated Order For Permanent Injunction and Final Judgment in the FTC Action (the "Stipulated Order"); and (ii) for all other countries, within two (2) years of entry of the Stipulated Order;

5. Provide consumers who initiate or send money transfers via the Internet, telephone, mobile app, or any other platform that is not in-person, with substantially the same clear, concise, conspicuous and uncontradicted fraud warning required by Subsection C.3, *provided that* the warning may

be abbreviated to accommodate the specific characteristics of the media or platform;

6. Provide the required warning to consumers in the language used on the send form or other media type or platform used for the money transfer, in a form appropriate for the media or platform;

7. Review and update the consumer warning as necessary to ensure its effectiveness in preventing fraud-induced money transfers; and

8. Submit modifications to the warning, if any, to the Executive Committee for review no less than ten (10) business days before any modified warning is disseminated to Western Union agents; *provided that* nothing herein shall prohibit Respondent from changing the nature or form of its service, send forms, or media or platform for offering money transfer services or from seeking to replace its send forms with an electronic form or entry system of some type in the future. In the event such changes are made, Respondent shall provide a consumer fraud warning substantially similar to that outlined in Subsection C.3 in a form appropriate to the media or platform;

D. Failing to reimburse the principal amount of a consumer's money transfer and any associated transfer fees whenever a consumer or his or her authorized representative reasonably claims that the transfer was fraudulently induced and:

1. The consumer or his or her authorized representative asks Respondent, the sending agent, or front line associates to reverse the transfer before the transferred funds have been picked up; or

2. Respondent, after reviewing information and data relating to the money transfer, determines that Respondent, its agents, or the front line associates failed to comply with any of Respondent's policies and procedures relating to detecting and preventing fraud-induced money transfers when sending or paying out the money transfer by failing to: provide the required consumer fraud warnings; comply with Respondent's interdiction or callback programs; verify the recipient's identification; or accurately record the recipient's identification(s) and other required biographical data;

E. Failing to promptly provide information to a consumer, or his or her authorized representative, who reports being a victim of fraud to Respondent, about the name of the recipient of the consumer's money transfer and the location where it was paid out, when such information is reasonably requested; and

F. Failing to establish and implement, and thereafter maintain, a comprehensive anti-fraud program that is reasonably designed to protect consumers by detecting and preventing fraud-induced money transfers worldwide and to avoid installing and doing business with Western Union agents who appear to be involved or complicit in processing fraud-induced money transfers or fail to comply with Respondent's policies and procedures to detect and prevent fraud (hereinafter referred to as "Respondent's Anti-Fraud Program"). As ordered in the FTC Action, Respondent is required to provide the FTC with a written copy of such program, which shall include at least the following requirements:

1. Performance of due diligence on all prospective Western Union agents and existing Western Union agents whose contracts are up for renewal;

2. Designation of an employee or employees to coordinate and be accountable for Respondent's Anti-Fraud Program;

3. Appropriate and adequate education and training on consumer fraud for Western Union agents and front line associates;

4. Appropriate and adequate monitoring of Western Union agent and front line associate activity relevant to the prevention of fraud-induced money transfers;

5. Prompt disciplinary action against Western Union agent locations where reasonably necessary to prevent fraud-induced money transfers;

6. Adequate systematic controls to detect and prevent fraud-induced money transfers, including, but not limited to:

   a. Imposing more stringent identification requirements for money transfers sent to, or paid out in, elevated fraud countries;

   b. Holding suspicious money transfers at certain dollar thresholds to elevated fraud countries until Respondent has confirmed with the sender that they are not fraud-induced or has refunded the money to the sender;

   c. Ensuring that Western Union agent locations are recording all required information about recipients required by Respondent's policies or procedures or by law, including, but not limited to, their names, addresses, telephone numbers, and identifications, before paying out money transfers; and

7. Periodic evaluation and adjustment of Respondent's Anti-Fraud Program in light of:

a. The results of the monitoring required by Subsection F.4 of this Section and Section III of this Assurance;

b. Any material changes to Respondent's operations or business arrangements; or

c. Any other circumstances that Respondent knows or reasonably should know may have a material impact on the effectiveness of Respondent's Anti-Fraud Program. As ordered in the FTC Action, Respondent is required to notify the FTC in writing of adjustments to its Anti-Fraud Program. Respondent is also required to notify the Executive Committee that it has sent the FTC such a notice of adjustments.

