A Payment Ecosystem Report by
Visa Payment Ecosystem Risk and Control

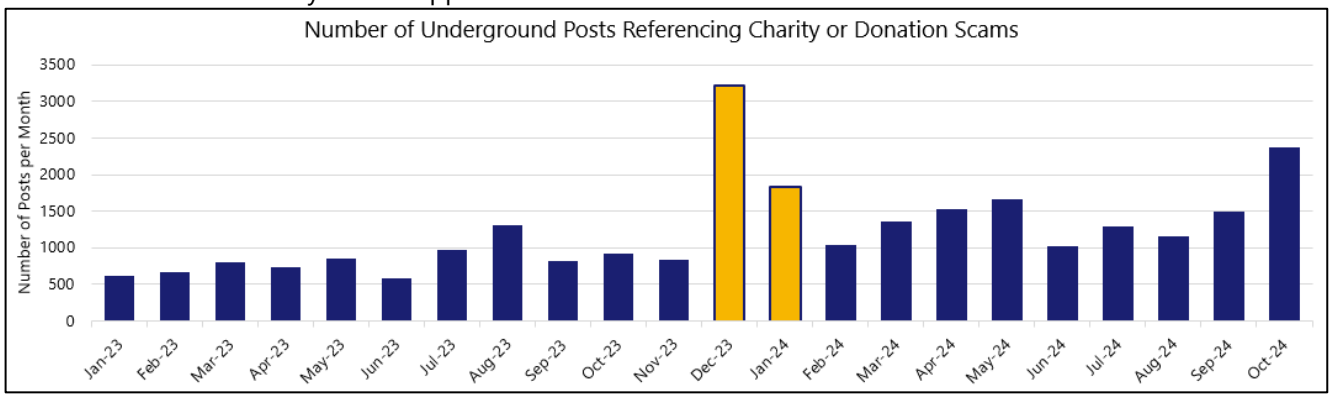
Scam Alert: Charity and Donation Scams

November 2024

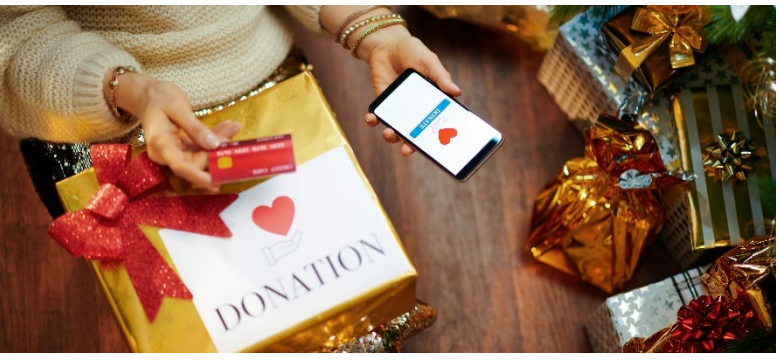
During this 2024 holiday season, scammers will take advantage of festive cheer and holiday spirit by establishing fake charities and fundraisers to scam giving individuals out of funds. Visa Payment Ecosystem Risk and Control (PERC) anticipates the number of fraudulent charities established during the holiday season will likely increase compared to non-holiday months and advises consumers to thoroughly vet any organization to which they will donate funds. This report identifies the popular charity and donation scams Visa PERC recommends consumers watch out for during the 2024 holiday season.

