

Payment Scams: Information on Financial Industry Efforts

GAO-24-107107

Q&A Report to Congressional Requesters

July 25, 2024

Why This Matters

Scams are a significant and growing problem for U.S. individuals and businesses. Some scams result in a fraudulently induced payment, which occurs when a person with payment authority is manipulated or deceived into making a payment for the benefit of the scammer. These scams succeed by playing on a victim's emotions and exploiting vulnerabilities, often resulting in significant financial losses.

For example, losses from one type of fraudulently induced payment scam—fake investment opportunities—rose from \$3.31 billion in 2022 to \$4.57 billion in 2023, according to the Federal Bureau of Investigation's (FBI) 2023 Internet Crime Report on reported complaints. The federal government has not reported on total losses associated with fraudulently induced payments, in part due to underreporting by victims. Even when victims do report such scams, it can be challenging to recover the funds.

We were asked to review the characteristics of fraudulently induced payments and how financial institutions and peer-to-peer (P2P) payment companies mitigate the impacts of these scams. This report provides information on fraudulently induced payment scams, including reported efforts by selected financial institutions to mitigate these scams.





Key Takeaways

- Fraudulently induced payment scams can take many forms, but they generally involve scammers playing on victims' emotions to manipulate them into sending money. Some scammers are using generative artificial intelligence (AI)—technology that can create text, images, audio, or video—which is making these scams harder for victims to detect, according to select industry stakeholders and federal agencies.
- Financial institutions are generally not required under federal law to reimburse consumers for losses stemming from a fraudulently induced payment because such a payment is authorized by a person with payment authority on the account (i.e., the owner of the account or other authorized person).
- Financial institutions and P2P payment companies provide consumer education and staff training in various manners and degrees, to help identify and avoid potential scams. Additionally, select institutions and payment apps have put in place measures to slow down payments to provide the consumer an opportunity to verify the legitimacy of the payment.
- Industry representatives we interviewed recommend a multisector approach, including telecommunications and social media companies, as well as law enforcement, to address fraudulently induced payments.

What kinds of scams involve fraudulently induced payments and how are they carried out?

Well known examples of scams that result in fraudulently induced payments include romance, government impersonation, investment, and business email compromise scams according to financial industry representatives and relevant federal agencies we spoke with (see fig. 1).¹

Figure 1: Examples of Fraudulently Induced Payment Scams

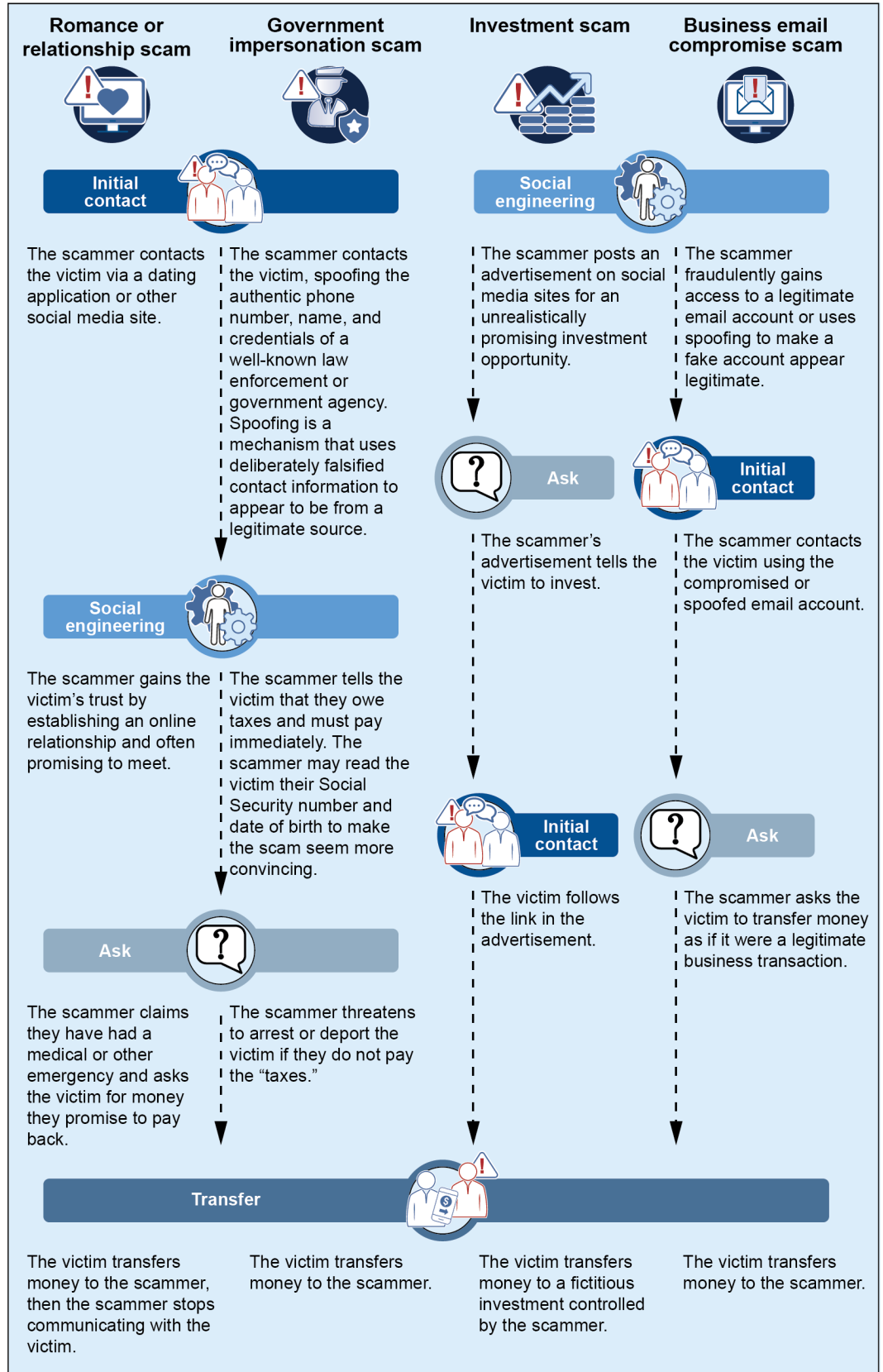
 <p>Romance/relationship scam</p>	<p>A scammer adopts a fake online identity to gain a victim's affection (romantic or platonic) and trust and then uses the illusion of a romantic or close relationship to manipulate or steal from the victim.</p>
 <p>Government impersonation scam</p>	<p>A scammer fraudulently identifies as a government official to manipulate or steal from the victim.</p>
 <p>Investment scam</p>	<p>A scammer offers low- or no-risk investments, guaranteed returns, overly consistent returns, complex strategies, or unregistered securities to manipulate or steal from the victim.</p>
 <p>Business email compromise scam</p>	<p>A scammer targets a business or individual and takes over an official account or uses email spoofing to attempt to redirect payments to an illicit account controlled by the fraudster to steal from the victim.</p>

Sources: GAO Antifraud Resource (information); Icons-Studio/stock.adobe.com, sdecoret/stock.adobe.com, GAO (icons). | GAO-24-107107

Individuals continue to fall victim to these scams because scammers use social engineering, a form of deception that uses human psychology to target and manipulate individuals and make them more susceptible to the scams, according to financial industry representatives and federal agencies we interviewed.

