SECOND ISSUE 2025

SPECIAL FRAUD ISSUE

CONSUMER COMPLIANCE OUTLOOK®

A FEDERAL RESERVE SYSTEM PUBLICATION FOCUSING ON CONSUMER COMPLIANCE TOPICS

INSIDE

A NOTE FROM THE EDITORS

Fraud is a top-of-mind concern for consumers, financial institutions, and businesses as schemes to defraud them have proliferated in recent years. The 2024 annual report[1] from the Federal Trade Commission's (FTC) Consumer Sentinel Network, which captures data from reports consumers filed with the FTC, highlights the cost of consumer fraud:

- Losses from all fraud/scam categories totaled $12.5 billion dollars — a 25 percent increase from 2023 losses of $10 billion.
- Losses from investment scams totaled $5.7 billion — a 24 percent increase from 2023 losses of $4.6 billion.
- Losses from imposter scams totaled $2.95 billion — a 10 percent increase from 2023 losses of $2.67 billion.
- Losses based on bank transfer/payment totaled $2.09 billion — a 13 percent increase from 2023 losses of $1.8 billion.
- Losses from social media scams totaled $1.9 billion — the single highest category of losses ranked by method of contacting the consumer.
- Losses for military consumers totaled $584 million — a 22 percent increase from 2023 losses of $477 million.

The actual total losses are much greater because the FTC data capture only reported incidents. But the trend is clear: Financial fraud against consumers is significantly increasing each year. Other data sources confirm this finding. Data from the Financial Crimes Enforcement Network (FinCEN) show a 110 percent increase in total Suspicious Activity Reports from financial institutions for fraud between 2020 (552,920 reports) and 2024 (1,165,642 reports) in the categories of automated clearinghouse, check, credit/debit card, mail, and wire.[2]

While technology has facilitated many common fraudulent schemes (such as social media scams, text messaging scams, and phishing emails), it is also providing ways to combat fraud. Through advances in technology, private companies are developing sophisticated tools to identify and block fraudulent transactions.

This special issue discusses several fraud topics, including the banking agencies' recent request for information on payment and check fraud. We hope you find this issue helpful.

---

[1] *Consumer Sentinel Network Data Book 2024*.

[2] Data were obtained from FinCEN's Suspicious Activity Report Statistics web page. *Consumer Compliance Outlook* created a custom report.

Responding to Counterfeit Instrument Scams and Mail-Related Check Fraud

By Kenneth J. Benton, Principal Consumer Regulations Specialist, Federal Reserve Bank of Philadelphia

Editor's Note: This article was originally published in 2008, with an updated version published in 2018. We have updated it further to reflect changes that have occurred since then.

Check fraud has become a growing concern for financial institutions, businesses, and consumers. According to the 2025 payment fraud survey of the Association of Financial Professionals (AFP), "checks continue to be the payment method most often subjected to payments fraud, with 63 percent of respondents experiencing attempted or actual fraud via checks in 2024."[1] Statistics for mail-related check fraud and counterfeit instrument scams confirm the gravity of this issue. The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) reported that during a six-month period in 2023, it received 15,417 Bank Secrecy Act reports involving mail-related check fraud with more than $688 million in transactions,[2] while the Federal Trade Commission received 13,616 consumer complaints of fake check scams in 2024.[3]

While the number of checks the Federal Reserve processes has generally been decreasing over the years,[4] the total check volume is still substantial: In 2024, the Federal Reserve processed nearly 3 billion commercial checks and 36 million government checks.[5] According to a 2024 AFP survey, 75 percent of surveyed organizations reported using checks, and 70 percent had no immediate plans to stop using them.[6] Thus, it is important for all stakeholders to understand check fraud risks and ways to respond. This article discusses two types of common check fraud — counterfeit instrument scams and mail-related check fraud — and ways financial institutions, businesses, and consumers can help mitigate these risks.

COUNTERFEIT INSTRUMENT SCAMS

Background

Congress passed the Expedited Funds Availability Act (EFAA) in 1987 to "end excessive holds on customer deposits by depository institutions"[7] by establishing the maximum permissible hold periods for checks and other types of deposits. For certain "safe" instruments considered low risk for being dishonored, the law requires funds be made available the next business day. These include cashier's and certified checks, Treasury checks, U.S. postal money orders, checks drawn on a Federal Reserve Bank or Federal Home Loan Bank, and checks issued by a state or local government.[8] For most other check deposits, Regulation CC, the EFAA's implementing regulation, requires funds be made available not later than the second business day following the banking day on which funds are deposited.[9]

When the EFAA was enacted, desktop publishing was in its infancy, and tools to create high-quality counterfeit checks were expensive and not readily available. But desktop publishing has evolved considerably since 1987. Inexpensive, off-the-shelf software and hardware can now create counterfeit instruments, such

as cashier's checks or money orders, that look identical to genuine ones.[10] Criminals understand that many people mistakenly believe that these checks or money orders cannot be rejected once the funds have been received, so they exploit the delay between the time deposits must be made available under the EFAA and the time it takes to discover an instrument is counterfeit. During this window of opportunity, fraudsters can deceive victims into wiring funds from the check or money order that was deposited.