Scammers Are Targeting Consumers, Especially During the Holidays

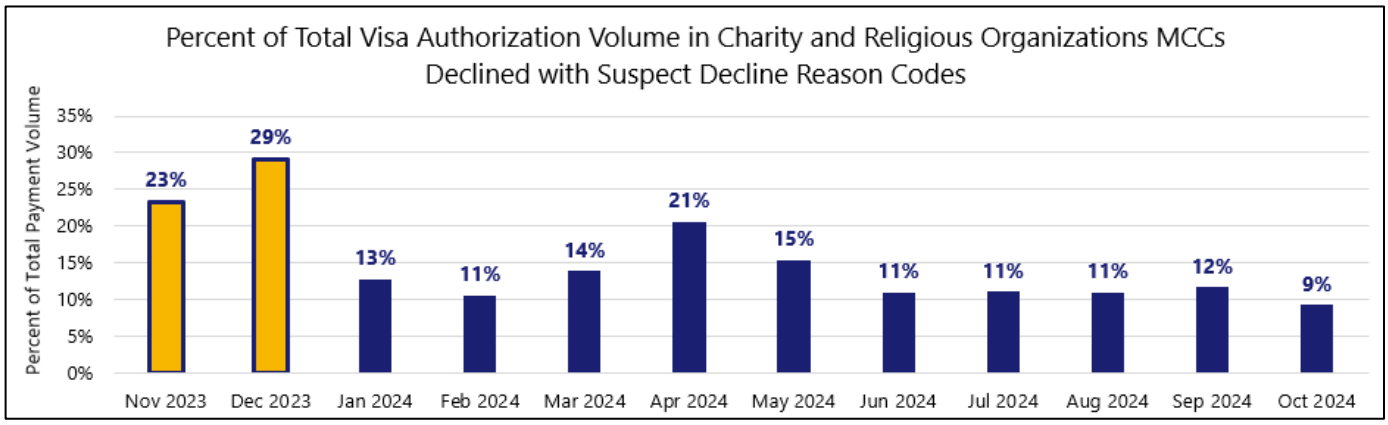
Visa PERC continues to monitor underground activity related to the development of new scams and fraud schemes targeting consumers. During the 2023 holiday season, Visa PERC identified an increase in underground chatter related to charity and donation scams during the holiday months and recently saw an increasing trend in similar chatter as the 2024 holiday season approaches.



Source: Visa Payment Ecosystem Risk and Control



Visa PERC identified a similar trend in Visa transactions where there is an increase in the number of transactions declined for "suspect reasons," including reasons like Stolen Card, Incorrect PIN, Invalid Merchant, or Suspected Fraud, during November and December on merchants within the Charity and Religious Organizations merchant categories. This indicates fraudsters may be establishing fake charity merchants and using stolen payment account information to attempt to send money to the fake charities in an effort to steal funds from victims.

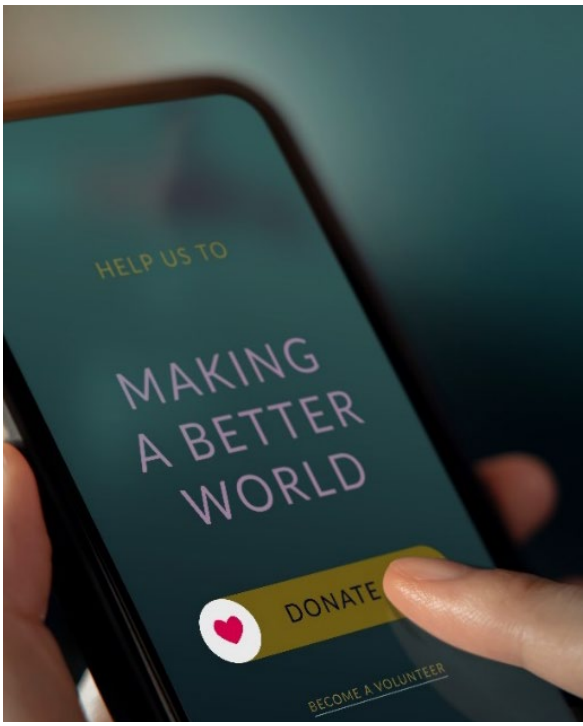


Source: Visa Payment Ecosystem Risk and Control

"Suspect declines" in the graph above includes banks declining transactions for reasons such as Suspected Fraud, Security Violation, Card Stolen, and Invalid Merchant, among other suspicious reasons. This does not include declines for reasons like data or system errors or non-sufficient funds. The increase in these suspect declines on charity and religious organization merchants during the giving season is likely due to two causes:

- Fraudsters have set up a fake charity merchant and have stolen card numbers and are attempting to "cash out" the stolen cards on the fraudulent merchants they control, or
- A cardholder is attempting to send money to a charity merchant and the transaction is flagged by the individual's banks for a possible scam; this could be that the merchant is suspicious for having invalid data, or the donation activity pattern doesn't match the account's normal spending habits, which sometimes can be an indication that the cardholder may be involved in a scam.

Donation and Charity Scammer Strategies:



1) Creating a fake charity: Fraudsters set up fake charities, creating websites and social media profiles. Fake charity websites can look very convincing and include stories and photos that pull on people's heartstrings in scammers' attempts to encourage victims to donate. Scammers also take to social media to request donations through social media posts containing links to cryptocurrency wallets or scammer-controlled peer-to-peer accounts, or the posts direct victims to the fake charity's website. Some scammers even go so far as to create additional fake social media posts from individuals claiming to have sent donations to the fraudulent charity in attempts to establish credibility for the fake post or website.