Social engineering tactics are becoming increasingly sophisticated. For example, a scammer may obtain a victim's personal information to better convince the victim that the scammer is calling from a federal agency. Additionally, scammers may adopt different roles to gain their victim's trust. For example, a scammer may initiate contact as a technical support person, then contact the victim impersonating a financial institution and finally, contact the victim posing as a government employee. Figure 2 illustrates scenarios of selected scams involving fraudulently induced payments and the text box below describes combined romance/ relationship and investment scams.

Figure 2: Illustrative Scenarios of Fraudulently Induced Payment Scams



Sources: GAO analysis of fraud awareness resources (information); Icons-Studio/stock.adobe.com, sdcoret/stock.adobe.com, GAO (icons). | GAO-24-107107

Combined Romance/Relationship and Investment Scams

In some cases, several types of scams may be used in combination. For example, a combined romance/relationship and investment scam, colloquially referred to by scammers as “pig butchering”, involves a series of manipulative tactics aimed at defrauding victims through fake relationships, and fraudulent investment opportunities through a website or application platform. Scammers gain their victim’s trust through a romance/relationship scam using an online platform, such as a dating app or social media site or through a seemingly misdirected text message. Once trust has been established, criminals introduce the topic of cryptocurrency investment and claim to have expertise or know an expert who can help potential investors achieve financial success. Criminals then convince their targets to use fraudulent websites or apps, controlled by the criminals, to invest in cryptocurrency. When the victim attempts to withdraw money, they are told they need to pay a fee or taxes. However, the criminals never release the funds, even if their victims pay the imposed fees or taxes. This can leave the victim financially devastated, sometimes having liquidated assets or mortgaged a home to make the “investments.” In our prior work we recommended, among other things, that the Consumer Financial Protection Bureau and other relevant regulators work jointly to adapt an existing formal coordination mechanism for collectively identifying risks posed by blockchain-related products and services, such as cryptocurrencies, and formulate a timely regulatory response.^a The recommendations to these agencies have not yet been addressed.

Source: GAO analysis of fraud awareness resources. | GAO-24-107107

^aSee GAO, *Blockchain in Finance: Legislative and Regulatory Actions Are Needed to Ensure Comprehensive Oversight of Crypto Assets*, GAO-23-105346 (Washington, D.C.: June 22, 2023).

How are criminals using technology in these scams?

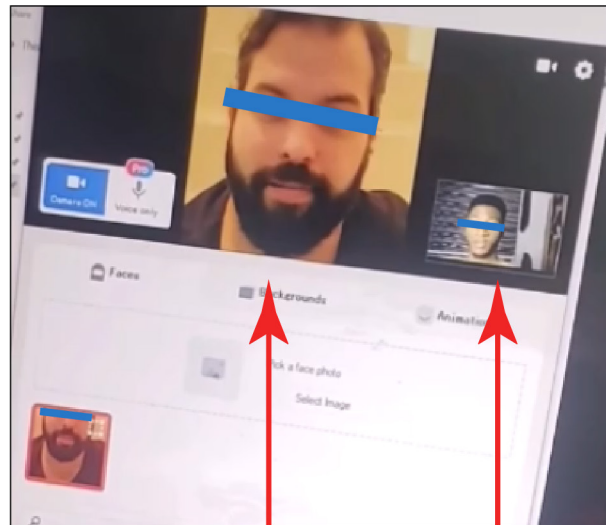
Some scammers are using technology, such as generative artificial intelligence (AI), to conduct fraudulently induced payment scams. Generative AI enables the creation of content, including text, images, audio, or video, when prompted by a user. This technology can be exploited by scammers to alter voices and images, according to our investigative research on scammers.

Use of generative AI is making these scams harder for victims to detect, according to industry stakeholders and officials we spoke with from federal agencies including the U.S. Secret Service, the Federal Reserve Board, and the Federal Deposit Insurance Corporation (FDIC).²

Scammers may use various tactics to deceive victims using generative AI, including the following:

- Through voice cloning, impersonating their family or friends, claiming to need money for an emergency;³
- Through voice cloning, impersonating business officials, urgently requesting immediate payment using changed payment instructions (such as a different account and routing number); and
- Through deepfakes (real-seeming but altered video, audio, or images) to gain trust (see fig. 3).⁴ Deepfakes allow scammers to misrepresent themselves as reflecting a variety of backgrounds, languages, statuses, and genders to build rapport with a victim.

Figure 3: Example of a Scammer's Use of Deepfake Technology



Artificial intelligence-manipulated image of a scammer

Original image of scammer

Source: GAO. | GAO-24-107107

The threat of deepfakes comes from people's natural inclination to believe what they see, and as a result, deepfakes do not need to be particularly advanced or believable to be effective in spreading misinformation, according to a report on deepfake identities published by the U.S. Department of Homeland Security.⁵

Some transnational criminal organizations have also built sophisticated websites and apps to facilitate their scams. These fraudulent platforms, such as cryptocurrency investment websites, often feature legitimate looking interfaces, "log-in" systems, and multifactor authentication to create the illusion of security, according to financial industry representatives we spoke with.⁶ In addition, it has been alleged that fake investment apps created by scammers have made their way on to well-known official stores for download to consumers.

Scammers also may use spoofing—deliberate use of false information in a caller ID—to disguise their identity, according to industry stakeholders and the FBI. To build trust, scammers use a local phone number or number of a company or government agency the victim knows. For example, scammers may impersonate a government official and claim the victim owes money to obtain a fraudulently induced payment.

