**Top 10 Scams of 2022**
**Reported to the Vermont Attorney General's Consumer Assistance Program**

## 1. Unauthorized Order/Package Delivery

The scam: You receive an automated phone call, text message, or email claiming that you have been charged for an online order, have an outstanding balance on your account, or are sent an item you did not order. The scammer then instructs you to call a number provided in the scammer's communications to get a refund or to resolve the charge. At this point, they will ask you to provide your card number to "confirm your account" or prompt you to provide them remote access to your computer. As soon as the scammer has remote access to your device, they can access every single document, file, and transaction you have saved to your device.

How to spot the scam: Companies will not call with tech support unless you requested that they contact you. If you receive a package that you do not recall ordering, check your statement history to see if you have been charged. Packages without a return address are highly suspicious.

What to do: Hang up the phone immediately and do not call back. If you receive an email or text regarding a package delivery or order that has been made, do not click on any links. Mark the email as "Junk" or "Spam". Furthermore, never allow remote access to your devices to unknown parties. If you are concerned about charges made to your accounts, log in to your account directly and contact your financial institution. If you receive a package that you did not order, mark it return to sender and give it back to the mail carrier.

## 2. Computer Tech Support

The scam: You receive a phone call, pop-up, or email on your computer claiming to be from Norton, Microsoft, Apple, or another well-known tech company. They will make claims such as your electronic device has a virus; your device security subscription has been automatically renewed; or state you have been charged for services you did not receive or ask for. You may be prompted to click a link or call a number to contact. They will try to persuade you to give remote access to your device to fix the issue, and sometimes will even ask for immediate payment for their services.

How to spot the scam: Legitimate tech support companies do not display communications to their customers as random pop-ups on your device. Tech support will not call you to warn of security incidents, that your account has been renewed for a subscription you do not

recognize, and will not send you random links, often shortened, with instructions for you to click on URLs.

What to do: When contacted about a supposed business relationship, take steps to verify, especially if you do not remember signing up for services. Never click on links or provide remote access to your computer from an unknown email sender or pop-up message on your device's screen. If you received a pop-up message you cannot click out of, shut down, restart, or unplug your device. If you get a call from "tech support", hang up. Also, be careful when searching for tech support online. Some users have been scammed by calling inaccurate phone numbers listed online.

3. **Sweepstakes/Lotteries**

The scam: You will be notified by phone, email, or mail that you won a prize or a quantity of money. In some cases, you will even receive a realistic-looking check – but it is fake! You are instructed to pay fees and give your financial and personal information to claim your prize. They often use a legitimate sweepstakes name, like Publishers Clearing House.

How to spot the scam: Legitimate sweepstakes and contest businesses, like Publishers Clearing House and Mega Millions lottery, will contact you in person if you win a major prize. For prizes under $10,000, the notification is done through certified mail by overnight delivery services (FedEx, UPS). They will not contact you by phone, nor require a payment or processing fee to release your prize.

What to do: If it sounds too good to be true, then it's not true. You don't need to pay fees or give your financial information in order to claim a prize.

4. **Law Enforcement Imposter**

The scam: You receive a phone call unexpectedly, claiming to be a police officer, U.S. Marshall, or U.S. Customs and Border Protection. The caller threatens arrest or legal action. When you engage, urgent payment is demanded to make the problem go away. Payment does not solve the supposed problem, and they keep calling.

How to spot the scam: The police would not warn you ahead of time about a pending warrant or arrest. Using such threatening tactics intend to spike your emotional response.

What to do: Hang up on all arrest threats and report them. Watch out for similar government imposter scams that purport to be agents of government, including from the Social Security Administration, the Department for Children and Families, the IRS and more.

5. **Family Emergency/Imposter**

The scam: Scammers pose to be someone you trust and pretend to be in an emergency to convince you to send them money or will ask you for a favor. These scammers pose as grandchildren, friends, relatives, and close contacts appearing to be someone you know. Scammers impersonate people you love and play on your fears to have you send money urgently. After the initial call, you may be told a lawyer, parole officer or courtroom may contact you for further information.

How to spot the scam: Contacts come in as calls, emails, or online messages. Sometimes it's someone you haven't heard from in a while. They require urgency and ask for secrecy. You may be instructed not to speak to your loved one on the phone.

