Consumer Advocate August 2020

A COVID Twist to Common Scams

Don't let fear and uncertainty surrounding COVID-19 make you fall victim to a scam. Thieves are on the prowl with scams relating to contact tracers, economic impact payments and used cars.

The imposter scam occurs when someone pretends to be from a government or law enforcement agency such as the Internal Revenue Service or the Social Security Administration. As a result of COVID-19, scammers are even impersonating contact tracers. Contact tracers work to identify and notify anyone who may have been in contact with a person recently diagnosed with COVID-19 so those individuals can quarantine and prevent further spread of the coronavirus. Contact tracers are employed by local and state health departments, universities and nonprofit organizations. Legitimate contact tracers will ask you who you have been in contact with and where you have traveled over the past two weeks. In Ohio, contract tracers will first reach out to you via a phone call.

Contact tracers will not:

- Provide you with the name of the person who has tested positive for COVID-19.
- Ask you for your Social Security number or access to your bank account.
- Tell you to download a tracing application.

Another version of the imposter scam involves a person impersonating a government agency issuing a payment, usually a tax refund or Social Security payment. The new version of this scam involves Economic Impact Payments (EIP), also referred to as stimulus checks. As a result of the CARES Act, the majority of Americans started to see some financial relief starting in April through EIPs issued by the Internal Revenue Service (IRS). Although the majority of eligible Americans have already received the payments, there are still scammers claiming to be able to

provide payment. The IRS is the only reliable source of information about the timing of your payment. The status of your payment can be found at <u>www.irs.gov</u>.

The IRS will not:

- Offer to "expedite" payment.
- Send a link in an email or text message to receive payment.
- Ask for your bank account or Social Security number.

One recent marketing ruse is the COVID-19 "Auto Stimulus" check promotional scam. The Federal Trade Commission recently reported that fake checks appearing to be from a fictitious Auto Stimulus program were circulating to lure consumers to used car sales. There is currently no stimulus program tied to auto purchasing. Here are some precautions to make sure you are not a victim of the scam:

- If you receive a promotional flyer for an auto dealership, you can check the dealership's status at <u>www.bmv.ohio.gov.</u>
- Do not click on any links in a message promoting the stimulus check; it could include malware designed to steal your personal information.
- Do not pay for promoted vehicles with a gift card or wire transfer. These are preferred payment methods of scammers.

Consumers who suspect an unfair or deceptive sales practice should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

COVID-19 General Purchasing Questions

As consumers get used to the gradual reopening of the economy and rescheduling of events that have been postponed or cancelled, it's a good time to review policies and procedures for COVID-19 related openings and closings, ticketed events, deposits for venues and gift cards.

Having a few resources to navigate current business practices can be helpful. For general health-related information you can go to:

- The Centers for Disease Control and Prevention: <u>www.cdc.gov/coronavirus/2019-</u> <u>nCoV/index.html</u>
- The Ohio Department of Health: <u>www.coronavirus.ohio.gov</u>

Refunds of Event Tickets as a Result of COVID-19

As Ohioans adjust to the new reality of social distancing, many consumers are questioning when events they have purchased tickets for will be rescheduled or how to receive a refund for those tickets.

Most venues with canceled events are either rescheduling the events, providing refunds or are offering credits toward future events.

For canceled events that have tickets sold by major ticket distributors (i.e.: Ticketmaster, StubHub, etc.):

• Distributors will refund the full cost of the ticket and fees or provide credit for future ticket purchases.

For rescheduled events that have tickets sold by major ticket distributors:

• Original tickets will be honored at the rescheduled event.

For canceled or rescheduled event tickets sold by the venue (for example, at the box office):

- Visit the venue's website. Most major venues' websites have notices regarding cancellations or rescheduling due to COVID-19.
- Contact the customer service number located on the back of your ticket or listed on the website.

If you are unable to reach a solution with the ticket seller, you may file a complaint with the Ohio Attorney General's Consumer Protection Section. In order to file a complaint, please fill out an <u>online form</u> or call 800-282-0515.

Return of Deposits for Canceled Events

The ability to recover deposits paid for events canceled due to COVID-19 depends largely on the type of event and whether the business where the event was scheduled is still in operation. Here are a few examples of different industries and how they are generally handling the return of deposits:

- Airline flights: Most airlines are offering credit for future flights. Customers who do not want to reschedule their flight or get credit for a future trip may request a refund.
- **Cruises:** Many cruise lines are offering a 100% cash refund, or the option to put the value paid toward a future cruise, with added incentives in the form of on-board credits. If a refund is preferred, you may have to wait to receive your initial deposit. Check the company website as polices on refunds continue to be updated.

