BEYOND A SCAM: CONNECTIONS TO OTHER TYPES OF PAYMENTS FRAUD

Scams can be an entry point to a broader range of illicit activity, including payments fraud and laundering of stolen funds. Criminals may convince victims to send a payment under false pretenses, but these are not always isolated one-time events. Scams also can lead to compromised information, system or device access, or be used to recruit money mules – all of which can be used by criminals to facilitate fraudulent payments, identity fraud and other types of criminal activity.

Understanding the connections that scams have to broader forms of payments fraud can aid in developing prevention and response strategies.

IMPOSTOR SCAMS AND THEIR LINKS TO BROADER FRAUD

Criminals often pose as legitimate people, businesses, government agencies or financial institutions to deceive or manipulate victims into sending money or performing a request. Impostor scams come in various forms – such as a phishing email from the "IT department," a phone call from someone pretending to be from a software company, or a text message that appears to be from a financial institution. These scams may cause the victim to share personally identifiable information, financial details or device access that can easily escalate into other types of fraud.

Account takeover. Criminals sometimes use virus pop-ups and pretend to be tech support specialists to deceive or manipulate a victim into allowing them to have remote access to their computer. Once criminals have access to a victim's computer, they can install malware and spyware, change settings and steal credentials to online accounts – such as banking, email and social media accounts.

Phishing emails that appear to be from a vendor, business executive or other trusted party also are used to gain access to accounts. Clicking on a link or attachment within the email could result in malware being installed on the user's device or prompt the user to enter credentials – giving the criminal access to the accounts and data.

Login credentials can be used to take over victims' accounts, change contact information or conduct transactions – including ACH transfers, wires or instant payment transfers – to siphon money out of their accounts. Victims' access and data on their devices are now compromised and can be used for fraudulent activity or sold on the dark web to other criminals.

Identity fraud. Criminals deceive or manipulate victims into divulging – or allowing access to – personal information. Social engineering, phishing emails and other scam tactics are used to convince a victim into performing an action that could provide a gateway into a network that leads to a data breach.

BEYOND A SCAM: CONNECTIONS TO OTHER TYPES OF PAYMENTS FRAUD

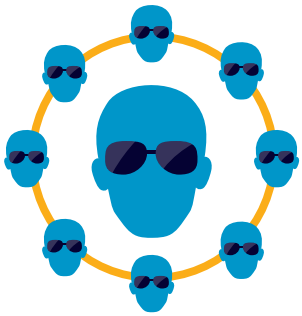
Criminals can use personally identifiable information as is or in the form of a synthetic identity to open new accounts, credit cards and loans. New accounts, credit cards and loans can be used to further their fraudulent activities – such as "cleaning" stolen funds, conducting account takeovers and committing authorized party fraud against a financial institution.

Check fraud. Romance impostors build a strong emotional connection online, then claim to face a sudden emergency – medical expenses, travel delays or family crisis. They need funds immediately, so the impostor sends a check, asking the victim to deposit it and wire part of the money back. Only later does the victim learn the check was fake, and they're left owing the refunded amount to the bank. Criminals also may pose as employers or buyers, sending checks for more than the agreed amount and asking the recipient to return the excess. This counterfeit check eventually bounces, but the money sent to the criminal is gone for good.

Money mules/laundering. Criminals often recruit money mules – someone who transfers or moves illegally acquired money on behalf of someone else – to help them move stolen funds and make it more difficult to trace the origin. A criminal may pretend to be a legitimate business with a fake employment opportunity for an accountant. Once the victim starts the new accounting job, they believe they are managing vendor payments or payroll for the company – but they are actually laundering illicit funds on behalf of a criminal.

SCAMS CONTINUE TO FUEL GLOBAL CRIME

Money stolen through scams and other types of fraud often is funneled through a complex network of accounts and transactions to conceal its original source. This network may include money mules, shell companies, fake accounts and cryptocurrency exchange services. These funds often end up funding more fraudulent and illegal activity, such as human trafficking and cybercrime.



CONCLUSION

Scams are far-reaching and part of a complex fraud ecosystem. They are a significant contributor to the ongoing payments fraud challenges – enabling identity theft, money laundering and the continued funding of the crime network. Reducing scams can decrease payments fraud, especially if individuals, financial institutions and other payments industry stakeholders work together to share information, raise awareness and strengthen fraud prevention across the board.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.