What to do: Take steps to verify. Check out if they really are who they say, even if they sound like a loved one. Slow down your response and contact someone you trust to verify if there is an emergency. You can also choose a "code word" with friends and family to verify the person is who they claim to be. If they don't know the word, they are not your friend or family member.

6. **Fake Websites/Online Listings**

The scam: Fake websites or phony listings draw you into a purchase that's likely too good to be true. Listings may include Facebook Marketplace and Craigslist posts that don't deliver after payment has been made, cheap pet sales, and websites with steep discounts. This scam can also appear in online rental listings as well as target online sellers.

How to spot the scam: Be skeptical of unrealistic offers. Watch out for requests for money in any form (gift cards, wire transfers, cash) when not made in person. Scammers likely will not want to talk on the phone or meet in person. Heed warnings in user reviews and other online commentary.

What to do: Investigate the person/profile of the seller. If their profile is new and they have no friends and photos, they are likely a scam. Research new websites you are considering doing business with by looking up online reviews and state business registrations, taking note of how long the company has been operating. Perform online searches of the business with "scam" and "complaints" to see if issues generate. Complete your transactions in cash and preferably a safe place in-person.

7. **Debt Collection**

The scam: Scammers pose as debt collectors and require immediate payment. They may claim to be familiar businesses and threaten utility disconnection or legal action.

How to spot the scam: Collectors are not allowed to threaten you with arrest over debts owed. You can request verification of the debt, which must 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 to use trusted contact information when communicating with them. You can also contact the originator of the debt to see if they sold the debt to a debt collection agency, and request they provide you with the name of the debt collector who took on the debt.

8. **Deceitful Solicitations**

The scam: You receive unsolicited communication with a deceptive promotion. Offers may appear to be from a known business, like Xfinity or DirecTV, and extend unreal offers. Solicitations may purport affiliation with a charitable cause or make low-ball offers on the sale of real estate, urging recipients to complete an enclosed one-page form contract to sign over their home.

How to spot the scam: Beware of unsolicited offers you cannot verify. Be especially weary of offers that ask you to complete the transaction in one sitting.

What to do: Hang up on unknown callers and let calls go to voicemail. When you receive mailings, take extra time to reply by inspecting the details and using your personal contacts as a sounding board. Never give over your payment information or sign on the line when you don't understand the offer or details.

9. **Identity Theft**

The scam: Your personal information is compromised and used for another's financial gain. This can look like receiving a letter about a new account opening, or the discontinuance of bills. You might stop receiving legitimate bills and other mail or start to get bills for products and services that you didn't arrange.

How to spot the scam: Beware of communications denoting unexpected bank transactions, credit card or benefit applications. If your expected bills are not showing up, or you are receiving correspondence in someone else's name, report it.

What to do: Don't give out personal information, such as your Social Security number, passwords, personal identification numbers, and financial accounts. Review your credit reports at least once a year. (You can access your credit report for free). Carefully check bank account statements and benefits to verify transactions. Shred documents and expired credit cards before you throw them out. Verify security breach notification letters received on the Attorney General's website. If your information has been stolen by an identity thief, take identity theft protection steps.

10. **Medicare Card Phishing**

The scam: Scammers will call, often with a live call and from a spoofed caller ID number, and pose as Medicare representatives to gain your personal information and money. These scams are most frequent during times of open enrollment but can occur year-round. The scammers will state they need your Medicare card number or Social Security number to keep your coverage active and verify medical information. The calls may also claim that coverage is expiring or in need of renewal. Scammers will also ask if you received a "new Medicare card."

How to spot the scam: In general, Medicare cards do not expire. Unless you have called Medicare using the 800 number on the back of your card and requested a callback, Medicare will not call you. If a phone call is required, you would receive a letter from the Social Security Administration to schedule a call. Medicare representatives will never call you in an attempt to verify your information, sell you products, tell you that your coverage is expiring, or to issue you a new card.

What to do: Never provide your Medicare number or other personal information and payment to unknown callers. In Vermont, representatives of the State Health Insurance Assistance Program (SHIP) at 1-800-642-5119 through local Area Agencies on Aging can help address Medicare questions. Other questions and concerns about Medicare coverage can be directed to Medicare at 1-800-MEDICARE.