VISA

The State of Scams

Spring 2024

Organized, sophisticated threat actors targeting the most vulnerable point in the payments' ecosystem: humans.

More than one-third of adults surveyed decided not to report scams committed against them, suggesting the losses are higher than reported, according to another recent Visa survey.

Proliferation of Scams

Scams directly targeting consumers continue to increase in both complexity and volume.

While the number of individual reports of scams decreased, the total lost by individuals increased, indicating scammers are targeting individual victims with larger and more costly scams.

Below are the top scams Visa has identified.

- **Romance Scams Advance to 'Pig Butchering'**
- **Inheritance Scams**
- **Humanitarian Relief Scams**
- **Triangulation Fraud**

Learn more [Click here to download the Visa Spring 2024 Biannual Threats Report.]

Romance Scams Advance to 'Pig Butchering'

In November, the U.S. Department of Justice seized

$9M

in cryptocurrency from scam profits gained by a criminal organization perpetrating pig butchering scams.

Recovered funds are linked to

70+

individual victims targeted with a "fake crypto dashboard" [1] pig butchering scheme by an organized fraud network.

During holidays such as Valentine's Day and New Year's, romance scammers target victims with more convincing phishing campaigns, such as dating profiles and initial correspondence using AI and deepfakes.

Pig Butchering combines general romance scams with investments scams resulting in billion-dollar losses. Per Visa's study, 10 percent of surveyed adults have been targeted in a pig butchering scam.These scammers use social media, dating sites and apps to lure victims into online relationships and subsequently convince them to invest in fake crypto trading platforms.

The devastation of these scams extends past the targeted victim as they sometimes rely on human trafficking victims to initiate and conduct the scams.

[1] Crypto scam: Inside the billion-dollar 'pig-butchering' industry (reuters.com)

Inheritance Scams

Hi John, this is confidential information. It concerns your long-lost relative's multi-million-dollar inheritance, and we at Smith & Smith think it might be you. Please do not share this information with others until the process is complete.

Really? Who is this relative and what do you need from me to verify?

You must act fast to secure the funds. You'll need to pay taxes, verify your identity and account information in order to begin the money acceptance process. Click here to start.

Threat actors are capitalizing on victims' excitement for financial gain with several versions of inheritance schemes.

Typically it involves victims being notified[1] via physical mail or email with an "official-looking" letter or notification about an inheritance left by a deceased or long-lost relative. According to a Visa survey, 15 percent of U.S. adults surveyed by Visa have been targeted in inheritance scams.

Variations of the scam claim the victim is likely the heir to millions of dollars. The message appears to come from a law firm or other seemingly legitimate professional entity[2], and typically contains red flags including:

✓ **Secrecy**
An attempt to keep the victim from speaking to others who may inform the victim of the scam by telling them not to disclose the inheritance before the money arrives.

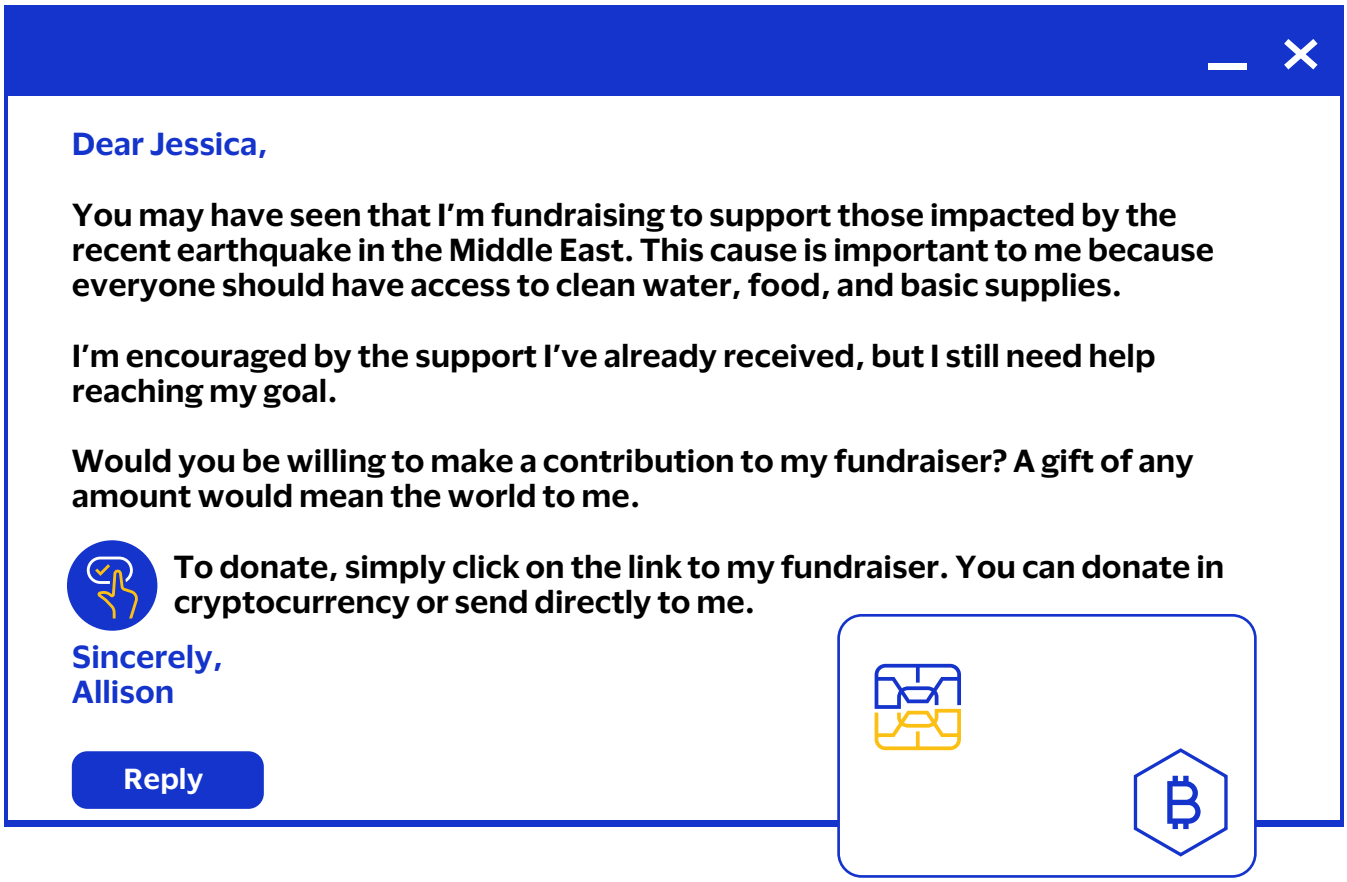
✓ **Urgency**
An attempt to get the recipient to act fast with a time-bound inheritance.