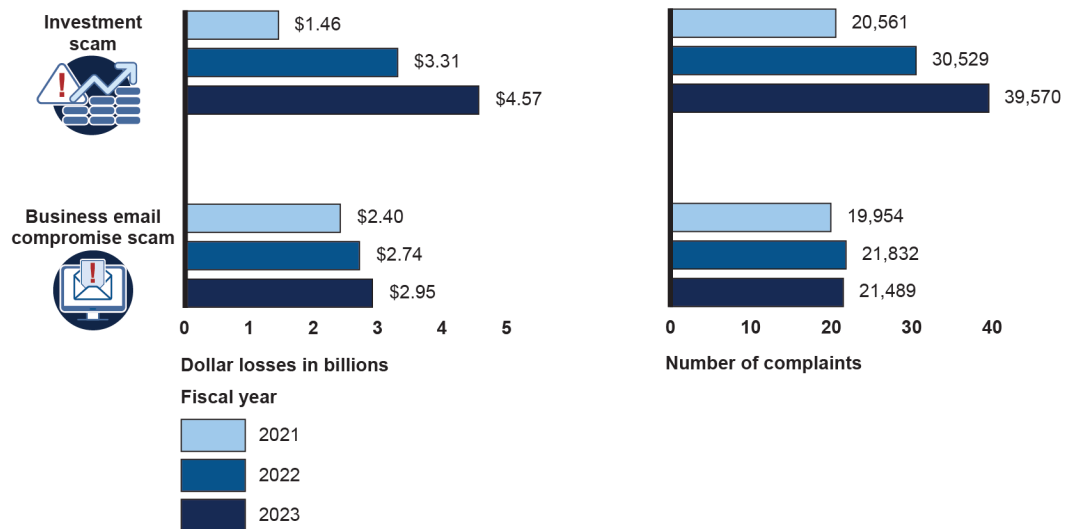
How widespread are fraudulently induced payment scams?

There are no complete measures or estimates of how widespread fraudulently induced payment scams are or the financial losses they have caused.⁷ While some federal agencies and financial institutions collect information on fraud, they do not specifically categorize the information as fraudulently induced payments as compared with other types of fraud. Officials from the Federal Trade Commission (FTC), the federal agency that seeks to protect consumers from deceptive or unfair business practices, told us this is due to the highly varied nature of these scams and the limitations of consumer self-reporting.

However, data from two federal agencies offer insights into the frequency and financial impact of certain scams, which can include fraudulently induced payments.⁸

- FTC.** According to the FTC's Consumer Sentinel Network Data Book, consumers reported losing over \$10 billion to fraud in 2023. Impersonation scams accounted for nearly \$2.7 billion of these losses, resulting from 853,935 reports.⁹ These scams include people falsely claiming to be a romantic interest, relative in distress, government representative, well-known business, or technical support expert. Additionally, consumers reported losing \$4.6 billion to investment-related fraud in 2023, stemming from 107,699 reports of scammers offering fake investment opportunities.¹⁰
- FBI.** According to the FBI's Internet Crime Complaint Center's 2023 Internet Crime Report, individuals reported losing \$4.57 billion to investment scams and \$2.95 billion to business email compromise scams in 2023 (see fig. 4).¹¹ These figures stem from 39,570 complaints and 21,489 complaints, respectively. The number of complaints of scams, and the amounts of losses, reported to the Internet Crime Complaint Center generally grew in the past 3 years, according to data.¹²

Figure 4: Financial Losses and Number of Complaints Related to Investment and Business Email Compromise Scams Reported to the Federal Bureau of Investigations, Fiscal Years 2021 through 2023



Sources: Federal Bureau of Investigation's Internet Crime Reports 2021-2023 (data); Icons-Studio/stock.adobe.com (icons). | GAO-24-107107

These measures have limitations, as they capture some types of scams and rely on victim reporting. Studies have found that a substantial portion of victims of fraudulently induced payment scams never report the scams. For example, the FTC reported that its 2005-2017 mass-market consumer fraud surveys suggest that less than 3 percent of consumers who experienced fraud reported it to a government entity.¹³

Estimates can be used to approximate the extent of scams beyond what can be directly counted through reported complaints. However, available estimates encompass various types of fraud and not just fraudulently induced payment scams. For example, the FTC estimated that consumer losses to fraud in 2022 may have been as high as \$137.4 billion.¹⁴ This estimate assumes a 2 percent reporting rate for losses of less than \$1,000 and a 6.7 percent reporting rate for losses over \$1,000. The FTC also estimated that if it assumed all individuals who





experienced a loss of \$10,000 or more reported it, consumer losses to fraud would have been estimated to have been \$20.5 billion in 2022.

The Global Anti-Scam Alliance, an international knowledge-sharing organization, estimated Americans lost \$159 billion to scams in the period from July 2022 through August 2023.¹⁵ This estimate was calculated by assuming an average \$2,663 loss per scam and that 23 percent of the U.S. adult population had been scam victims that year.

What are examples of enforcement actions involving fraudulently induced payments that have been pursued by the Department of Justice and federal regulators?

The Department of Justice (DOJ) and federal regulators have pursued criminal and civil enforcement actions against entities charged with scams involving fraudulently induced payments. Figure 5 provides examples of adjudicated cases pursued by DOJ.¹⁶

Figure 5: Selected Examples of Criminal Cases Brought by DOJ for Scams Involving Fraudulently Induced Payments

Type of scam	Description of losses	Impacts
 <p>Romance scam</p>	<p>Victims lost more than \$11.8 million in romance scams organized by a coordinated group of scammers.</p>	<ul style="list-style-type: none"> ● In 2023, seven individuals were sentenced to between 60 months in prison to probation. ● The individuals were ordered to pay approximately \$11.8 million in restitution.
 <p>Romance scam</p>  <p>Business email compromise scam</p>	<p>Victims lost at least \$30 million to romance scams, business email compromise scams, and other scams perpetrated by a large-scale fraud ring.</p>	<ul style="list-style-type: none"> ● From 2020 to 2023, 41 individuals were sentenced to up to 97 months in prison. ● The individuals were ordered to pay up to \$9 million in restitution.
 <p>Government impersonation scam</p>	<p>Over 2,700 victims lost more than \$2.4 million in a government impersonation scam.</p>	<ul style="list-style-type: none"> ● In 2024, an individual was sentenced to more than 30 months in prison. ● The individual was ordered to pay over \$2 million in restitution.