Nature of the Schemes

Criminals create a counterfeit financial instrument believed to be a form of guaranteed payment, such as a cashier's check or postal money order, and trick consumers or businesses into depositing it and wiring back a portion of the deposit based on a contrived explanation. The check will appear to have cleared because the EFAA and Regulation CC limit the hold periods for deposited checks and other instruments, even though they may not have been paid yet by the payor bank. Eventually, the payor bank to which the check will be presented for payment will flag it as a counterfeit and return it to the depositary bank.[11] When the check is returned unpaid, the depositary bank will typically seek to reverse the deposit that was originally in the customer's account. The customer may have assumed the check was legitimate because the funds were made available and blames the depositary bank for this misunderstanding; however, the depositary bank has simply complied with federal law by crediting the account within the Regulation CC time frames.[12]

Common counterfeit instrument scams many institutions encounter include:[13]

- **Job/task scams:** A consumer is told he can earn a commission by completing different online tasks such as rating product images. Before receiving the commission, the consumer is told he must "charge up" his online account by making a deposit, after which he will receive the amount of the deposit back plus his commission.[14]
- **Car wrap:** A consumer is told she can earn money by agreeing to have her car wrapped to advertise a product such as an energy drink. The scammer sends the consumer a counterfeit check to cover the cost of having the car wrapped and instructions to deposit the check and then wire the money to the company performing the car wrap.[15]
- **Mystery shopper:** A consumer receives a letter stating he has been chosen to act as a mystery shopper and receives a cashier's check to deposit. The consumer is told to use a portion of the funds to purchase merchandise at the designated stores, transfer a portion of the funds to a third party using a designated wire service company, and keep the remainder.
- **Online transactions:** A consumer sells an item through an online marketplace, and someone offers to buy it using a cashier's check (or similar instrument) for an amount greater than the asking price. The buyer offers a contrived explanation for the overpayment and asks the seller to deposit the check, keep the amount of the selling price plus an extra amount, and wire the balance back to the buyer.

While these schemes initially focused on consumers, businesses also have been targeted in recent years. In one common scheme, fraudsters contact law firms pretending to be new clients seeking representation to collect debts. The law firm contacts the alleged debtor, who agrees to pay the debt and sends the law firm a counterfeit check. The law firm deposits the check and sends the client the payment less attorney's fees and later learns the check was counterfeit. In 2024, the FBI issued an alert about this issue.[16]

RISK MITIGANTS

Exception Holds

Regulation CC contains several exceptions to its expedited funds availability requirements for check deposits.[17] Of relevance here, a depository bank may extend the hold period for check deposits when it has reasonable cause to believe the check is uncollectible from the paying bank.[18] Banks may leverage this exception when they have reason to believe a depositor is attempting to cash a counterfeit or altered check, provided the reason satisfies the regulation's standard for invoking this exception: "Reasonable cause to believe a check is uncollectible requires the existence of facts that would cause a well-grounded belief in the mind of a reasonable person. Such belief shall not be based on the fact that the check is of a particular class or is deposited by a particular class of persons."[19]

If a bank has reasonable cause to believe a check is uncollectible from the paying bank, written notice must be provided to the depositor that includes the time period within which the funds will be available for withdrawal and the reason the exception was invoked.[20] An exception hold extends the hold period by a "reasonable period of time" beyond the period that would otherwise be required for the type of instrument.[21] The regulation includes safe harbors for "a reasonable period of time." If a hold exceeds the applicable safe harbor, the burden is on the bank to justify it.[22]

Educating Customers

Counterfeit instrument scams present challenges for financial

"Financial institutions can play an important role by educating their customers about this issue. This is admittedly a delicate task because banks want to educate their customers without alarming them."

institutions because many consumers and businesses believe that certain instruments, such as a cashier's check or a money order, cannot be dishonored. They therefore assume that next-day funds availability means their financial institution was paid on the deposited instrument.

Financial institutions can play an important role by educating their customers about this issue. This is admittedly a delicate task because banks want to educate their customers without alarming them.

For deposits made in person, banks could consider training tellers to discuss the risks of accepting cashier's checks or similar instruments from parties with whom they have few or no prior dealings.