• Wedding-related expenses: The ability to receive a refund may depend upon the type of expense and how much work has been done or supplies ordered for that portion of the event. Customers with event-cancellation insurance have the best chance of receiving a full refund. Be sure to read and evaluate contracts carefully when seeking a refund or when entering into a new contract.

Gift Cards

If you purchased gift cards in recent months to support local businesses, be sure to check the policies on redemption, including:

- Time period to use the gift card
- Operational status of the business

If you are unsure about the stability of a business, it may be best to use the gift card as soon as possible.

If you suspect a scam or an unfair business practice, report it to the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

AG Yost Continues to Hold Nuisance Robocallers Accountable

After developing and launching Ohio's Robocall Enforcement Unit in March 2020, Attorney General Dave Yost has continued to take action to shut down illegal robocallers and help make Ohio the toughest state for them to operate.

In June 2020, Attorney General Yost joined six other states in filing suit against a pair of Texas businesses accused of blasting billions of illegal robocalls, including over 59 million calls to Ohioans.

The <u>federal lawsuit</u> alleges that Rising Eagle Capital Group LLC and JSquared Telecom LLC are behind a bombardment of robocalls offering extended car warranties and health care services.

More than 70 complaints reported to the Robocall Enforcement Unit were tied to Rising Eagle and JSquared. John Spiller II, owner of the businesses, and his business partner, Jakob Mears, are also named in the lawsuit. In a separate matter, Ohio Attorney General Dave Yost announced that a Texas business agreed to a permanent ban on payment processing to settle allegations that it helped scammers defraud millions of dollars from Americans.

The settlement with Madera Merchant Services LLC and its operators, Bruce Woods, Patricia Woods and Victor Rodriguez, is the result of a <u>joint complaint</u> filed in federal court by Yost's office and the Federal Trade Commission in 2019.

The complaint alleged that Madera Merchant Services, also known as B&P Enterprises, operated as a third-party payment processor, charging consumer checking accounts on behalf of unscrupulous telemarketers.

One of those telemarketers, Educare Centre Services, was allegedly behind a flood of robocalls that misled victims with false promises of consolidated credit services. Madera processed more than \$11.8 million in transactions for Educare, which remains the subject of a separate lawsuit.

Since its inception in March of this year, the Robocall Enforcement Unit has received over 20,000 reports of unwanted calls. Robocalls involving auto service warranties are the most frequently reported type of complaint as of August.

Signs of an illegal robocall include:

- The call appears to be coming from your area code but has no relation to the area.
- The call urges you to act quickly.
- The call requests that you press a number to speak with a representative or unsubscribe.
- The caller requests payment via wire, prepaid money card or gift card.

Remember, the best advice to help you combat robocalls is: Just Don't Answer!

Ohioans can report unwanted robocalls to the Robocall Enforcement Unit by texting "ROBO" to 888111, visiting <u>OhioProtects.org</u> or calling 800-282-0515.

CyberSmarts for Older Adults

With the increased use of computers, tablets and smartphones by older adults, they are more vulnerable to online scams and fraud. Whether using technology in public or at home, protect yourself and loved ones with these tips.

Internet tips

- Install and use a pop-up blocker. Pop-up blockers are often available for free and are included within some internet browsers.
- Use a secure website whenever you purchase items online. Secure web addresses begin with "https" rather than "http."
- When conducting internet searches, remember that the top search results may not always be from legitimate companies or organizations.
- To reduce security and privacy risks, log out of websites when you're finished.

Wireless/Wi-Fi tips

- Verify the specific network name with the network owner before connecting to Wi-Fi.
- Never disclose personal information passwords and credit card numbers included when using a public Wi-Fi connection.
- Assume that everyone can see what you're doing when you use a public network.
- Do not set your devices to automatically connect to any public Wi-Fi networks.

Email tips

- Never respond to unexpected requests for your personal information, even if the sender appears to have some details about you or your account. Scammers may pretend to be your bank, your credit card company or a government agency, and they may ask you to confirm your account by submitting your account number, password and/or Social Security number.
- Do not click on links, open attachments or download anything from a suspicious message, even when they appear to be from a friend or trusted source.

Social media tips

- When on social media, change privacy settings to meet your needs. Understand that when you leave your account "public," anyone can see information about you, including your pictures and names of your family members and friends.
- Watch out for scammers who may impersonate your social media friends or who may tell you that they need money or unexpectedly have money to give to you.

Computer maintenance tips

- Install and maintain an anti-virus and anti-spyware program. Set the program to update automatically or check regularly for updates because new viruses are launched all the time. Do not buy protection software and services based on telephone calls, pop-up advertisements, unexpected virus warnings or email messages claiming that your device has a virus. They are probably scams.
- Visit <u>www.staysafeonline.org</u> for a list of free security products that scan for and detect malware.

For more tips, information and resources, view the Ohio Attorney General's new publication, <u>CyberSmarts for Older Adults</u>.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.