Sources: GAO analysis of Department of Justice (DOJ) information; Icons-Studio/stock.adobe.com, bsd studio/stock.adobe.com, GAO (icons). | GAO-24-107107

DOJ has also brought indictments in cases related to combined romance/investment scams. In one case, DOJ alleges victims lost more than \$80 million through at least 284 transactions. In another case, DOJ alleges victims lost at least \$73 million. Both cases are currently pending.

In addition, the FTC and the Consumer Financial Protection Bureau (CFPB) have taken civil actions related to such scams. For example, the FTC has brought cases against companies using spoofed caller ID information to send robocalls, including one company that impersonated the Social Security Administration.¹⁷ The FTC also has taken action against companies for facilitating consumer harm by allowing scammers to use their payment systems to perpetrate romance and other scams.¹⁸ Similarly, the CFPB brought charges in March 2021 against a company for knowingly processing payments for companies engaged in internet-based technical-support fraud.¹⁹

Are financial institutions required by federal law to reimburse consumers who are victims of fraudulently induced payments?

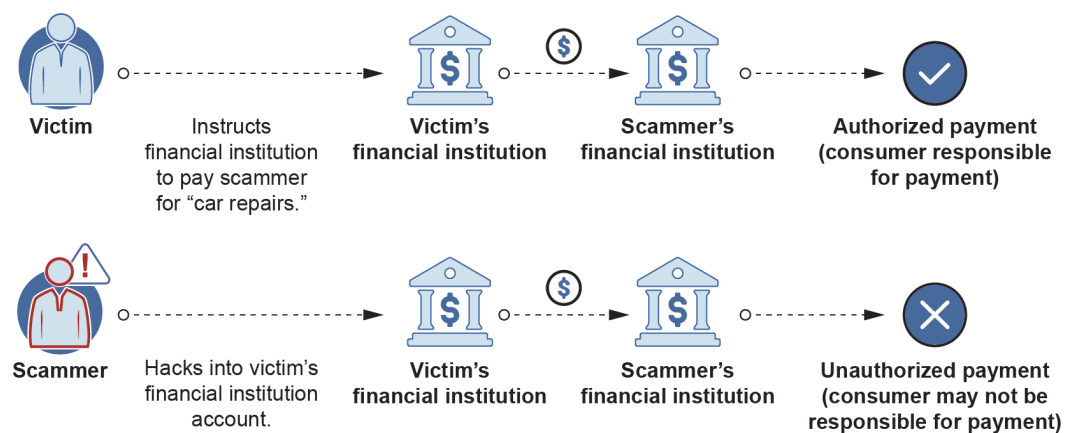
Generally, no. If a consumer is fraudulently induced to authorize a payment from their account, the consumer may be responsible for the payment under federal law, notwithstanding the circumstances because they authorized the payment.²⁰ The Electronic Fund Transfer Act, as implemented by Regulation E, is the primary federal law that governs who is liable (i.e., responsible) for a fraudulently induced payment.²¹ Regulation E applies to financial institutions, which covers both depository institutions, such as banks and credit unions, and nondepository institutions, which can include entities such as P2P companies.²²

Generally, under Regulation E, a consumer is responsible for payments from their account that have been authorized.²³ In contrast, when an unauthorized payment is made from their account, the consumer may not be held responsible for that payment in its entirety; rather, the financial institution holding the account may bear some responsibility. Consumers can only be held responsible under Regulation E for an unauthorized payment up to the amounts prescribed in the regulation (e.g., up to \$50, if the consumer notifies the financial institution within 2 business days after learning of the loss or theft of the access device that was used to initiate the unauthorized payment).²⁴

Under Regulation E, a payment is defined to be “unauthorized” when the payment made from the consumer’s account is not made by that consumer (or a person who otherwise has authority to initiate the payment) and the consumer receives no benefit from the transaction.²⁵ In the case of a fraudulently induced payment, the scammer induces the consumer victim to make the payment and send it to the scammer for the scammer’s benefit. Under Regulation E, this generally would be an authorized payment. Accordingly, the consumer would be responsible for the payment and the financial institution would have no obligation to reimburse the consumer for their loss.²⁶

For example, if Scammer convinces Victim under false pretenses to send Scammer \$1,000 for car repairs and Victim uses their bank account to electronically send \$1,000 to the account of Scammer, this is an authorized payment under Regulation E, because Victim sent the funds themselves. In this case, the financial institution holding Victim’s account would generally not be required to reimburse Victim, pursuant to Regulation E. (see fig. 6)

Figure 6: Illustrative Scenarios of Consumer Responsibility for Payment under Regulation E



Sources: GAO (information); Icons-Studio/stock.adobe.com, GAO (icons). | GAO-24-107107

If a consumer reports a fraudulent payment to a financial institution (i.e., asserts an “error” on the account), a financial institution is required to investigate the transaction to determine whether the consumer or the financial institution is

responsible for the payment, pursuant to its error resolution obligations under Regulation E.²⁷ This investigation determines whether the payment was authorized or unauthorized and, accordingly, who is responsible for the payment and in what amount.²⁸ The financial institution has up to 10 business days, or up to 90 days in certain circumstances, to complete its investigation, upon receipt of notice from the consumer that they believe an “error” has occurred. Once the investigation is complete, the institution must report the results to the consumer within 3 business days. If the investigation determines that an error occurred as relevant here, there’s a determination that an unauthorized payment occurred — the financial institution must correct the error (e.g., reimburse the consumer).

How does the financial industry mitigate fraudulently induced payments?

According to our interviews with members of the financial industry, including representatives of select financial institutions, the industry seeks to mitigate fraudulently induced payments through consumer education, staff training, and process and technology solutions. Financial institution representatives informed us that these activities are part of financial institutions’ programs to combat fraud and other illicit financial activity, some of which help meet their obligations under the Bank Secrecy Act.²⁹ Actions include, for example, the following:

Consumer education. Institutions stated they educate consumers through various channels, including websites and app notifications, mailers, and outreach to specific groups such as older Americans in assisted living facilities or medical facilities. For example, one financial services company we spoke with worked with an online media company to create a website explaining how to spot potential scams and what steps consumers can take to protect themselves.³⁰ While financial institution representatives and federal regulators told us they consider consumer education important, they also noted its limitations. They explained that consumers often ignore education campaigns believing they will not be scammed.³¹ Therefore, focusing on implementing effective fraud prevention methods is imperative.