Banks can also consider posting advisories on their websites, in their mobile applications, and in branches about counterfeit check scams to alert customers to the red flags of suspicious transactions.[23]

Educating Employees

A well-trained staff can also help detect counterfeit or altered checks. Physical signs of counterfeiting that employees can be vigilant for include evidence of alteration or erasing, spelling errors, mistakes, suspicious check amounts, a lack of or incorrect financial institution information, and a routing number that does not match the routing number of the instrument's issuer.

A bank could also mitigate risks by including its wire department in any educational campaign because many schemes require the consumer or business to wire funds to a fraudster. Banks may consider training wire department staff to recognize suspicious transactions in which bank customers are at high risk for counterfeit check scams. Typically, these scams involve some or all of the following characteristics:

- A wire transfer request is made shortly after the deposit of an instrument subject to next-day availability that a customer received from a third party with whom the customer has no prior dealings.
- The instrument deposited is generally believed by consumers to be incapable of bouncing such as a cashier's check or certified check.
- A customer who rarely makes wire transfers makes a transfer.
- A recipient is outside the United States.

When a wire transfer involves some or all of these characteristics, staff may consider informing the customer about counterfeit check scams and the risk of wiring funds to someone with whom the customer has no prior relationship.

Verifying Suspected Counterfeit Instruments

Treasury Checks

Executive Order 14247 generally phases out Treasury checks, but they will still be issued on an exception basis. The Department of the Treasury maintains a website to verify whether a Treasury check is valid.[24]

Postal Money Orders

The U.S. Postal Service provides a phone number to verify postal money orders: 866-459-7822. The Postal Service also has a web page discussing security features.[25]

Other Money Orders

Some private money order providers offer verification services.

MAIL-RELATED CHECK FRAUD

Mail-related check fraud occurs when criminals steal checks from mail receptacles to facilitate check fraud. For example, criminals might break into a U.S. Postal Service blue collection box after the last collection for the day or steal mail left overnight in someone's mailbox.

In a 2024 report,[26] FinCEN identified principal ways criminals use stolen checks:

- Altering and depositing them
- Using the account number and bank routing number to create counterfeit checks
- Fraudulently signing and depositing them
- Selling them on the dark web

Between October 2021 and October 2022, the Postal Service reported 38,500 mail theft incidents involving mail receptacles.[27] In the first half of fiscal 2023, more than 25,000 such incidents were reported. Furthermore, the U.S. Postal Inspection Service (USPIS) reported 299,020 mail theft complaints between March 2020 and February 2021, an increase of 161 percent over the prior year, while the number of Suspicious Activity Reports for check fraud nearly doubled between 2021 and 2023.[28]

RISK MITIGANTS

Positive Pay

To combat check fraud, banks have begun offering positive pay as a service to commercial customers. Under positive pay, an automated system compares checks presented to the bank with a list of information on checks sent by a business.[29] Checks deemed suspicious are sent back to the business for verification, and they are cleared only when the business approves them. Since businesses update these lists on a regular basis, positive pay allows them to bank more securely when issuing paper checks.

Other Mitigants

- Making payments electronically when possible and encouraging payors to send electronic payments
- Using checks with security features, writing checks in nonerasable ink, and filling out checks as fully as possible to make it more difficult for criminals to alter the information, known as check washing
- Taking checks directly to the post office instead of putting them in a mailbox

EXECUTIVE ORDER ON PAYMENTS TO AND FROM THE FEDERAL GOVERNMENT

On March 25, 2025, President Trump signed Executive Order 14247, "Modernizing Payments to and from America's Bank Account," which will implement significant changes regarding Treasury checks. The order directs the Secretary of the Treasury to cease issuing paper checks, with limited exceptions, for all federal disbursements, including intragovernmental payments, benefits payments, vendor payments, and tax refunds beginning on September 30, 2025, to the extent provided by law.[30] In addition, the order provides that as soon as practicable, and to the extent permitted by law, all payments made to the federal government, with limited exceptions, shall be processed electronically.

The order notes that maintaining the existing infrastructure for issuing Treasury checks and digitizing paper records cost over $657 million for fiscal 2024.[31] According to the order, Treasury checks are more likely to be stolen, altered, or returned undeliverable than electronic funds transfers.

The order includes certain exceptions where electronic payment and collection methods are not feasible. These exceptions, listed in §4(a) of the order, include individuals lacking access to banking services and electronic payments, emergency payments where electronic transfers would cause undue hardship, and security-related activities where issuing electronic payments would pose a hindrance.