II.

DUE DILIGENCE ON PROSPECTIVE AND EXISTING WESTERN UNION AGENTS

IT IS FURTHER AGREED that Respondent, Respondent's officers, agents, and employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Assurance, whether acting directly or indirectly, in connection with promoting, offering for sale, or providing money transfer services, are hereby restrained and enjoined from:

A. Failing to conduct thorough due diligence on all persons applying to become, or renewing their contracts as, Western Union agents, including any sub-representative or subagent,

to avoid installing Western Union agents worldwide who may become elevated fraud risk agent locations, including, but not limited to, by:

1. Verifying government-issued identification;
2. Conducting all reasonably necessary background checks (criminal, employment, or otherwise) where permissible under local law;
3. Determining whether information or statements made during the agent application process are false or inconsistent with the results of Respondent's background checks or other due diligence;
4. Taking reasonable steps to ascertain whether the prospective agent formerly owned, operated, had been a front line associate of, or had a familial, beneficial, or straw relationship with any location of any money services business that was suspended or terminated for fraud-related reasons, as permitted by applicable laws and regulations (including foreign laws and regulations) and with the required cooperation from other money transfer companies;
5. Ascertaining whether the prospective agent had previously been interdicted by Respondent for suspicious activities or had been reported to Respondent as a recipient of fraud-induced money transfers;
6. Conducting an individualized assessment of the particular risk factors involved with each Western Union agent application and conducting all reasonably necessary investigative steps consistent with those risks; and
7. Maintaining information about Respondent's due diligence, including, but not limited to, information about the identities of the owners, their

government-issued identifications, and the background check(s) conducted;

B. Failing to reject applications where Respondent becomes aware or reasonably should have become aware based upon its due diligence that the applicant, or any of the applicant's sub- representatives or subagents, presents a material risk of becoming an elevated fraud risk;

C. Failing to ensure that the written agreements entered into with all new Western Union agents require them to comply with Section I.C.2 of this Assurance;

D. Failing to ensure that all new Western Union agents have effective policies and procedures in place at each of the agent's locations to detect and prevent fraud-induced money transfers and other acts or practices that violate Section I of this Assurance;

E. Failing to take reasonable steps to confirm that Western Union agents whose contracts are up for renewal are complying with the terms of their agreements with Respondent, including, but not limited to, by having effective policies and procedures in place to detect and prevent fraud- induced money transfers; and

F. Failing to require all new Western Union agents, and existing Western Union agents, to: (i) disclose and update the identities of any sub-representative or subagent; and (ii) maintain records on the identities of any front line associates at their sub-representatives' or subagents' locations.

III.

MONITORING COMPLIANCE OF WESTERN UNION AGENTS

IT IS FURTHER AGREED that Respondent, Respondent's officers, agents, and employees, and all other persons in active concert or participation with any of them, who receive

actual notice of this Assurance, whether acting directly or indirectly, in connection with promoting, offering for sale, or providing money transfer services, are hereby restrained and enjoined from:

A. Failing to provide appropriate and adequate ongoing education and training on consumer fraud for all Western Union agents, and other appropriate Western Union personnel, including, but not limited to, education and training on detecting, investigating, preventing, reporting, and otherwise handling suspicious transactions and fraud-induced money transfers, and ensuring that all Western Union agents and front line associates are notified of their obligations to comply with Respondent's policies and procedures and to implement and maintain policies and procedures to detect and prevent fraud-induced money transfers or other acts or practices that violate Section I of this Assurance;

B. Failing to take all reasonable steps necessary to monitor and investigate Western Union agent location activity to detect and prevent fraud-induced money transfers, including, but not limited to:

1. Developing, implementing, adequately staffing, and continuously operating and maintaining a system to receive and retain all complaints and data received from any source, anywhere in the world, involving alleged fraud-induced money transfers, and taking all reasonable steps to obtain, record, retain, and make easily accessible to Respondent and, upon reasonable request and to the extent the information is not accessible via FTC's Consumer Sentinel Network ("Consumer Sentinel"), the Executive Committee, all relevant information regarding all complaints related to alleged fraud-induced money transfers, including, but not limited to:

a. The consumer's name, address, and telephone number;

b. The substance of the complaint, including the fraud type and fraud method, and the name of any person referenced;

c. The reference number, or Money Transfer Control Number, for each money transfer related to the complaint;

d. The name, agent identification number, telephone number, and address of the sending agent(s);

e. The date of each money transfer;

f. The amount of each money transfer;

g. The money transfer fee for each money transfer;

h. The date each money transfer is received;

i. The name, agent identification number, telephone number, and address of the receiving agent(s);

j. The name, address and telephone number of the recipient, as provided by the recipient, of each money transfer;

k. The identification, if any, presented by the recipient, and recorded, for each money transfer;

l. All transactions conducted by the consumer bearing any relationship to the complaint; and

m. To the extent there is any investigation concerning, and/or resolution of, the complaint:

    1. The nature and result of any investigation conducted concerning the complaint;

2. Any response to the complaint and the date of such response to the complaint;

3. The final resolution of the complaint, the date of such resolution, and an explanation for the resolution; and

4. If the resolution does not include the issuance of a refund, the reason for the denial of a refund;

2. Taking all reasonable steps to identify Western Union agents or front line associates involved or complicit in fraud;

3. Routinely reviewing and analyzing data regarding the activities of Western Union agent locations in order to identify the following:

a. Agent locations that have processed transactions associated with two (2) or more complaints about alleged fraud-induced money transfers, received by Respondent from any source, during a thirty (30) day period;

b. Elevated fraud risk agent locations, as defined above; and

4. For agent locations identified pursuant to Subsection B.3 of this Section, fully investigate the agent location by reviewing transaction data and conducting analyses to determine if the agent location displayed any unusual or suspicious money transfer activity that cannot reasonably be explained or justified, including, but not limited to:

a. Data integrity issues, including, but not limited to, invalid, illegible, incomplete, missing, or conflicting biographical data for consumers or recipients of money transfers;

b. Significant changes in the transaction patterns experienced at the agent location;

c. Significant differences in the transaction patterns experienced at an agent location relative to the patterns experienced at other agent locations in the same country;

d. Unusual demographic activity;

e. Irregular concentrations of send and/or pay activity between the agent and one or more other Western Union agent locations;

f. Irregular concentrations of send and/or pay activity between the agent and one or more geographical areas that have been identified as high risk for fraud;

g. Unusual transaction patterns by senders or recipients;

h. Flipping patterns;

i. Suspicious structuring or splitting of money transfers; or

j. Suspicious surfing patterns;

C. Failing to take the following actions to prevent further fraud-induced money transfers, including, but not limited to, by:

1. Suspending Western Union agent locations, as follows, pending further investigation to determine whether the Western Union agent locations can continue operating consistent with this Assurance's requirements:

a. For agent locations identified pursuant to Subsection B.3.a of this Section, if the investigation of the agent location required by Subsection B.4 of this Section is not completed within fourteen

(14) days after the agent location is identified, suspending the Western Union agent location's ability to conduct further money transfers until the investigation is completed; and

b. For elevated fraud risk agent locations, immediately suspending the Western Union agent's ability to conduct further money transfers until the review required by Subsection B.4 of this Section is completed, *except that*, for a Western Union agent that is a bank or bank branch and otherwise subject to this immediate suspension requirement by virtue of fraud complaints about money transfers that are transferred directly into its account holders' bank accounts, Western Union shall comply with Subsection III.C.1.a. and also permanently block, or request that the Western Union agent block, all further money transfers to bank accounts for which Western Union has received any fraud complaint;