✓ **Personal Information**
The sender asks the recipient for sensitive personal identifiable information (PII) and/or payment account information.

✓ **Initial Payment**
They need to pay fees or taxes in order to begin the money acceptance process; payment is requested by money transfer, gift cards, or cryptocurrency, or for the recipient to provide their credit/debit card or bank account details.

[1] Contacted about a long-lost relative's inheritance? Hold on a minute | Consumer Advice (ftc.gov)
[2] Inheritance Scams – United States Postal Inspection Service (uspis.gov)

Humanitarian Relief Scams



Visa regularly tracks global conflicts and crises to identify tactics threat actors devise to target victims.

Whether national disaster or global conflict, threat actors look for upticks in charitable giving and exploit calls for donations across social media to defraud unsuspecting donors with fake charities, fundraisers and other scams.

Such scams request fake donations through social media posts with links to cryptocurrency wallets, often under the control of the threat actors. These social media campaigns also involve the use of posts from various individuals, likely from either fraudulent/fake accounts or from associates of the scammer, claiming they donated to the fraudulent charity, further legitimizing the scam.

Phishing emails[1] associated with these scams typically contain images and language that evoke emotion within the readers to hopefully draw more fake donations and the majority contained malicious attachments that enable the theft of victim information. Some of the fake websites resemble the layout of legitimate charities to make the scam emails more legitimate.

[1] Global Conflict Phishing Schemes (phishingbox.com)

Triangulation Fraud

Triangulation fraud impacts banks and businesses and has increasingly played a role in human trafficking.

Here, threat actors create illegitimate businesses and accompanying websites offering bargains on luxury goods/services. They then use legitimate businesses to fulfill the customer orders and monetize stolen payment accounts through a seemingly legitimate transaction. The "fake" business then requests positive ratings from the customer which improves their search engine result and boosts credibility.

Payments industry estimates financial losses to merchants due to Triangulation Fraud range from

$660M - $1B+

for 1 month in 2022 alone.[1]

Global efforts continued throughout 2023, with Interpol announcing the success of an operation targeting online scam centers with ties to human trafficking.[2]

GLOBAL LAW AGENCIES

281 INDIVIDUALS ARRESTED

5 MONTHS

149 FREED VICTIMS

[1] FS-ISAC: TriangulationFraud-WhitePaper (fsisac.com)
[2] INTERPOL operation reveals further insights into 'globalization' of cyber scam centres

Visa is committed to securing commerce

With the use of Generative AI and other emerging technologies, scams are more convincing than ever, leading to unprecedented losses for consumers. Visa is uniquely positioned to address these threats, with investments in tech and innovation reaching over $10 billion over the past five years. These investments, in addition to our ongoing education and top talent, allow us to stay ahead of scams and protect consumers.

Paul Fabara
Chief Risk Officer

How Visa Protects Consumers

Visa Risk Operations Center (ROC) instituted blocks of presumed fraudulent transactions (from June through December 2023) resulted in

49.8M+ declined transactions

for

$5.6B+

In the past seven months Visa identified

327K primary account numbers and

4.9K merchants associated with high-risk purchase return authorizations (PRA) that accounted for **$58.6M**.

Visa invested **$10B** since 2019 and employs **1,000+** cyber professionals.

Not every network can match this level of security and reliability.

In FY2023, Visa blocked **$40B** in fraud, compared to $23B in FY2022.

Methodology: This report provides an overview of the top payment ecosystem threats from June 2023-December 2023 as identified by Visa Payment Fraud Disruption team in the Visa's Spring 2024 Biannual Threats Report. The team works around the clock globally to look at macro trends bad actors are using to commit fraud with average time identifying and shutting down an attack being less than an hour. Additional survey data included in the report includes third-party data from the Consumer Scam Report commissioned with Morning Consult.