U.S. Department of Justice Federal Bureau of Investigation *El Paso Field Office*
SAC Jeffrey R. Downey

FOR IMMEDIATE RELEASE
November 22, 2021
15:00 MST

PRESS
OFFICE (915) 832-5000
www.elpaso.fbi.gov

HO, HO, HO Holiday Scams

If you're doing online shopping this holiday season, be on the lookout for scammers trying to steal a deal, too! With more people shopping online this year, shoppers may encounter more online shopping scams.

"Scammers don't take holidays off from swindling unsuspecting shoppers," said Jeffrey R. Downey, Special Agent in Charge of the FBI El Paso Field Office. "There are a variety of ways fraudsters try to scam you during the holiday season, including through online shopping scams. As more people shop online this year, the FBI is asking the public to know the telltale signs of these scams and protect yourself and your financial information. The simplest tips can save you a lot of money: verify the legitimacy of websites before providing financial or personal information; if the deal from an unknown seller looks too good to be true it just may be a scam so do your due diligence; and do not click on e-mail or text message links from unknown senders. If you believe you have been the victim of a scam, please report it to the FBI at IC3.gov or contact the FBI El Paso Field Office at 915-832-5000."

The FBI El Paso Field Office reminds El Paso and Midland/Odessa-area shoppers to beware of scams and stay vigilant of scammers who may try to steal your money and personal information. Remember, if it looks too good to be true, it probably is!

Common Scams

Online Shopping Scams:

- Scammers often offer too-good-to-be-true deals via phishing e-mails or advertisements. Such schemes may offer brand-name merchandise at extremely low prices or offer gift cards as an incentive. Other sites may offer products at a great price, but the products being sold are not the same as the products advertised.
- Consumers should steer clear of untrustworthy sites or ads offering items at unrealistic discounts or with special coupons. The victims end up paying for an item, give away personal information and credit card details, then receive nothing in return except a compromised or stolen identity.

Social Media Shopping Scams:

- Consumers should beware of posts on social media sites that appear to offer vouchers or gift cards. Some may appear as holiday promotions or contests. Others may appear to be from known friends who have shared the link. Often, these scams lead consumers to participate in an online survey that is designed to steal personal information.
- If you click an ad through a social media platform, do your due diligence to check the legitimacy of the website before providing credit card or personal information.

Work-From-Home Scams:

- Consumers should beware of sites and posts offering work they can do from home. These opportunities rely on convenience as a selling point but may have fraudulent intentions. Consumers should carefully research the job posting and individuals or company offering employment.

Gift Card Scams:

- During the holiday season, consumers should be careful if someone asks them to purchase gift cards for them. In these scams, the victims received either a spoofed e-mail, a spoofed phone call, or a spoofed text from a person in authority requesting the victim purchase multiple gift cards for either personal or business reasons.
- As an example, a victim receives a request to purchase gift cards for a work-related function or as a present for a special occasion. The gift cards are then used to facilitate the purchase of goods and services, which may or may not be legitimate. Some of these incidents are combined with additional requests for wire transfer payments, as described in classic Business E-mail Compromise (BEC) scenarios.

Charity Scams:

- Fraudulent charity scams, in which perpetrators set up false charities and profit from individuals who believe they are making donations to legitimate charitable organizations, are common after disasters, which the FBI has seen during the COVID pandemic. Charity fraud also rises during the holiday season, when individuals seek to make end-of-year tax deductible gifts or are reminded of those less fortunate and wish to contribute to a good cause. Seasonal charity scams can pose greater difficulties in monitoring because of their widespread reach, limited duration and, when done over the Internet, minimal oversight.
- Charity scam solicitations may come through cold calls, e-mail campaigns, crowdfunding platforms, or fake social media accounts and websites. They are designed to make it easy for victims to give money and feel like they're making a difference. Perpetrators may divert some or all the funds for their personal use, and those most in need will never see the donations.

Reshipping Scams

- These scams involve fraudsters who use stolen credit cards to buy items—usually expensive items—online. Instead of having the items shipped to the billing address, the fraudster sends them to what's called a "reshipper." At the "reshipper" location, the items

are repackaged and usually sent overseas. There, they can often be sold at a high price on the black market.
- Fraudsters will convince unwitting individuals to be money mules and accept the deliveries and become the "reshipper." That person has now become part of their criminal enterprise without knowing it. Don't be a money mule!

Tips to Avoid Being Victimized

- Do your homework on the retailer/website/person to ensure legitimacy.
- Conduct a business inquiry of the online retailer on the Better Business Bureau's website (www.bbb.org).
- Check other websites regarding the company for reviews and complaints.
- Check the contact details of the website on the "Contact Us" page, specifically the address, e-mail, and phone number, to confirm whether the retailer is legitimate.
- Be wary of online retailers offering goods at significantly discounted prices.
- Be wary of online retailers who use a free e-mail service instead of a company e-mail address.
- Don't judge a company by their website; flashy websites can be set up and taken down quickly.
- Beware of purchases or services that require payment with a gift card.
- Beware of providing credit card information when requested through unsolicited e-mails.
- Do not click on links contained within an unsolicited e-mail or respond to them.
- Check credit card statements routinely. If possible, set up credit card transaction auto alerts, or check balance after every online purchase. It is important to check statements after the holiday season, as many fraudulent charges can show up even several weeks later.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Be cautious of e-mails claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan all attachments for viruses if possible.
- Verify requests for personal information from any business or financial institution by contacting them using the main contact information on their official website.
- Secure credit card accounts, even rewards accounts, with strong passwords. Change passwords and check accounts routinely.
- Make charitable contributions directly, rather than through an intermediary, and pay via credit card or check; avoid cash donations, if possible.
- Beware of organizations with copycat names similar to reputable charities; most legitimate charity websites use .org (NOT .com).
- Don't be a money mule; it's illegal!

What to Do if You Are a Victim

If you are a victim of an online scam, the FBI recommends taking the following actions:

- Report the activity to the Internet Crime Complaint Center at IC3.gov, regardless of dollar loss. Provide all relevant information in the complaint.
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.

- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.

For additional information and consumer alerts, and to report scams to the FBI, visit IC3.gov.