2. Upon completion of the investigation, terminating, suspending, or restricting Western Union agent locations as follows:

a. Terminating or suspending the Western Union agent location; or restricting the agent location's ability to send and/or receive certain money transfers, if the findings indicate that the Western Union agent location is not, or has not been, complying with Respondent's Anti-Fraud Program and other policies and procedures relating to detecting and preventing fraud-induced money transfers, including, but not limited to, by failing to collect

and record required and accurate biographical information about, and government-issued identifications for, the recipients of money transfers; and

b. Terminating the Western Union agent location if the findings indicate that the Western Union agent location or any of its front line associates is, or may be, complicit in the fraud-induced money transfers, has failed to comply with Section IV of this Assurance, or has repeatedly failed to comply with Respondent's Anti-Fraud and other policies and procedures relating to detecting and preventing fraud-induced money transfers;

3. On at least a monthly basis, providing notice to all Western Union agents in elevated fraud countries the substance of any complaints Respondent received involving transactions processed by the agents' locations; and

4. Ensuring that all Western Union agents are enforcing effective policies and procedures to detect and prevent fraud-induced money transfers, or other acts or practices that violate Section I of this Assurance; and

D. Failing to establish adequate controls to ensure that, prior to paying out money transfers, Western Union agent locations are recording all required information about the recipients of money transfers, including, but not limited to, the recipients' names, addresses, telephone numbers, and identifications, and are taking reasonable steps to verify the identification presented by the recipients or, for money transfers that are directed to bank accounts, the identities of the account holders.

IV.

REQUIREMENTS FOR ELEVATED FRAUD RISK AGENT LOCATIONS

IT IS FURTHER AGREED that Respondent, Respondent's officers, agents, and employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Assurance, whether acting directly or indirectly, in connection with promoting, offering for sale, or providing money transfer services, shall require and ensure that all elevated fraud risk agent locations that are still operating do the following for one (1) year from the date that Respondent identifies the agent as an elevated fraud risk agent location under the terms of this Assurance:

A. For money transfers that are not transferred directly into a recipient's bank account, photocopy or scan the identification documents or biometric information presented by the recipient and retain the photocopies or images, along with the receive forms, for a period of five (5) years; and

B. Demonstrate during compliance reviews or mystery shops, which Respondent shall conduct on at least a quarterly basis, that the agent location is complying with the requirements in this Section.

Provided, however, that if Defendant reasonably believes that complying with Subsection A of this Section for money transfers received by an elevated fraud agent location in a particular foreign jurisdiction would violate that jurisdiction's laws, Defendant may instead, upon notice to FTC staff, block all money transfers from the United States to that elevated fraud risk agent location or, with the agreement of FTC staff, take other appropriate action at that location to protect consumers from fraud.

V.

SHARING COMPLAINT INFORMATION

IT IS FURTHER AGREED that, Respondent, Respondent's officers, agents, and employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Assurance, whether acting directly or indirectly, shall, in addition to, or as a modification of, any other policy or practice that the Respondent may have, including Respondent's ongoing submission of information to the FTC for inclusion in Consumer Sentinel:

A. Provide notice to the consumer, or his or her authorized representative, at the time the Respondent is contacted with a complaint about alleged fraudulent activity associated with a money transfer, that (i) Respondent's practice is to share information regarding the consumer's money transfer and complaint with a database used by law enforcement authorities in the United States and other countries; and (ii) if the consumer does not want his or her name, address, and identification shared with law enforcement, Respondent will honor that request unless applicable law permits or requires Respondent to provide that information; and

B. Regularly, but no more than every thirty (30) days, submit electronically to the FTC, or its designated agent, for inclusion in Consumer Sentinel, all relevant information Respondent possesses regarding complaints received from consumers, their authorized representatives, or any other source, anywhere worldwide, about alleged fraud-induced money transfers and regarding the underlying transfer itself, including, but not limited to, the information set forth in Section III.B.1.a through III.B.1.l. *Provided, however*, if Respondent receives a request from a consumer or the consumer's authorized representative, which is documented by Respondent, stating that the consumer does not want the information shared with the database, or if Respondent received the complaint from a source other than the consumer or

the consumer's authorized representative, Respondent shall submit to the FTC an anonymized complaint with the consumer's name, address, and telephone number redacted. *Provided further*, that Respondent shall cooperate with the FTC in order to facilitate compliance with this Section.

VI.