Staff training. Financial institutions provide training to their front-line staff, including tellers and managers to help them identify potential fraud. This training includes recognizing red flags for transactions that might be fraudulently induced. It also includes learning interdiction techniques to use when fraud is suspected. For example, representatives from one credit union we spoke to said the credit union provides tellers a series of questions to ask consumers if they suspect fraud. Another financial institution uses video calls to explain to consumers that they may be the victim of a scam. Additionally, the Financial Crimes Enforcement Network (FinCEN) issues public and nonpublic advisories to financial institutions concerning threats and vulnerabilities, including fraud. These advisories may provide typologies—categories of fraud—and red flags that aid in monitoring as well as guidance to address these threats. According to FinCEN, financial institutions may use this information to train staff and enhance antifraud monitoring systems.

Slowing down the payments process to combat fraud. Financial institutions and payment apps have reported putting in place additional measures to slow down payment transactions, giving consumers a chance to verify the payment’s legitimacy. For example, one institution said it uses popups and warnings before a consumer can make a transaction such as to verify the consumer knows the recipient and wants to move forward with the transaction. Additionally, institutions and payment apps reported limiting the number or dollar amount of transactions allowed per week.

Investments in technology and expertise. Financial institutions have invested in advanced technology and expertise to enhance fraud detection and prevention. Representatives from our selected financial institutions told us they had enhanced their fraud monitoring systems and data analytic tools and hired specialized staff such as data scientists. Institutions also stated they were using AI or machine learning to help monitor transactions for fraud and other suspicious activity. They noted the importance of monitoring both outgoing and incoming payments due to the increased use of “money mule” accounts. Such accounts are typically used to transfer fraudulently obtained funds, often out of the country by an unwitting consumer on behalf of a scammer. Institutions and other financial industry representatives told us that technology for fraud monitoring is expensive, especially for real time monitoring. Larger institutions explained to us they already have made such investments, but these technologies may represent significant capital costs, especially for smaller institutions. Financial institutions stated that additional investments in technology and expertise could reduce their ability to offer services to customers, such as education for first time homebuyers or other services some of which may specifically benefit low-income consumers.³²

What does the financial industry see as some challenges in mitigating fraudulently induced payments?

Financial institutions and other industry representatives cited the human elements as the greatest challenge in preventing scams that involve fraudulently induced payments.

Convincing consumers that they can fall victim to fraud. Financial institutions face a challenge in effectively conveying to consumers fraud warnings and helping consumers better understand how scams play out. Despite efforts to educate consumers, financial institution representatives told us many consumers believe they will not fall victim to fraud. Institutions reported that consumers often ignore scam warnings until it is too late. As scams have become more sophisticated more people are falling victim. According to an April 2024 FTC report, its Scams Against Older Adults Advisory Group recently reviewed research that showed consumer education can be effective in preventing scams, but that more research is needed to help develop effective campaigns and warnings.³³

Preventing a consumer from sending a fraudulent payment. Financial institutions reported difficulty preventing victims from making payments even once they have been informed of the scam. Sophisticated social engineering tactics manipulate victims, sometimes making them unwilling to believe they are being scammed. Further, financial institutions may hesitate to intervene, such as by refusing to complete the transaction, for fear of losing the customer. For example, officials from one financial institution said that if they refuse to complete the transaction because they suspect fraud, they risk customers closing their accounts and going to another financial institution that will process the transaction. However, according to the FTC, third-party intervention by a financial institution can be effective. A 2019 study from the FINRA (Financial Industry Regulatory Authority) Investor Education Foundation, the Better Business Bureau, and the Stanford Center on Longevity conducted a survey of Americans and Canadians who reported a scam. They found that in cases where a third party intervened, 51 percent of victims were able to avoid losing money.³⁴

What other sectors did select financial industry members indicate could help reduce fraudulently induced payments?

While financial institutions and industry representatives we spoke with acknowledged that they play a role in stopping fraudulently induced payments, they noted that a solution will require a multisector approach. In particular, they cited the key roles of telecommunications and social media companies, and of law enforcement agencies.

Telecommunications and social media companies. Financial institutions and industry representatives we spoke with said they believed telecommunication and social media companies could play a greater role in reducing these scams by making it more difficult for scammers to communicate with potential victims. Other countries have begun addressing fraudulently induced payments with similar strategies. For example, the Australian government is piloting an SMS Sender ID Registry with telecommunication companies that provides message headers for texts from legitimate businesses, which make it difficult for scammers to impersonate these companies over text.³⁵ In the United Kingdom, social media companies and online service providers signed the Online Fraud Charter. This voluntary agreement commits them to protect users from fraud through different means including blocking fraudulent material on their platforms, taking down fraudulent advertisements, and having a mechanism for users to report fraudulent content.³⁶

Law enforcement. Financial institutions and industry representatives we interviewed told us that law enforcement could play more of a role in deterring scams involving fraudulently induced payments by increasing the number of investigations and prosecutions of fraudulently induced payments. One industry representative we spoke with said that doing so might decrease instances of fraudulently induced payments because it could demonstrate to other scammers that there are consequences for this behavior.

The FBI uses information contained in reports from consumer to initiate investigations to include fraudulently induced payments. However, according to a study based on FTC surveys, consumers underreport fraud, including fraudulently induced payments.³⁷ Such underreporting could impact the FBI's ability to identify patterns and commonalities among consumer reports, and deconfliction efforts. Additionally, according to FBI officials we spoke with, some cases of fraudulently induced payments may not be investigated because individual scam reports may not provide sufficient information to identify and prosecute suspects and may involve relatively low dollar amounts per individual victim. Therefore, investigating each case individually may not be the most effective use of resources. In addition, fraudulently induced payment scams may involve transnational criminal enterprises located in foreign countries, thereby increasing the complexity in investigating these types of cases, according to the FBI.

A local prosecutor we interviewed who leads a task force specializing in investigating and tracking assets related to combined romance/relationship and investment scams stated that victims who report scams to law enforcement are often told that law enforcement does not have the resources to investigate.³⁸ The prosecutor, also told us that federal law enforcement rarely gets involved in individual asset recovery because such cases typically involve smaller losses.

Despite these challenges, law enforcement agencies have investigated and prosecuted cases of fraudulently induced payments. Federal agencies, including the FBI's Internet Crime Complaint Center's Recovery Asset Team (RAT) and FinCEN's Rapid Response Program, have been able to freeze and support the recovery of funds stolen through fraudulently induced payments. For example, FinCEN's program works with law enforcement and foreign Financial Intelligence

Units (FIUs) to share information about cyber-enabled financial fraud. FinCEN encourages the FIUs to interdict fraudulent transactions, freeze funds, and stop or recall payments under their legal authorities.

