A Payment Ecosystem Report by
Visa Payment Ecosystem Risk and Control

2024 Holiday Threats Report

November 2024

For the upcoming 2024 holiday season, Visa Payment Ecosystem Risk and Control (PERC) anticipates fraudsters will take advantage of holiday season-specific commerce, such as an increase in travel and in-demand goods/services, to conduct a variety of old and new scams. This report identifies the top five fraud schemes Visa PERC recommends consumers watch out for during the 2024 holiday season.

What Fraudsters Want

Visa PERC anticipates scammers will use various methods to steal cardholder information and money due to increased eCommerce and in-person shopping during the upcoming holiday season. Fraudsters' main goals are typically:

Account Takeover

Scammers take over accounts by convincing victims to hand over data, such as one-time passcodes (OTPs), that allows them to bypass account authentication. They often use phishing and social engineering to trick victims into providing OTPs.

Theft of Data

Scammers steal payment data and personal information through social engineering and malware. Tactics include phishing, fake websites, and infecting victims' devices with malware.

Theft of Funds

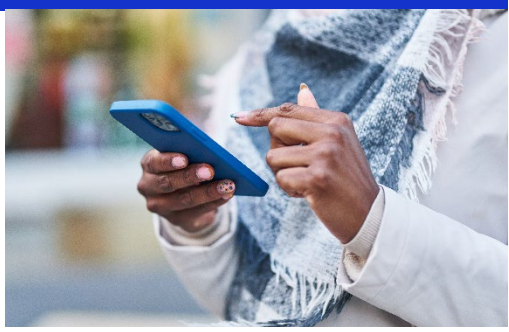
Scammers use stolen data and account takeover to withdraw funds, buy goods to resell, or transfer money. They also create fake online stores and websites to steal money from victims.

Top 5 Ways Fraudsters Will Try to Get What They Want This Holiday Season

Here are the top five ways Visa PERC expects fraudsters will attempt to take over accounts or steal data or funds this holiday season:

1. Phishing and Social Engineering
2. Scam Merchants
3. Holiday Travel Scams
4. Malicious Holiday Apps
5. Physical Theft

1. Phishing and Social Engineering



Phishing and social engineering involve scammers pretending to be trustworthy entities to steal sensitive information. Visa PERC anticipates an increase in these attacks during the holiday season. There are four main types to watch out for:

Email Phishing: Scammers send emails that look like they're from trusted organizations. Be cautious of emails asking for personal info, containing suspicious links, or creating urgency about financial matters. Common holiday scams include discounted goods/shopping deals or fake black Friday deals, heavily discounted travel deals, and spoofed well-known and in-demand brands/merchant emails.

Phone Phishing: Phishing over the phone, also called "vishing", occurs when scammers call pretending to be from financial institutions or other trusted services to trick victims into giving sensitive information. Common holiday phone scams include bank impersonation scams, utility/services impersonation scams, and charity/donation scams.

Text Message Phishing: Also known as "smishing," text message phishing involves scammers sending text messages to ask for account information or direct victims to malicious links or spoofed sites. Common holiday scams include package delivery scams, prize or free giveaway scams, and financial/account problem text messages.

Social engineering: Scammers have additional tricks up their sleeves during the holiday season and will look to specific seasonal topics to carry out additional social engineering scams, including seasonal job scams, fake charities and donation scams, and year-end flexible spending account schemes.

- **Seasonal job scams**: Scammers are likely to exploit seasonal holiday job seekers. Last year, reports of employment scams increased by 545% during the holiday season. Scammers use legitimate job boards to post fake listings, spoof real company websites, or pose as recruiters. Once a job seeker is "hired," scammers request sensitive personal information or payments for things like office equipment or background checks. This can lead to identity theft, account takeover, or the victim becoming an unwitting money mule.
- **Donation scams and fake charities**: Scammers exploit the holiday spirit by setting up fake charities to steal donations. They create websites that mimic real charities and use social media to ask for donations via cryptocurrency wallets or peer-to-peer accounts. Some even fake testimonials to build credibility. To avoid these scams, research charities on trusted websites like the IRS, UK Charity Register, or BBB's Wise Giving Alliance.
- **FSA Account Takeover Scams**: As the year ends, people with Flexible Spending Accounts (FSA) may get reminders about the "use it or lose it" rule, which forfeits unused funds at the end of the year. Scammers exploit this by sending fake emails pretending to be healthcare providers, offering ways to extend fund availability, in attempts to steal login credentials and drain spending accounts.