INDEPENDENT COMPLIANCE AUDITOR

As ordered in *Federal Trade Commission v. The Western Union Company,* Civil Action No. 1:17-cv-00110-CCC, in the United States District Court for the Middle District of Pennsylvania (FTC Judgment), an independent compliance auditor shall be appointed to further ensure compliance with Sections I through V.

VII.

MONETARY PAYMENT TO THE STATES

IT IS FURTHER AGREED THAT:

A. Western Union shall pay a total of Five Million Dollars ($5,000,000.00) to the Participating States, to be distributed among such states as agreed by the Attorneys' General. Each state shall use its portion of funds as compensation for recovery of its costs and attorney's fees in investigating this matter, future monitoring and enforcement of this Assurance, future enforcement of its consumer protection laws or for any lawful purpose including consumer education or redress in the discharge of the Attorney General's duties at the sole discretion of the Attorney General in accordance with applicable state laws and procedures. Western Union's monetary payment to the Participating States shall not be deemed, or deemed in lieu of, a fine, penalty, forfeiture, or punitive assessment and may not be characterized as such.

B. Western Union's payment to the states shall be made no later than fifteen (15) days after Western Union's receipt through its counsel of record in this case of written wire

transfer instructions from Vermont Assistant Attorney General James Layman, who is authorized by the Executive Committee to provide those instructions. The monetary award in this case is accepted by the Participating States which acknowledge that redress for consumers shall be made available through the Stipulated Order for Permanent Injunction and Final Judgment entered in *Federal Trade Commission v. The Western Union Company,* Civil Action No. 1:17-cv-00110-CCC, in the United States District Court for the Middle District of Pennsylvania, which requires that Respondent pay Five Hundred Eighty-Six Million Dollars ($586,000,000) and that such funds be deposited into a fund to be used to compensate fraud victims as detailed in Section VII of the Stipulated Order.

VIII.

ACKNOWLEDGMENT OF ASSURANCE

IT IS FURTHER AGREED that Respondent will obtain acknowledgments of receipt of this Assurance. Respondent, within seven (7) days of the Effective Date, must submit to the Executive Committee an acknowledgment of receipt of this Assurance sworn under penalty of perjury.

IX.

COMPLIANCE REPORTING

As ordered in the FTC Action, Respondent is required to submit compliance reports to the FTC, as detailed in Section IX of the Stipulated Order.

X.

COMPLIANCE MONITORING

As ordered in the FTC Action, Respondent is required to monitor its compliance with the Stipulated Order and may be required to submit additional compliance reports or requested information to the FTC, as detailed in Section XI of the Stipulated Order.

XI.

RELEASE

By execution of this assurance, the Participating States hereby fully release and discharge Western Union, its parents, affiliates, subsidiaries, employees, officers, and directors (collectively, the "Released Parties"), from the following: any and all civil and administrative actions, claims, and causes of action that were or could have been asserted against the Released Parties by the Participating States' respective Attorneys General under the States' consumer protection laws, or any amendments thereto, resulting from the conduct complained of in the complaint filed by the FTC in the FTC Action and/or the matters addressed in this Assurance, up to and including the effective date of this Assurance (collectively, the "Released Claims").

A. Nothing in this Assurance or in this release shall be construed to alter, waive, or limit any private right of action specifically provided by state law.

B. Notwithstanding any term of this Assurance, any and all of the following forms of liability are specifically reserved and excluded from the Released Claims:

1. Any criminal liability that any person or entity, including Western Union, has or may have in the Participating State;
2. Any civil or administrative liability that any person or entity, including Western Union, has or may have to the Participating State under any

statute, regulation or rule not expressly covered by the release in this Section, including but not limited to, any money laundering claims and any and all of the following claims:

a. state or federal antitrust violations,

b. state or federal securities violations, and

c. state or federal tax claims.

XII.

GENERAL PROVISIONS

IT IS FURTHER AGREED that Respondent shall execute and deliver all authorizations, documents and instruments which are necessary to effectuate the terms and conditions of this Assurance, whether required prior to, contemporaneous with, or subsequent to the Effective Date.