Agency Comments

We provided a draft of this report to the CFPB, Department of Homeland Security, DOJ, FDIC, Federal Reserve, FTC, National Credit Union Administration, Office of the Comptroller of the Currency, Department of State, and Treasury for review and comment. The CFPB, DHS, DOJ, FDIC, FTC, and Treasury provided technical comments. In addition, NCUA provided a formal response (reproduced in appendix I).

How GAO Did This Study

To identify the characteristics of fraudulently induced payments, we reviewed publicly available reports from the FBI and the FTC that summarize data on complaints from consumers and businesses who report being a scam victim.³⁹ We also conducted a literature review of studies that measure or estimate the extent of fraudulently induced payments published between January 2019 and June 2024. We identified these studies from peer-reviewed journals by searching various databases, such as Scopus and SSRN.com. We also asked stakeholders we interviewed to recommend additional studies. Additionally, we conducted investigative research of scammers to identify techniques and tools that may be used to perpetrate scams resulting in fraudulently induced payments on two online social networking sites.

To identify how financial institutions and federal agencies address fraudulently induced payments, we interviewed officials from 10 federal agencies (CFPB, the FBI, Federal Deposit Insurance Corporation, Federal Reserve, the FTC, National Credit Union Administration, Office of the Comptroller of the Currency, Department of State, Secret Service and Treasury's Office of Terrorist Financing and Financial Crimes and FinCEN). Additionally, we reached out to four financial industry trade groups to solicit their views and also request assistance in identifying member institutions (American Bankers Association, Americas Credit Unions, Bank Policy Institute, and Independent Community Bankers Association). With the assistance of these trade groups, we contacted and interviewed representatives from nine financial institutions including credit unions and banks. We also interviewed two payment application companies that allow for P2P payments and three companies that help the financial industry mitigate fraud. We selected these trade groups and institutions because they represent a mix of financial institution types and sizes. We also met with six knowledgeable stakeholders—people who have experience working to combat fraud, including one local prosecutor, to better understand the types of scams they have seen resulting in fraudulently induced payments and the extent to which these scams are occurring. These stakeholders were identified through our prior work on fraud, other knowledgeable stakeholders, and research on fraudulently induced payment scams.

To describe applicable federal law, we reviewed The Electronic Fund Transfer Act and its implementing regulation, Regulation E, as well as Regulation Z. In addition, we interviewed officials from CFPB, the FTC, and the federal financial regulators to understand the requirements under the law and, where applicable, their process for handling a consumer complaint.

To identify recent federal enforcement activity involving fraudulently induced payment scams, we reviewed DOJ press releases as of June 2024. For identified cases, we obtained relevant court documents by searching Public Access to Court Electronic Records.⁴⁰

We conducted this performance audit from October 2023 to July 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

List of Addressees

The Honorable Sherrod Brown
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Robert P. Casey, Jr.
Chairman
Special Committee on Aging
United States Senate

We are sending copies of this report to the appropriate congressional committees, the Director of the Consumer Financial Protection Bureau, the Chair of the Federal Deposit Insurance Corporation, the Chair of the Federal Reserve, the Chair of the Federal Trade Commission, the Secretary of the U.S. Department of Homeland Security, the Attorney General of the United States, the Chairman of the National Credit Union Administration, the Comptroller of the Currency, the Secretary of State, and the Secretary of the Treasury. We are also sending informational copies to other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

GAO Contact Information

For more information, contact: Rebecca Shea, Director, Forensic Audits and Investigative Service, Shear@gao.gov, (202) 512-6722, or Michael E. Clements, Director, Financial Markets and Community Investment, Clements@gao.gov, (202) 512-8678.

Sarah Kaczmarek, Acting Managing Director, Public Affairs, Kaczmareks@gao.gov, (202) 512-4800.

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

Staff Acknowledgments: Tonita Gillich (Assistant Director), Rachel Siegel (Analyst-in-Charge), Bri Bovbjerg, Lauren Capitini, Leia Dickerson, Colin Fallon, Lydie Loth, Lauren Kirkpatrick, Moon Parks, Patricia L. Powell, Joseph Rini, and Sabrina Streagle.

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).

Visit GAO on the web at <https://www.gao.gov>.

This work of the United States may include copyrighted material, details at <https://www.gao.gov/copyright>.

**Appendix I: Comments
from the National Credit
Union Administration**



National Credit Union Administration
Office of the Executive Director

July 11, 2024

Rebecca Shea
Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Shea,

We reviewed GAO's draft report (GAO 24-107107) entitled *Payment Scams: Information on Financial Industry Efforts*. The report highlights valuable information about fraudulently induced payment scams. The NCUA will continue to educate credit unions and consumers about payment scams, including on our consumer facing website www.mycreditunion.gov.

Thank you for the opportunity to review and comment on the draft report.

Sincerely,

A handwritten signature in cursive script, appearing to read "Larry Fazio".

Larry Fazio
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320

Endnotes

¹Other fraudulently induced payment scams mentioned in our interviews with federal agencies, financial institutions, and financial industry representatives included tech/customer support, grandparent/person in need, and bank/financial institution impersonation scams. In addition, these scams can be used for types of fraud other than fraudulently induced payments. For example, victims may be induced to reveal personal information that can be used to commit identity theft.

²Generative AI systems create responses using algorithms that are trained often on open-source information, such as text and images from the internet. See GAO, *Science & Tech Spotlight: Generative AI*, GAO-23-106782 (Washington, D.C., June 13, 2023).

³To promote the development of solutions to protect consumers from the misuse of AI, the FTC held the Voice Cloning Challenge in January 2024. The event was an exploratory competition with the goal of fostering breakthrough ideas on preventing, monitoring, and evaluating malicious voice cloning. According to the FTC, the winning submissions demonstrate the potential for cutting edge technology to help mitigate risks of voice cloning in the marketplace. Federal Trade Commission, Press Release, *FTC Announces Winners of Voice Cloning Challenge* (Apr. 8, 2024).

⁴ See GAO, *Science & Tech Spotlight: Deepfakes*, GAO-20-379SP (Washington, D.C.: Feb. 20, 2020); and *Technology Assessment: Artificial Intelligence: Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 18, 2018).

⁵U.S. Department of Homeland Security, *Increasing Threat of Deepfake Identities*, (Sept. 14, 2021).

⁶Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number) and something you have (cryptographic identification device or token), or something that you are (biometric). The combination of identification and authentication provides the basis for establishing accountability and for controlling access to the system. For more information, see GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C., Sept. 29, 2015).

