THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

JOSHUA DIAMOND
DEPUTY ATTORNEY GENERAL

WILLIAM E. GRIFFIN
CHIEF ASST. ATTORNEY GENERAL

TEL: (802) 828-3171
FAX: (802) 828-2154

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER
05609-1001

February 7, 2018

John A. Yanchunis
Morgan & Morgan
One Tampa City Center
201 North Franklin Street
Tampa, FL 33602
jyanchunis@forthepeople.com

Re: Public Records Request

Dear Mr. Yanchunis:

I write in response to your public records act request dated January 31, 2018. Enclosed please find all correspondence and other information provided by Solera in connection with a data security incident that took place in the Spring of 2017.

Sincerely,

/s/ Ryan G. Kriger

Ryan G. Kriger
Assistant Attorney General

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2732
david.navetta@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

April 19, 2017

By Certified Mail
Return Receipt Requested

Office of the Vermont Attorney General
109 State Street
Montpelier, VT 05609-1001

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Solera Holdings, Inc., and its affiliated companies ("Solera") to inform you of a data security incident that affected the personal information of certain Vermont residents. Solera is notifying these individuals and outlining some steps that potentially affected individuals may take to help protect themselves.

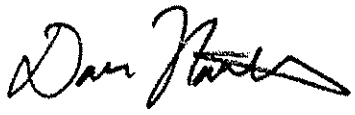
Several employees of Solera recently received alerts from the Internal Revenue Service that fraudulent income tax returns had been filed in their names for the 2016 tax year. Upon learning of these incidents, Solera promptly engaged an independent computer forensic firm to assist with an investigation into whether the company may have been affected by a data security incident. On April 9, 2017, Solera discovered that the source of the suspected data compromise was a phishing email sent to a Solera employee on February 14, 2017, purporting to be from one of the company's executives. The impersonator requested information relating to employees' 2016 Form W-2s. Before it could be determined that the email was fraudulent, the employee provided the requested information.

Solera took steps to address this incident promptly after it was discovered, including convening an incident response team and engaging external advisors to perform a forensic investigation. The company also notified impacted persons and reported this matter to the IRS, FBI, and other authorities. Solera takes the privacy of personal information seriously, and deeply regrets that this incident occurred despite various preventative efforts, including implementing employee phishing awareness campaigns and mandatory cyber security training. To prevent this type of incident from recurring, Solera will continue to train and educate employees regarding cyber security, phishing scams and related issues, and has implemented strict controls regarding the sharing of personal or sensitive information within the human resources department.

Affected individuals are being notified via written letter, which will begin mailing on or about April 14, 2017. Solera is offering two years of complimentary credit monitoring to affected individuals along with additional information about preventing identity theft and reporting fraud to the IRS. A form copy of the notice being sent to Vermont residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2732 or david.navetta@nortonrosefulbright.com.

Very truly yours,



David Navetta

DJN/smm
Enclosure

1301 Solana Blvd.
Bldg. 2, Suite 2100
Westlake, TX 76262
+1 817.961.2100

April 14, 2017

<First Name> <Last Name>
<Street Address>
<City, <State> <Zip>

Dear <First Name>,

We are writing to inform you of a security incident that may have affected certain personal information of current and former employees of Solera Holdings, Inc. and its affiliated companies ("Solera"). As a precaution, we would like to call your attention to steps you can take to help protect your information. We sincerely regret any concern this incident may cause.

What Happened?
Recently, certain employees of Solera reported receiving alerts from the IRS that fraudulent 2016 income tax returns had been filed in their names. Solera immediately formed an incident response team consisting of senior representatives from IT, legal, internal audit, and human resources, as well as external professional cyberthreat resources, to investigate whether the company had been impacted by a data security incident, determine the root cause and implement a remediation plan.

On April 9, 2017, our ongoing investigation confirmed that the source of the suspected data compromise was a phishing email that was sent to one of our employees. In that email, an unauthorized individual impersonating a Solera executive requested certain information relating to employees' 2016 Form W-2s. Unfortunately, before it was determined that the request was fraudulent, the employee provided the requested information.

