

'Tis The Season: Fraudsters ready to target holiday shoppers

December 7, 2022



The holiday season can be joyous, but can also be a time for fraud.

The following is from Umpqua Bank.

Tips on how to avoid popular scams

As the holiday season swings into full gear, shoppers need to maintain their vigilance in guarding against fraud. While consumers navigate the tighter budgets this year due to higher inflation, fraudsters are likely doing the same, and will be extra desperate – and motivated – to take advantage of the seasonal rush.

Holiday fraud is a big business, and criminals stand to generate hundreds of millions of dollars in illicit gains during the shopping season. Combined retail sales for November and December could top \$960 billion, according to a forecast by the National Retail Federation (NRF), an industry trade group. Fraudsters will be tapping into this volume.

Just for card payments alone, fraud rates in recent years have hovered around 7 cents per \$100 of volume worldwide, according to the Nilson Report. By that measure, for every \$100 billion in card volume during the holidays, thieves will siphon off \$70 million.

The gap between self-perception and reality

Consumer gullibility turbocharges the payday for fraudsters. Nearly half (48%) of consumers globally are confident they can recognize a scam, according to a 2022 fraud report by Visa Inc. Yet almost three in four (73%) typically respond to terms or phrases scammers commonly use in emails and text messages, such as “Win online gift card” and “Act now.”

The vulnerability of the general population is still high: 63% incorrectly believe or are unsure that online retailers such as Amazon and eBay will request login information to provide customer support, according to a November report by AARP. And 53% incorrectly believe or are unsure that payment apps such as Cash App, Zelle, or Venmo have the same consumer protections as credit cards. About 4 in 10 said they believe (incorrectly) that ads for merchandise on social media online are trustworthy.

“Fraudsters are always working to outsmart consumers, but during the holidays, their fervor is especially acute,” Umpqua Bank Executive Vice President and Head of Global Payments and Deposits Kathryn Albright said. “Criminals exploit this time of year to prey on busy individuals who are pressed for time, luring them into traps and robbing them of their hard-earned money. But taking some simple precautions will help thwart these schemes.”

Individuals need to be especially aware of common holiday tricks used by thieves, such as:

Gift card payment scams. Gift cards are a preferred method of choice for criminals, who convince consumers to pay a bogus financial obligation by purchasing gift cards and handing over the numbers to the fraudsters. Criminals also scam retailers by returning stolen merchandise to stores and receiving gift cards since they don’t have a receipt. They then sell those cards online at a discount. For the 12 months ended June 30, 74% of retailers reported this practice, according to the NRF.

Charity scams. Fake charities use the holidays to lure victims to donate to bogus enterprises. They mimic real charities and often use terms such as “federal” or “national.” Criminals sometimes pose as religious leaders, preying on the generosity of others by telling a story about people in need.

Non-delivery and non-payment crimes. In non-delivery scams, buyers pay for goods and services online, but never receive the items. For non-payment scams, it’s the merchants who are the victims, with goods and items shipped but are never paid. Losses for these two types of fraud amounted to \$337 million in 2021, according to the Internet Crime and Complaint Center (IC3), a division of the FBI.

Tips to reduce the risk of fraud

Review your account activity regularly. Everyone should review personal financial accounts often for activity to make sure there aren’t any suspicious transactions. Consumers also should carry fewer cards in

their wallets when they shop and store the others in a safe place at home.

Don't click on email links. Fraudsters are getting better at impersonating retailers. But even when it seems real, it's better just to go to the website via a browser. Bad links take consumers to fake portals, which typically ask for credit card information.

Don't give out sensitive information. When you receive a call, email, or text from someone claiming to represent your bank, or another company, do not give them your user ID or password. No legitimate company will ever ask you for this information.

Watch for key fraud terms. Consumers fall for a variety of phrases, according to a report by Visa, including "Win online gift card," "Exclusive deal," "Act now," "Click here," "Limited time offer," "Urgent," "Action needed," and "Free/giveaway." Be on the lookout and steer clear of any correspondence containing this messaging.

Stay on top of deliveries. Almost three in 10 (27%) of consumers reported having a package stolen outside their door, according to a November fraud report by AARP. Consumers should track various items for delivery. When consumers won't be at home, they should call the retailer or delivery service and try to delay the shipment or arrange to have it sent to an office or designated receiving location, such as Amazon Hub Locker.

Avoid clicking on ads. Malvertising is malicious advertising that often takes the form of pop-up ads. Similar to erroneous email links, these ads can lead you to sites that ask for personal information and credit card numbers. They can also infect your device with malware and make the season anything but merry.

Don't shop on public Wi-Fi networks. If you're shopping online, do it at home using your own private, secure network. Cybercriminals can easily tap into public Wi-Fi, so you don't want to input passwords and visit your bank account when browsing on these networks.

Use fraud alerts. Fraud alerts can be very helpful to consumers in staying on top of any suspicious activity regarding their accounts. Alerts can be tailored to transaction size, and are delivered via phone (voice), text, and email. Update any new contact information to keep accounts secure.

Use cards rather than payment apps. Cards offer more protections. Those using major brands offer \$0 liability for unauthorized charges. Peer-to-peer apps such as Venmo, Zelle, and CashApp process payments immediately, just like cash. These transactions cannot be reversed.

Use caution when buying gift cards. Don't buy gift cards outside of retailers and established companies. Look to make sure the protective stickers on the card are not tampered with. Also check to see that the PIN number on the back isn't showing. Keep your receipt, which will help identify the card in case it is stolen.

"The holidays can be a stressful time of year, but don't let the pressures get in the way of common-sense shopping," Albright said. "Taking the time to safeguard your shopping and payment information online and in person will go a long way toward preventing anguish, and real losses to your household budget."

What do if you have been compromised

Take action immediately. Call the merchant and credit card bank to report the issue. For gift card scams, reporting to the retailer might help recoup the loss if the card hasn't been used.

Notify regulators and law enforcement. IC3 tracks internet crimes, and the Federal Trade Commission monitors gift card scams. It also helps your community to report an incident to the state attorney general and local law enforcement.