2) Imitating a real charity: Similar to the "spoofed" websites in the online shopping space, some fake charity websites are set up as an imitation of the real charity, including mimicking the layout, design, and wording of official charities, to entice victims to make donations through the spoofed website instead of the legitimate site.

These tactics, often used in combination by the same scammers, can often be lucrative for fraudsters. In a well-known 2022 law enforcement case, a New York man was arrested and charged with creating 23 fake cancer charities, some spoofing legitimate cancer charities. With names like "American Cancer Society for Children" and "United Way of New York Inc.", he registered the fake charities across the US and pocketed over $150,000 in donations made to the fake charities.

Donation and Charity Scam Tactics to Watch Out For:

Phishing

Scammers send emails and text messages or make phone calls pretending to be from a charity or religious organization, requesting donations for a wide variety of reasons. Phishing emails and texts will typically include a link that takes the victim to the fake or spoofed charity website. Scam phone calls are often made by well-organized scam call centers in which numerous scammers place mass amounts of calls to prospective victims. Scammers also post on social media using profiles created to align with the fake charity, along with paying for social media advertisements hoping victims will respond to a heartwarming post or click on a sponsored advertisement.

Types of charities scammers fake or impersonate include humanitarian relief organizations, religious organizations, law enforcement and first responder-based holiday donation campaigns, and animal welfare and environmental protection charities, among others.

Celebrity Impersonation and "Matching Scams"

As Artificial Intelligence (AI) technology gains users and becomes easier to access, scammers are also using AI to create "deepfake" images and videos of celebrities and other famous individuals and using those deepfakes to carry out donation scams. Recently, a social media platform reported deleting over 9,000 celebrity deepfake scam social media pages over a six-month period that were being used to facilitate financial scams. In charity and donation scams, celebrity deepfakes can be used to persuade people to donate to a charity, when in fact the charity may be fake and/or the celebrity doesn't actually endorse that charity. A US consumer advocate government agency also recently warned consumers that these types of celebrity endorsement deepfake scams are on the rise.

Exploitation of Natural Disasters, Regional Conflicts, and Humanitarian Crises

Current events, including regional conflicts, natural disasters, or humanitarian crises often spark an influx in fraudulent charities, due to an increase in charitable giving during natural disasters or other global crises. The Federal Bureau of Investigation (FBI) warns the public that criminals often use funds from fraudulent donation sites to fund criminal activity. In the early days of the Israel-Hamas conflict, fraudsters tried to scam unsuspecting donors with fake charities and fundraisers related to both sides of the conflict. Researchers identified over 500 different scam emails in circulation, containing links to illegitimate charity websites and containing images and news updates to evoke emotion in hopes to draw in more donations. Some of the websites also mimic the layout of the websites of official charities, to make the sites seem more legitimate. Scammers use AI to create fake photos and videos of people or animals in distress in attempts to evoke emotional responses of caring individuals to convince them to donate money.

How to Protect Yourself:

The FBI advises individuals interested in making donations to research the charity. 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, reviewing the website domain to avoid spoofed domains or hijacked URLs, searching the domain history on a domain registrar's records, and looking for notable spelling and grammar issues on the website. 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.

Be on the lookout for phishing emails, text messages, and phone calls:

- 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 login 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.
- Never provide a One-Time Passcode (OTP) 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.
- 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.
- 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.

What to do if you think you've been scammed:

- **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.
- **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.
- **Contact your bank directly** using the information listed on the back of your card or on the bank's official website. Avoid guidance from unsolicited emails, phone calls, or text messages.
- **Change your logins, passwords, and PINs**. Ensure new account information is strong and unique.
- **Check your other accounts**. Review accounts with similar usernames and passwords for abnormal activity. Change logins and passwords for those accounts.
- **Submit a fraud alert**. Place a free fraud alert with one or more of the credit bureaus. This will make it harder for someone to open new accounts in your name.
- **File IC3 and FTC reports**. The FBI's IC3 (Internet Crime Complaint Center) and US FTC (Federal Trade Commission) reports play crucial roles in addressing cybercrime and consumer protection.

- **Keep documentation**. Maintain records of all communications with your bank, including names, dates, and reference numbers. Also save copies of the IC3 and FTC reports filed. Such evidence can be valuable for resolving the account takeover and recovering any losses.

Disclaimer: This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it. All Visa Payment Ecosystem Risk and Control (PERC) Situational Intelligence Assessment content is provided for the intended recipient only, and on a need-to-know basis. PERC reporting and intelligence are intended solely for the internal use of the individual and organization to which they are addressed. Dissemination or redistribution of PERC products without express permission is strictly prohibited.