THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

JOSHUA R. DIAMOND
DEPUTY ATTORNEY GENERAL

SARAH E.B. LONDON
CHIEF ASST. ATTORNEY GENERAL

ADDRESS REPLY TO:
CONSUMER ASSISTANCE PROGRAM
109 State Street
Montpelier, Vt 05609-1001
Website: ago.vermont.gov/cap
e-mail: ago.cap@vermont.gov

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
PUBLIC PROTECTION DIVISION
TEL: 1-800-649-2424
FAX: (802) 304-1014

June 8, 2020

Via email to: dom.amato@wcax.com

Dominic Amato
Weekend Evening Anchor/Multimedia Journalist
WCAX
dom.amato@wcax.com

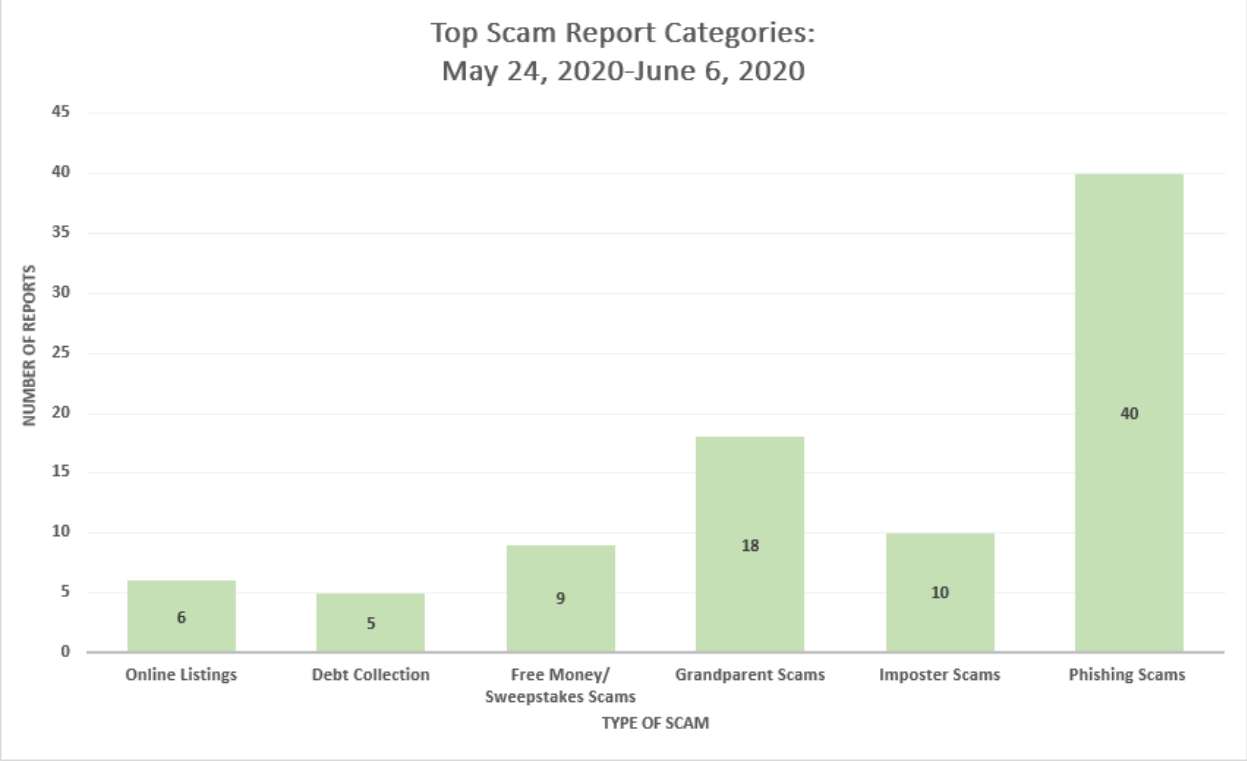
Dear Dom Amato,

I write in response to your Public Records Act request dated June 5, 2020, a copy of which attached for your convenience.

In your request, you ask that the Vermont Attorney General's Office provide "a summarizing chart of any recent scam complaints related to COVID-19, sent to the Attorney General's office. Maybe from the last week of May, to this first week of June." The Consumer Assistance Program (CAP) tracks scam reports and trends affecting Vermonters. Between May 24, 2020-June 6, 2020, CAP did not record a rise in COVID-19 related scams. To satisfy your request, CAP compiled data that reflects the types of scams reported during that time period.

Figure 1 highlights the top 6 scams reported to our office between May 24, 2020-June 6, 2020.

Figure 1: Top Scam Report Categories: May 24, 2020-June 6, 2020



The data illustrated above can also be found in the corresponding table below:

Table 1: Top Scam Report Categories: May 24, 2020-June 6, 2020

Type of Scam	Number of Reports
Online Listings	6
Debt Collection	5
Free Money/ Sweepstakes Scams	9
Grandparent Scams	18
Imposter Scams	10
Phishing Scams	40

Below you will find a description of each of the scam categories:

Online Listings Scams:

- The scam: Sometimes the scammer responds to a seller post, overpays with a check, and asks for the remainder to be wired back. Sometimes the post is for a fictitious rental property and the scammer is looking for the deposit and first month's rent to be sent immediately. Scams even happen when you are looking for that perfect puppy or pet to expand your family, but the transport of the animal is supposedly held up at the airport or elsewhere.
- How to spot the scam: If you feel suspicious, stop the sale or purchase. The scammer may ask you to wire them money, send a bank transfer, or pay using gift cards. They may not

want to talk on the phone or meet in person. Remember, you should not provide a rental deposit before signing the lease or contract in-person.
- What to do: Complete your transactions in cash and preferably in-person. If they refuse to meet in-person or talk on the phone, ignore them and end communication.