A. The settlement negotiations resulting in this Assurance have been undertaken by Respondent and the Attorneys General in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Assurance shall be offered or received in evidence in any action or proceeding for any purpose.

B. To the extent this Assurance is filed in any Court, Respondent waives notice and service of process for the filing, and such Court retains jurisdiction over this Assurance and the parties hereto for the purpose of enforcing and modifying this Assurance and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Assurance shall be valid or binding unless made in writing, signed by the parties, and approved by any Court in which this Assurance is filed, and then only to the extent

specifically set forth in such a Court's Order. The Parties may agree in writing, through counsel, to an extension of any time period in this Assurance without a court order.

C. To the extent this Assurance must be approved by any Court, Respondent does not object to the Attorney General's ex parte submission and presentation of this Assurance to the Court, does not object to the Court's approval of this Assurance, and does not object to the entry of this Assurance by the clerk of the Court if entry is required.

D. Nothing in this Assurance shall be construed as relieving Respondent of its obligation to comply with all state and federal laws, regulations or rules, or as granting permission to engage in any acts or practices prohibited by such law, regulation or rule.

E. This Assurance does not constitute an approval by the Attorneys General of any of Respondent's past, present or future business acts and practices.

F. If any portion of this Assurance is held invalid by operation of law, the remaining terms of this Assurance shall not be affected and shall remain in full force and effect.

G. Nothing in this Assurance shall be construed to waive, limit, or expand any claim of sovereign immunity the Attorneys General may have in any action or proceeding.

H. This Assurance may be enforced only by the Parties hereto. Nothing in this Assurance shall provide any rights or permit any person or entity not a party hereto to enforce any provision of this Assurance.

I. The Parties agree that a Participating State will provide Respondent with written notice if it believes that Respondent is in violation of any of its obligations under this Assurance ("Notice"). Respondent shall have 30 business days after the date of receipt of the Notice to demonstrate to the State's satisfaction that:

1. Respondent is in compliance with the obligations of this Assurance cited by that State as being violated;

2. the violation has been addressed, including, but not limited to, by remedial actions having been taken against an employee for actions inconsistent with this Assurance; or

3. the alleged violation cannot be addressed within the 30 business day period, but that: (a) Respondent has begun to take action to address the violation; (b) Respondent is pursuing such action with due diligence; and (c) Respondent has provided a reasonable timetable for addressing the violation.

J. Nothing shall prevent the State from agreeing in writing to provide Respondent with additional time beyond the 30 business days to respond to the notice.

K. No person, entity or official not a signatory hereto is a third-party beneficiary of this Assurance. Nothing in this Assurance shall be construed to affect, limit, alter or assist any private right of action that a consumer may hold against Respondent, nor shall anything in this Assurance confer upon any consumer standing to pursue any private right of action against Respondent.

OFFICE OF THE ATTORNEY GENERAL

FOR Vermont

By: James Layman, Asst. Atty. General

James Layman

Date: 1/31/2017

RESPONDENT THE WESTERN UNION COMPANY

John R. Dye
Executive Vice President and General Counsel

Dated: January 23, 2017

COUNSEL FOR RESPONDENT, THE WESTERN UNION COMPANY

Edward B. Schwartz
Steptoe & Johnson LLP
1330 Connecticut Avenue, NW
Washington, DC 20036

Dated: January 23, 2017

Sean M. Berkowitz
Latham & Watkins LLP
330 North Wabash Avenue, Suite 2800
Chicago, Illinois 60611

Dated: January 23, 2017

LOCAL COUNSEL FOR RESPONDENT, THE WESTERN UNION COMPANY

Jennifer H. McDonald Dated: January 26, 2017

Jennifer H. McDonald
Downs Rachlin Martin PLLC
199 Main Street
P.O. Box 190
Burlington, Vermont 05402-0190
Telephone: 802-863-2375