⁷In this report, we refer to measures as counts of detected activities, and to estimates as projections or inferences based on measures, assumptions, or analytical techniques. Estimates are often used when direct measures are unavailable, incomplete, or unreliable.

⁸In addition to estimates from FBI and FTC, the Financial Crimes Enforcement Network (FinCEN) issued a Financial Trend Analysis that reviewed Suspicious Activity Reports from 2021 for identity-related suspicious activity in early 2024. Part of this analysis highlighted data where reports identified impersonation as a concern. FinCEN suggests these reports could indicate potential impersonation scams. For more information see U.S. Treasury Financial Crimes Enforcement Network, *Financial Trend Analysis: Identity-Related Suspicious Activity: 2021 Threats and Trends*, (Jan. 2024).

⁹The FTC's Consumer Sentinel Network collects reports from consumers about fraud, identity theft, and other consumer protection topics in an online database available to law enforcement. Federal Trade Commission, *Consumer Sentinel Network Data Book 2023*, (Feb. 2024). Imposter scams, as reported by the FTC in its Data Book, may include instances of fraud not included in our definition of fraudulently induced payments.

¹⁰Investment-related fraud, as reported by the FTC in its Data Book, may include instances of fraud not included in of our definition of fraudulently induced payments.

¹¹Federal Bureau of Investigation, *Internet Crime Report 2023*, (Mar. 6, 2024).

¹²Federal Bureau of Investigation, *Internet Crime Report 2022*, (Mar. 14, 2023) and *Internet Crime Report 2021*, (Mar. 22, 2022). The scam types and associated losses and complaints reported by the FBI may include instances of fraud outside of our definition of fraudulently induced payments. For example, while these scams often result in a victim making a fraudulently induced payment, the victim may instead provide personal information to the scammer, resulting in the scammer making an unauthorized transaction.

¹³Federal Trade Commission, *Protecting Older Consumers 2022-2023: A Report of the Federal Trade Commission*, (Oct. 18, 2023).

¹⁴Federal Trade Commission, *Protecting Older Consumers 2022-2023: A Report of the Federal Trade Commission*, (Oct. 18, 2023).

¹⁵Global Anti-Scam Alliance, *The State of Scams in the United States of America*, (2023). The international alliance is composed of entities from government (including law enforcement), private, and nonprofit consumer protection sectors.

¹⁶The federal government may enforce laws through civil or criminal action. According to DOJ officials, such action may be resolved through a trial, a permanent injunction, a civil settlement, a guilty plea, or other disruption. Details of fraud cases and schemes presented in court documents may not be complete. DOJ tracks cases by convictions of specific statutory violations rather than by “fraudulently induced payments”. Accordingly, cases involving fraudulently induced payments are not specifically tracked by DOJ but are instead tracked by a variety of potential statutory charges or resolutions, according to these officials.

¹⁷Federal Trade Commission Press Release, *FTC Sues to Stop VoIP Services Provider That Assisted and Facilitated Telemarketers in Sending Hundreds of Millions of Illegal Robocalls to Consumers Nationwide* (May 12, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-sues-stop-voip-service-provider-assisted-facilitated-telemarketers-sending-hundreds-millions>.

¹⁸The FTC enforces Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair and deceptive acts or practices in or affecting commerce. The FTC also enforces several regulations that prohibit or relate to fraud, including in some circumstances those that may involve fraudulently induced payments, such as Regulation E, 12 C.F.R. part 1005, the Telemarketing Sales Rule, 16 C.F.R. part 310, and the Business Opportunity Rule, 16 C.F.R. part 437. See, for example, Federal Trade Commission Press Release, *MoneyGram Agrees to Pay \$125 Million to Settle Allegations that the Company Violated the FTC’s 2009 Order and Breached a 2012 DOJ Deferred Prosecution Agreement* (Nov. 8, 2018), available at <https://www.ftc.gov/news-events/news/press-releases/2018/11/moneygram-agrees-pay-125-million-settle-allegations-company-violated-ftcs-2009-order-breached-2012>; Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits \$586 Million in Settlement with FTC and Justice Department (Jan. 19, 2017), available at <https://www.ftc.gov/news-events/news/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles-consumer-fraud-charges-forfeits-586>; and FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions (June 28, 2022), available at <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-sues-walmart-facilitating-money-transfer-fraud-fleeced-customers-out-hundreds-millions>.

¹⁹ Consumer Financial Protection Bureau Press Release, *Consumer Financial Protection Bureau Takes Action Against Payment Processor and Its Former CEO for Supporting Internet-Based Technical-Support Scams* (Mar. 3, 2021), available at <https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-takes-action-against-payment-processor-and-its-former-ceo-for-supporting-internet-based-technical-support-scams/>.

²⁰There are several types of payments, both electronic and nonelectronic, that can occur because of fraudulent inducement (e.g., electronic transfer via a bank account or P2P payment app, wire transfer, money transfer, or payment via check). Additionally, these types of fraud can be perpetrated on businesses and consumers alike. Our review and analysis focus on fraudulently induced payments, as defined herein for purposes of this report, that are made electronically and perpetrated on individual consumers. Regulation E applies to electronic fund transfers, which means any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account. 12 C.F.R. § 1005.3(a), (b). There are also exclusions from the definition of electronic fund transfer. 12 C.F.R. § 1005.3(c). When we use the term “payment” in this section, we mean electronic fund transfer as defined in Regulation E, unless otherwise stated.

²¹See Regulation Z, 12 C.F.R. § 1026.12(g), § 1026.13(i), and Regulation E, 12 C.F.R. § 1005.12(a) regarding whether Regulation Z or Regulation E would apply in the case where a credit card is involved in a fraudulently induced electronic payment. CFPB officials noted that the impact of Regulation Z on P2P transactions may be limited because it is less common for these transactions to be routed using a credit card. Additionally, other laws or regulations could be at issue when resolving disputes between consumers and financial institutions; for example, the Uniform Commercial Code, the Expedited Funds Availability Act, codified as amended at 12 U.S.C. chapter 41, and its implementing Regulation CC, 12 C.F.R. part 229, or contractual or warranty claims made under state law.