Debt Collection Scams:
- The scam: Scammers pose as debt collectors or law enforcement and say legal action will be taken against you if you don't pay them what you owe.
- How to spot the scam: If you did owe a debt, collectors are not allowed to threaten you with arrest over the phone. You can request verification of the debt, which has to be sent to you in writing. If you ask them to stop calling you, they are generally required to stop.
- What to do: Hang up the phone, and if they call again, let the call go to voicemail. If you think you do actually owe money to a debt collector or other agency, make sure you call using a trusted number.

Free Money/Sweepstakes Scams:
- The scam: A phone call or mailing claiming that you won money or a prize but have to make a payment in order to receive it. Sometimes the outreach includes a realistic-looking fake check. The check bounces and no "winnings" are ever dispersed. Often, they claim to be Publisher's Clearinghouse.
- How to spot the scam: If you actually win a major prize from Publisher's Clearinghouse, they will contact you in person. For smaller prizes (less than $10,000), winners are notified by overnight delivery services (FedEx, UPS), certified mail, or email in the case on online giveaways. They never make phone calls. An unsolicited check in the mail from an unknown sender is usually a scam.
- What to do: Never pay an upfront fee to receive winnings. If you win something, they will pay you – not the other way around. No actual contest or sweepstakes would you make you pay first to receive money.

Grandparent Scams:
- The scam: Scammers pose as grandchildren and claim to be in serious trouble, such as in prison or at the hospital. They urgently request money in the form of wired funds or prepaid gift cards. They may also claim that their voice sounds unfamiliar due to injury.
- How to spot the scam: Call your grandchild or family members on known phone numbers to ensure your grandchild is safe.
- What to do: Never wire or otherwise send funds unless you can verify the emergency.

Imposter Scams:
- The scam: There is a wide variety of imposter scams. Sometimes, the scammer pretends to be someone you know, like a love interest, friend, relative, or even a religious leader. They reach out to you online or on the phone, claiming to need money
- How to spot the scam: They ask you to send money immediately, often in the form of wire transfers or gift cards.
- What to do: If they claim to be someone you know, call the person using a verified phone number. If you receive a suspicious email, be sure to double-check the email address. If

you're feeling suspicious, get the real story and talk to someone you trust. Cut off communication with the scammer.

Phishing Scams:

- In the data summary above, the category "phishing scams" encompasses several subcategories, including (but not limited to): Social Security Number Phishing scams (15 reports), Computer Tech Support Phishing scams (6 reports), and Medicare Card Phishing scams (5 reports).
- Generally speaking, phishing scams attempt to obtain your sensitive personal information and money. Scammers try to get information such as social security number, bank account numbers, email passwords, etc. Phishing attacks are initiated by the scammer, who contact people via phone calls, computer pop-ups, scam emails, and text messages.
- **Social Security Number Phishing Scams:**
    - The scam: An attempt to obtain your Social Security number by posing as the Social Security Administration or a business. They may try to get access to your Social Security number by telling you it has been compromised or stolen, or that it has expired.
    - How to spot the scam: If Social Security (or any official agency) wanted to contact you, they would not call to ask for your personal information, especially your Social Security number, over the phone. These agencies mail communications and would never threaten you for information or payment over the phone.
    - What to do: Be wary responding to unsolicited contacts and never provide personal information to unknown contactors, especially over the phone.
- **Computer Tech Support Scams:**
    - The scam: A phone call or pop-up message on your computer claiming to be from Microsoft, Windows, or another well-known tech company. They will say there is a virus or other problem with your computer and try to persuade you to give them remote access to resolve the issue. They may also ask for immediate payment for their services.
    - How to spot the scam: Legitimate customer service information usually won't display as a pop-up. Companies like Microsoft, Apple, and Google do not call you to notify you of malware on your computer.
    - What to do: Never provide remote access to your computer to a stranger or click links from an unknown sender in an e-mail or pop-up message. If you get a call from "tech support," hang up. Also, be careful when searching for tech support numbers online. Some users have been scammed by calling illegitimate numbers for legitimate companies.
- **Medicare Card Phishing Scams**
    - The scam: Scammers are posing as Medicare saying they need your Medicare card number or Social Security Number to issue a new card or to verify medical information to keep your coverage active. The calls may also claim that coverage is expiring or in need of renewal. This scam attempts to gain access to your Medicare card number or social security number to commit Medicare fraud and identity theft.

- How to spot the scam: Neither insurance companies nor insurance agents are permitted to make unsolicited Medicare-related calls.
- What to do: Never provide personal information or payment to unknown callers. Vermonters must be particularly cautious about this scam as the calls originate from a spoofed number, appearing as a local phone number on your caller ID, and the scammer is a live caller.

Thank you for contacting the Vermont Attorney General Office. We hope this information satisfies your request and can be used to educate fellow Vermonters.

Sincerely,

/s/

[redacted]
Consumer Assistance Program
Office of the Attorney General
State of Vermont