How to Protect Yourself from Phishing and Social Engineering

- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Ensure Multi-Factor Authentication (MFA) is implemented on all sensitive log in environments.
- Use cybersecurity best practices, including enabling anti-phishing protection on your web browser and using unique, strong passwords for different accounts.
- Do not click on unsolicited links and remain vigilant of the URLs you are visiting.
- Contact your bank directly by using the phone number or website listed on the back of your card, rather than following guidance from an email, phone call, or text message you received.

- Never provide a one-time-passcode to an unknown caller, or via email or SMS text message, and do not install Remote Access software unless instructed by a trusted system support provider.
- Review bills, bank statements, and credit reports to identify anomalies that could indicate fraud, identity theft, or if someone else has access to your account.
- Sign up for purchase alerts with your card issuer. Purchase alerts are customizable, can be received via email or text, and can be used to confirm legitimate purchases or notify you of suspicious activity.
- Use caution when posting on social media. Be aware that sharing sensitive personal information can provide criminals with clues to answer your security questions or craft believable, targeted scam messages.
- Job seekers are advised to be cautious of job postings not listed on official company websites, communications from non-company email domains, payment requests, or unusual interview procedures. These are potential red flags for scams.
- Individuals interested in making donations should research the charity on trusted websites (e.g., the IRS website, United Kingdom Charity Register, Better Business Bureau's Wise Giving Alliance, etc.), verifying the contact information on the website and reviewing the website domain to avoid fake sites. There are many resources available to equip consumers with information to help avoid donating to scams. The US Federal Trade Commission published advice on safe donation avenues and the European Anti-Fraud Office provides contacts for consumers to report fraud.
- Consumers should be cautious of unsolicited emails offering help with FSA accounts or taxes, especially if they ask for personal or financial information.
- If you suspect a scam, stop and talk to someone you trust about the situation and seek guidance from the organization's official website before acting on the suspected scammers request.

2. Scam Merchants

Scammers create fake merchants and advertise heavily discounted popular or luxury items on social media and other platforms to lure shoppers to their websites. In the past four months, **Visa PERC identified a 284% increase in fake and spoofed merchant websites as compared to the prior 4 months.** When shoppers make purchases on these fake sites, scammers steal payment data and personal information, receiving funds into their accounts. During the holiday season, these fake sites are expected to increase due to more online shopping. Scammers also spoof well-known brand websites and use search engine optimization (SEO) techniques to appear higher in search results, tricking shoppers into believing they are making legitimate purchases. This results in stolen data and payments for orders that are never fulfilled. Researchers polled holiday shoppers after the 2023 holiday season and found that **one third of respondents in the 18-44 age group said they experienced fraud from purchasing a product they found by clicking a social media advertisement**.

How to Protect Yourself from Scam Merchants

- Do not click on unsolicited links and remain vigilant of the URLs you are visiting.
- Review bills, bank statements, and credit reports to identify anomalies that could indicate fraud, identity theft, or if someone else has access to your account.
- Sign up for purchase alerts with your card issuer. Purchase alerts are customizable, can be received via email or text, and can be used to confirm legitimate purchases or notify you of suspicious activity.
- Look for the "s" – When paying online, check the URL to ensure it begins with "https://". The "s" at the end indicates a secure connection. Additionally, check that the name of the web page does not contain spelling errors or strange characters.
- Watch for scam indicators in the method of payment being requested: scammers often ask for payment in the form of wire transfers or other money transfers, reloadable or prepaid gift cards, cryptocurrency, or sending cash, since these formats are more difficult to trace.