²²Regulation E, 12 C.F.R. § 1005.2(i), defines a “financial institution” as a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services, other than a person excluded from coverage of this part by section 1029 of the Consumer Financial Protection Act of 2010, title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, 124 Stat. 1376. An account is further defined as a checking, savings, or other consumer asset account, with some exceptions, that is held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes. 12 C.F.R. § 1005.2(b)(1). Consistent with the CFPB’s Electronic Fund Transfer FAQs, Regulation E applies to any P2P or mobile payment transactions that meet the definition of an electronic fund transfer. CFPB has described application of Regulation E to P2P payment

providers via its Electronic Fund Transfer FAQs, last updated on December 13, 2021 (available at <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>).

²³There may be circumstances when a consumer is not responsible (in whole or in part) for an authorized payment because there is an error with the payment (e.g., the payment was processed for an incorrect amount or was misdirected to an unintended recipient). See 12 C.F.R. § 1005.11(a) (defining an “error” for purposes of Regulation E).

²⁴Tiers and conditions of liability are set forth at 12 C.F.R. § 1005.6. Financial institutions may impose less liability on the consumer by contractual agreement. For example, a financial institution can include a provision in its Terms and Conditions of Account that a consumer will have \$0 liability if notice is given to the financial institution within a prescribed period. See 12 C.F.R. § 1005.6(b)(6). Financial institutions can also impose less or no liability as a courtesy to the consumer.

²⁵12 C.F.R. § 1005.2(m) (defining unauthorized electronic fund transfer). The term “unauthorized electronic fund transfer” does not include a payment initiated: (1) by a person who was furnished the access device to the consumer’s account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized; (2) with fraudulent intent by the consumer or any person acting in concert with the consumer; and (3) by the financial institution or its employee. See also the official interpretation of 12 C.F.R. § 1005.2(m) (among other things, explaining that, in contrast, if an access device (e.g., a debit card) was obtained from the consumer through fraud or robbery and a transfer was then initiated by the person who committed the fraud or robbery, this *would be* an unauthorized transaction. Comment 1005.2(m)-3).

²⁶Whether a payment is considered authorized or unauthorized depends on the facts and circumstances at issue. Additionally, as noted above, there may be circumstances when a consumer is not responsible (in whole or in part) for an authorized payment because there is an error with the payment (e.g., the payment was processed for an incorrect amount or was misdirected to an unintended recipient). See 12 C.F.R. § 1005.11(a) (defining an “error” for purposes of Regulation E). According to CFPB, it has taken supervisory action against institutions that failed to determine that certain authorized transactions were errors – incorrect electronic fund transfers – for which the institution may not hold the consumer liable. See the [Bureau’s Fall 2021 Supervisory Highlights](https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-25_2021-12.pdf) at page 6 (available at https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-25_2021-12.pdf). Furthermore, there may be certain circumstances under which financial institutions may impose less or no liability in the case of a fraudulently induced payment (e.g., based on contract, policies, or as a courtesy to the consumer).

²⁷See 12 C.F.R. § 1005.11 for the procedures and timeframes required of financial institutions to resolve errors.

²⁸An error is defined to include an unauthorized payment. 12 C.F.R. § 1005.11(a)(1). In contrast, an authorized payment is not considered an error. However, as noted above, there are other types of errors that may be asserted on an authorized payment (e.g., the payment was processed for an incorrect amount or was misdirected to an unintended recipient). See 12 C.F.R. § 1005.11(a)(1). As relevant here it may be the case that the consumer reports fraud on the account without providing sufficient details for the financial institution to determine whether an error has or has not occurred (that is, whether the payment was authorized or unauthorized). In this case, the financial institution would engage in an investigation consistent with 12 C.F.R. § 1005.11(c) to determine whether an error occurred and, accordingly, whether the financial institution or consumer is responsible for the payment. See also 12 C.F.R. § 1005.11(d).

²⁹Under the Bank Secrecy Act (BSA), as amended, and its implementing regulations, financial institutions are required to maintain an anti-money-laundering and countering the financing of terrorism program (known as a BSA/AML program) that is tailored to the size and risks of the organization. According to financial institutions, these BSA/AML programs include a variety of measures taken to address the risk of fraud. Additionally, as part of their BSA obligations, financial institutions are required to monitor consumer transactions to identify suspicious activity that may indicate money laundering or other criminal activity, and file suspicious activity reports in certain circumstances.

³⁰See [Zelle Pay It Safe \(voxcreative.com\)](https://www.voxcreative.com/).

³¹We have ongoing work examining federal agency efforts to address fraudulently induced payments, including those related to consumer education.

³²As discussed in GAO, *Banking Services: Regulators Have Taken Actions to Increase Access, but Measurement of Actions’ Effectiveness Could Be Improved*, GAO-22-104468 (Washington, D.C.: Feb. 14, 2022), a study conducted by Federal Reserve economists showed that certain banks raised fees after a federal regulation that increased costs to financial institutions.

³³Federal Trade Commission, *A Review of Scam Prevention Messaging Research: Takeaways and Recommendations*. (Apr. 2024).

³⁴FINRA Investor Education Foundation, the BBB Institute for Marketplace Trust, and Stanford Center on Longevity; *Exposed to Scams: What Separates Victims from Nonvictims*. (Sept. 2019).

³⁵Scammers will send victims SMS texts imitating trusted brands to trick victims into giving over personal information or money. These scam texts are often difficult to distinguish from legitimate texts from businesses. The SMS Sender ID Registry allows brands to register their sender ID and blocks other messages from other users trying to use the same sender ID.

³⁶The Federal Communications Commission has implemented strategies to reduce robocalls to American consumers including fining telemarketers for illegal caller ID spoofing and robocalling, and caller ID authentication between networks.

³⁷ Keith B. Anderson, "To Whom Do Victims of Mass-Market Consumer Fraud Complain?" *SSRN* (May 24, 2021), <http://dx.doi.org/10.2139/ssrn.3852323>.

³⁸The Regional Enforcement Allied Computer Team (REACT) Task Force is a partnership of local, state, and federal agencies. REACT's mission is to combat advanced cybercrime, including scams that result in fraudulently induced payments. REACT conducts multijurisdictional investigations, combining resources and expertise, to arrest and prosecute scammers and other sophisticated cyber criminals.

³⁹Federal Bureau of Investigation, *Internet Crime Report 2023*; *Internet Crime Report 2022*; *Internet Crime Report 2021*; and Federal Trade Commission, *Consumer Sentinel Network Data Book 2023*.

⁴⁰Public Access to Court Electronic Records is a service of the federal judiciary that enables the public to search online for case information from U.S. district, bankruptcy, and appellate courts. Federal court records available through this system include case information (such as names of parties, proceedings, and documents filed), as well as information on case status.