FRAUD PREVENTION HOLIDAY EDITION

Community Bankers of Michigan™

Tuesday, November 24, 2026



Criminals Are Prepping For Black Friday Too

Source: Q6 Cyber

As cybercriminals prepare for the holiday shopping season, financial institutions should be aware of emerging fraud tactics being discussed across underground forums and messaging platforms. The attached article, **Criminals Are Prepping For Black Friday Too**, highlights how threat actors are actively sharing strategies to blend fraudulent transactions into the surge of legitimate Black Friday activity, making detection more challenging for banks.

To stay informed about the latest cyber threats targeting financial institutions, we encourage you to follow Q6 Cyber on LinkedIn. Their analysts regularly share intelligence gathered from dark web forums, Telegram channels, and other underground sources, providing valuable insights that can help your institution better understand and prepare for evolving fraud and cybersecurity risks.

(*Click the heading link to read more.*)

Top News

- Criminals Are Prepping For Black Friday Too
- Holiday Scams To Watch Out For
- The Naughty List: BBB's 12 Scams of the Holidays
- How to Avoid Holiday Shopping Scams in Your Search Results
- Debit Card Fraud Remains the Top Payment Risk for Financial Institutions



Holiday Scams To Watch Out For

Source: Federal Bureau of Investigation

When shopping online during the holiday season—or any time of year—always be wary of deals that seem too good to be true. Don't become a scammer's next victim.

Every year, thousands of people become victims of holiday scams. Scammers can rob you of hard-earned money, personal information, and, at the very least, a festive mood.

Scams include:

- non-delivery scams, where you pay for goods or services you find online, but you never receive your items
- non-payment scams, where you ship purchased goods or services, but you never receive payment for them
- auction fraud, where a product you purchase was misrepresented on an auction site
- gift card fraud, where a seller asks you to pay with a pre-paid card

According to the Internet Crime Complaint Center's (IC3) 2025 report, non-payment and non-delivery scams cost people more than $503 million that year. Credit card fraud accounted for another $282 million in losses.

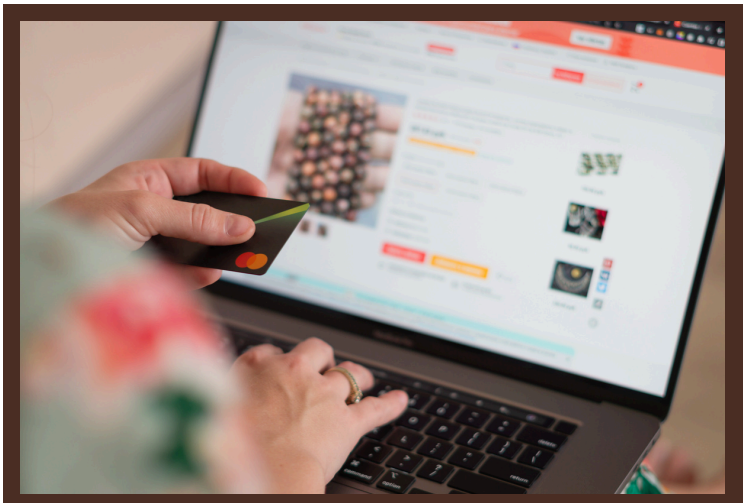
The IC3 receives a large volume of complaints in the early months of each year, suggesting a correlation with the previous holiday season's shopping scams.

Whether you're the buyer or the seller, there are a number of ways you can protect yourself—and your wallet. Remember: If it seems too good to be true, that's because it is.

Practice good cybersecurity hygiene.

- Don't click any suspicious links or attachments in emails, on websites, or on social media. Phishing scams and similar crimes get you to click on links and give up personal information like your name, password, and bank account number. In some cases, you may unknowingly download malware to your device.

(Click the heading link to read more.)



The Naughty List: BBB's 12 Scams of the Holidays

Source: Better Business Bureau

When shopping, traveling or donating this holiday season, watch out for scams trying to steal your personal information.

Be mindful of these scams that could cut into your holiday cheer.

You can avoid most of the scams on this list by taking a few simple precautions. Be cautious with social media ads promoting discounted items, holiday events, job opportunities and donation requests, as well as texts and direct messages from strangers. Scammers now use artificial intelligence to write convincing messages, build realistic websites and even copy the voices of people you know, so slow down and verify before you act. If someone asks you to pay by wire transfer, cryptocurrency, a payment app or a gift card, treat it as a red flag.

Misleading Social Media Ads:
As you scroll through your social media feed, you see products advertised everywhere. Some ads now use AI-generated videos of celebrities and influencers endorsing products they have never used.

Always research before you buy. BBB Scam Tracker receives daily reports of people paying for items they never receive, getting charged monthly for a free trial they never signed up for, or receiving an item that is counterfeit or much different from the one advertised.

(Click the heading link to read more.)



How to Avoid Holiday Shopping Scams in Your Search Results

Source: Federal Trade Commission Consumer Advice

When stores start filling shelves with decorations, you know the holiday gift-giving season is here.

The safest way to shop online is usually to go straight to a company's website. But when you're hunting for a hard-to-find item or a new store, that's not always possible. You may turn to Google or Bing, and that's where search scams can catch you.

How search scams work

Slow down before you click the top search result. Scammers often use paid search ads, too, and their ads can appear right next to those from legit companies. Sometimes their ads appear right at the top of your search. And if you click on a link for a scam site, you could end up paying a scammer or sharing personal information like your bank account number, which a scammer might use to steal your identity.

Three ways to protect yourself

Since scammers hope you won't notice their site isn't the real deal, give them the surprise this holiday season. Slow down and take these steps to avoid scams while shopping online:

- Scroll past the top results. The organic results below the paid ads are ranked by relevance, not by who paid the most. They're more likely to get you to the right place.
- Check out the seller. If you're not sure about the site, search for the company name, plus the words "complaint" or "scam." See what other people are saying about their experience.
- Type the company's web address (if you know it) directly into your browser to find the right site.

(Click the heading link to read more.)



Debit Card Fraud Remains the Top Payment Risk for Financial Institutions

Source: HUB International

Holiday Debit Card Fraud: Where the Losses Come From and How Debit Card Fraud Coverage Responds.

What the losses look like, what they cost, and how Debit Card Fraud Coverage responds.

Heading into the holiday season, debit card fraud is still the payments risk financial institutions see most often. Losses come from breached merchants, skimmed cards, and card numbers criminals generate themselves, and each one lands on the bank's balance sheet.

The Fraud Environment

- 75% of surveyed financial institutions saw debit card fraud attempts in the prior year.
- 56% of surveyed financial institutions sustained debit card fraud losses.
- 40% of total payment fraud losses at responding institutions came from debit cards.
- $3.50 to $8.75 per card to reissue cards after a large retail breach, based on recent claims paid under Debit Card Fraud Coverage.

What Claims Look Like

1. Breach-driven card compromise. A financial institution had more than 300 debit cards used fraudulently after a merchant data breach. Total losses reached about $74,000, roughly $250 per card, and no single card carried more than $500...

(Click the heading link to read more.)