Our investigation uncovered no evidence that this incident involved any wider unauthorized access to or use of any Solera computer system or network.

What Information Was Involved?
The information sent to the unknown perpetrator included your first and last name, home address, Social Security number, 2016 wage and deduction information, work email addresses, and the EINs of certain Solera group companies.

What We Are Doing
Solera takes the privacy and protection of personal information very seriously, and has previously taken various steps to try to prevent incidents like this at our company, including by sending out US-wide phishing awareness emails weeks before this incident occurred and previously implementing mandatory cyber security training for employees. We deeply regret that this incident occurred despite our preventative efforts.

We took steps to address this incident promptly after it was discovered, including convening an incident response team and engaging external advisors to perform a forensic investigation, notifying impacted persons, and reporting to the IRS, FBI, and other authorities.

What You Can Do
A new IRS unit dedicated to helping companies victimized by W-2 scams has been established, and we have notified this unit about the incident we experienced. While the IRS is taking steps to help protect you from tax-related fraud, we want to make you aware of additional steps you can take to guard against fraud or identity theft.

First, we have engaged Experian® to offer you complimentary fraud resolution and identity protection services for two years. These services help detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. To enroll, please follow these steps:

- Visit www.experianidworks.com/3bcreditone to enroll
- Provide the following activation code: **<ACTIVATION CODE>**
- Enroll by **7.31.17** (your code will not work after this date)
- You may also enroll over the phone by calling 877-890-9332 between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **XXXXXX**.

Also note that the IRS recommends that you file your tax return as soon as possible each year. If the IRS sends you a request for additional information about your 2016 tax return, please respond immediately. To further protect your personal information, you may also wish to file a Form 14039 "Identity Theft Affidavit" with the IRS to help prevent someone from filing a fraudulent tax return in your name in future tax years. For additional information from the IRS for employees impacted by W-2 scams, visit www.irs.gov/identitytheft or call their Identity Theft Hotline at 1-800-908-4490. There may also be similar resources and forms to file for individual states, so you may wish to contact your state department of revenue directly for more information.

As an additional precautionary measure and good practice, you should carefully review your credit reports for suspicious activity, accounts you did not open, or inquiries from creditors you did not initiate. You should also remain vigilant and continue to monitor your reports for unusual activity going forward . If you see anything you do not understand on your credit report, call a credit agency immediately. If you find that unauthorized accounts were opened, you should also call your local police or sheriff's office, file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

Finally, please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information
For more information about this incident, or if you have additional questions or concerns, you may contact us at the dedicated call center line we have established at (866) 578-5412. Again, we sincerely regret any concern this incident may cause you.

Sincerely,

Solera Holdings, Inc.

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Experian Membership: We have engaged Experian® to offer you complimentary fraud resolution and identity protection services for two years. You can contact Experian **immediately** in the event you experience any fraud to speak to an Identity Restoration Specialist (see below description). Be prepared to provide engagement number **DB01417** as proof of eligibility for the identity restoration services.

You have access to the following features once you activate your Experian membership:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet surveillance**: daily scanning of the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian online, please contact Experian's customer care team at 877-890-9332 by July 31, 2017.

A credit card is **not** required for enrollment in Experian IdentityWorks. The Terms and Conditions for this offer are located at **www.ExperianIDWorks.com/restoration**. You will also find self-help tips and information about identity protection at this site.

Review of Accounts and Credit Reports: As a precaution you may regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the end of this guide.

Remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the relevant institutions, the credit bureaus, the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may request an extended fraud alert if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur

fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting agency. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
Credit Freezes:
https://www.freeze.equifax.com

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts:
https://www.experian.com/fraud/center.html
Credit Freezes:
https://www.experian.com/consumer/security_freeze.html

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts:
http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page
Credit Freezes:
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page