WESTERN UNION EXHIBIT A - List of State Laws

1. Alabama Deceptive Trade Practices Act, Alabama Code Section 8-19-1, et seq.
2. Alaska Unfair Trade Practices and Consumer Protection Act, AS 45.50.471 et seq.
3. Arizona Consumer Fraud Act, A.R.S. §§ 44-1521, et seq., except matters related to A.R.S. § 36-798, et seq
4. Arkansas Deceptive Trade Practices Act, Arkansas Code Ann. 4-88-101, et seq.
5. Colorado Consumer Protection Act, Colorado Revised Statutes § 6-1-101, et seq.
6. Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110b, et seq.
7. Delaware Code Ann. Tit. 6, §§ 2511 to 2536.
8. District of Columbia D.C. Code § 28-3901 et seq. (2001).
9. Florida Deceptive and Unfair Trade Practices Act, Ch. 501 Part II, Fla Stat. (2016).
10. Georgia Fair Business Practices Act of 1975, O.C.G.A. § 10-1-390 et seq.
11. Hawaii Uniform Deceptive Trade Practices Act, Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. § 480-1 et seq.
12. Idaho Consumer Protection Act, Idaho Code Section 48-601 et seq.
13. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, et seq.
14. Indiana Deceptive Consumer Sales Act, Indiana Code 24-5-0.5-1 et. seq.
15. Iowa Consumer Fraud Act, Iowa Code § 714.16.
16. Kansas Consumer Protection Act, K.S.A. 50-623 et seq.
17. Kentucky Consumer Protection Act, K.R.S. 367.110 et seq.
18. Louisiana Unfair Trade Practices and Consumer Protection Law, La. R.S. 51:1401, et seq.
19. Maine Unfair Trade Practices Act, 5 M.R.S. §§ 207 and 209.
20. Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101 through 13- 501
21. Massachusetts Consumer Protection Act, M.G.L. c. 93A, § 1 et seq.
22. Michigan Consumer Protection Act, MCL 445.901, et seq.
23. Minnesota Consumer Fraud Act, Minn. Stat. §§ 325F.68 and 325F.69, Minnesota Deceptive Trade Practices Act, Minn. Stat. § 325D.43-.48, and Minnesota False Statement in Advertising Act, Minn. Stat. § 325F.67.
24. Mississippi Consumer Protection Act, § 74-24-1 through § 74-24-357 (1972, as amended).
25. Missouri Merchandising Practices Act, § 407.010, et seq, RSMo.
26. Montana Unfair Trade Practices and Consumer Protection Act (MUTCPA), Mont. Code Ann. § 30-l4-101 et seq.
27. Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601 et seq., and the Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 et seq.
28. Nevada Deceptive Trade Practices Act, NRS 598.0903 et seq.
29. New Hampshire Rev. Stat. Ann. 358-A.
30. New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq.
31. New Mexico Unfair Practices Act, NMSA § 57-12-1 et seq. (1967), NMSA § 57-15-1, et seq., and N. M. Admin. Code 12.2.11.
32. N.Y. Gen. Bus. Law §§ 349 and 350, N.Y. Executive Law § 63(12).
33. North Carolina Unfair and Deceptive Trade Practices Act, N.C.G.S. 75-1.1 et seq.

34. N.D.C.C. §§ 51-12-08 et seq. and 51-15-01 et seq.
35. Ohio Consumer Sales Practices Act, R.C. 1345.01 et seq.
36. Oklahoma Consumer Protection Act, 15 O.S. §§ 751 et seq.
37. Oregon Unlawful Trade Practices Act, ORS §§ 646.605 et seq.
38. Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, et seq.
39. Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1, et seq.
40. South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-10 et seq.
41. South Dakota Codified Laws Chapter 37-24
42. Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. § 47-18-101, et seq.
43. Texas - Tex. Bus. & Com. Code Ann. § 17.41 et seq.
44. Utah Code Ann. § 13-11-1, et seq.
45. Vermont Consumer Fraud Act, 9 V.S.A. §§ 2451-2466.
46. Virginia Consumer Protection Act, Va. Code §§ 59.1-196 through 59.1-207.
47. Washington Revised Code of Washington RCW 19.86.020.
48. West Virginia Consumer Credit and Protection Act, W.Va. Code §§ 46A-1-101 et seq.
49. Wisconsin Stat. §§ 100.18(1) fraudulent representations
50. Wyoming Consumer Protection Act, Wyo. Stat. Ann. §§ 40-12-101 through 114.