3. Holiday Travel Scams

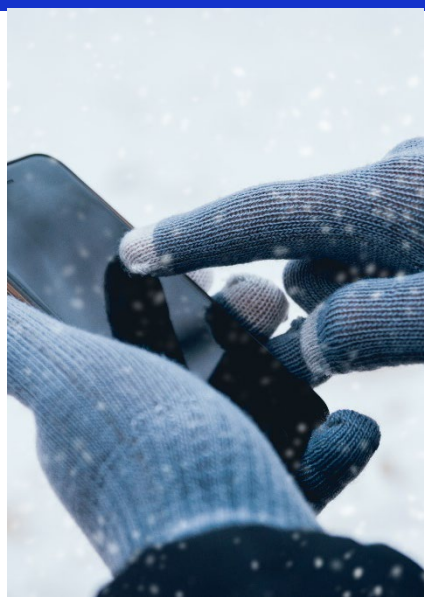
With millions traveling during the holidays, scammers target hotel, holiday rental, and airline industries. They create fake travel websites, send phishing emails about flight cancellations, and list non-existent holiday rentals to steal data and money. Common scams include:

- Fake Travel Websites: Pretending to offer travel services or spoofing major airlines to lure customers with low prices. Scammers then upcharge for amenities and cut off communication.
- Phishing Emails: Impersonating airline officials to send fake flight cancellation emails, asking for payment information to rebook flights.
- Call Center Scams: Using malicious advertising or SEO to promote fake sites, leading victims to chat with fake customer service reps who steal payment details or charge high fees to "change bookings."
- Fake Rental Listings: Posting fake accommodation listings with stolen photos and descriptions, often at below-market prices. Victims pay for non-existent rentals or are advised to pay outside legitimate platforms.

How to Protect Yourself from Holiday Travel Scams

- Verify URLs of airlines, travel, or hospitality providers.
- Avoid clicking on travel sites and advertisements from social media ads or sponsored search results.
- Research rentals thoroughly, verify addresses using other research sites, and ask family, friends, or trusted sources for travel agency, rental, hotel, and travel package recommendations.
- Use legitimate booking platforms: look up travel companies, hotels, rentals, and agents with terms like "scam," "review," or "complaint."
- Avoid uncommon payment methods like cryptocurrency, wire transfers, or gift cards as these payment methods are often untraceable and non-refundable if there's a problem.
- Be cautious of deals that seem too good to be true.
- If you suspect a scam, stop and talk to someone you trust about the situation and seek guidance from the organization's official website before acting on the suspected scammers request.

4. Malicious Holiday Apps



Scammers use holiday-themed apps to deliver malware to victims' devices. That adorable Santa tracking app that you see advertised on social media that has few or no reviews and requires you to download it by clicking a link rather than visiting a known and trusted app store…*Beware*! Scammers create new apps or imitate legitimate apps that, when downloaded, infect devices and steal sensitive data like login credentials and payment information. Visa PERC expects an increase in these malicious apps during the holiday season and advises consumers to be careful when downloading unknown apps.

How to Protect Yourself from Malicious Apps

- Always research and vet apps before downloading and only use known and trusted sources.
- Even trusted apps sources can house malicious apps, so thoroughly research and vet any apps you decide to download.
- Maintain device and software security by keeping software patched and up-to-date.
- Do not click on unsolicited links and remain vigilant of the URLs you are visiting.

5. Physical Theft

During the holiday season, scammers may physically steal payment cards or phones from consumers in crowded stores, malls, or parking lots. They often target unattended bags or wait for shoppers to exit stores to steal their cards and make purchases. Scammers also steal card data by targeting ATMs and POS terminals with skimming attacks due to increased shopping. They place devices called "skimmers" on terminals to steal payment card data. In crowded stores, scammers can install skimmers unnoticed, hiding the installation behind large items or distractions. Another method used to steal money is "digital pickpocketing," where scammers use mobile point-of-sale (MPOS) devices to conduct fraudulent contactless transactions by tapping against a victim's purse, wallet, or pocket.

How to Protect Yourself from Physical Theft

- Consumers should stay aware of their surroundings, keep wallets and purses secure and in sight, and report any theft to their bank immediately.
- Shoppers should stay vigilant and report any suspicious devices at ATMs or POS terminals to store personnel.
- In the event of a stolen card, take advantage of identity and credit monitoring services. These services may be provided by your bank/credit union, credit card provider, employer, or insurance company.