FEDERAL BANKING AGENCIES' REQUEST FOR INFORMATION ON POTENTIAL ACTIONS TO ADDRESS PAYMENTS FRAUD

In June 2025, the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation published a request for information (RFI) on payments fraud in the *Federal Register* with a comment period ending September 18, 2025.[32] The RFI is summarized on page 11 of this issue.

INTERAGENCY STATEMENT ON ELDER FINANCIAL EXPLOITATION

Federal and state financial regulators issued a joint statement in December 2024 that provides examples of risk management and other practices for elder financial exploitation that may also be effective in mitigating check fraud risk.

CONCLUSION

Mail-related check fraud and counterfeit instrument scams present challenges for financial institutions, businesses, and consumers. This article discussed these risks and ways to help mitigate them. The federal banking agencies are soliciting information from the public to help them explore ways in which they can use their authorities to mitigate payment and check fraud. Specific issues or questions should be discussed with your primary regulator. ■

Endnotes*

1 See "Survey: 79% of Organizations Were Victims of Attempted or Actual Payments Fraud Activity in 2024" AFP press release, April 15, 2025.

2 "Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023," FinCEN (September 2024). See also Ann Carrns, "Check Fraud Is on the Rise. Here's What You Can Do to Prevent It," *New York Times* (March 10, 2023); Ron Lieber, "Stolen Checks Are for Sale Online. We Called Some of the Victims," *New York Times* (July 3, 2024).

3 *Consumer Sentinel Data Book 2024* at p. 87. See also Ann Carrns, "Got an Unexpected Check in the Mail? It May Be Fake," *New York Times* (February 21, 2020).

4 The Federal Reserve publishes annual data on check volumes for commercial and government checks and postal money orders. The Clearing House also processes checks through its network, so these data understate the total number of checks processed.

5 *Id*.

6 "2024 AFP Payments Fraud and Control Survey Report Key Highlights," Association for Financial Professionals (April 2024).

7 S. REP. No. 100-19, at p. 1 (1987).

8 12 C.F.R. §229.10(c).

9 12 C.F.R. §229.12(b).

10 George Brandon and Matthew J. Ohre, "The Nigerian Check Scam: An Oldie Revisited," 126 *Banking Law Journal* at pp. 223–224 (March 2009).

11 "Beware of Fake Checks," Federal Deposit Insurance Corporation (August 2019).

12 12 C.F.R. Part 229, subpart B.

13 The FTC has provided data on some of the top check scams: "Don't Bank on a 'Cleared' Check" (February 10, 2020). See also "Don't Cash That Check: BBB Study Shows How Fake Check Scams Bait Consumers," Better Business Bureau (September 2018).

14 "Paying to Get Paid: Gamified Job Scams Drive Record Losses," FTC Data Spotlight (December 12, 2024).

15 "How to Avoid Getting Wrapped Up in a Car Wrap Scam," FTC Consumer Alert (April 1, 2024).

16 "Counterfeit Check Scam Targets Law Firms Via Debt Collection Scheme," FBI Alert Number: I-100824-PSA (October 8, 2024).

17 12 C.F.R. §229.13.

18 12 C.F.R. §229.13(e).

19 12 C.F.R. §229.13(e)(1).

20 12 C.F.R. §229.13(g).

21 12 C.F.R. §229.13(h)(1); Comments 13(h)-1, -2, -3, -4.

22 12 C.F.R. §229.13(h)(4); Comment 13(h)-1. Records of exception holds must be retained. 12 C.F.R. §229.13(g)(5).

23 The Georgia Department of Banking and Finance has a web page discussing red flags for counterfeit checks.

24 See the Treasury Check Verification System.

25 See "Verifying U.S. Postal Service Money Orders" at www.usps.com. The *New York Times* published an article in 2005 detailing the increase in counterfeit postal money orders. See Tom Zeller Jr., "Authorities Note Surge in Online Fraud Involving Money Orders," *New York Times* (April 26, 2005).

26 "Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023," FinCEN (September 2024).

27 *Id*.

28 "Mail Theft-Related Check Fraud Is on the Rise," FBI and USPIS public service announcement (January 27, 2025).

29 See "Positive Pay 101: A Guide to Preventing Payment Fraud" at www.bill.com.

30 90 FR 14001 (March 25, 2025).

31 *Id.*

32 90 FR 26293 (June 20, 2025).

* Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

Confidence Scams: What They Are and How to Protect Your Customers

*By Steve Jones, Risk Specialist, Supervision and Risk Management, Federal Reserve Bank of Kansas City, and Alinda Murphy, Former Lead Examiner, Federal Reserve Bank of Kansas City**

Editor's Note: This article was originally published in the Second Release 2025 of Community Banking Connections.

Financial risks related to confidence scams are growing, and scammers are taking advantage of newer technologies that increase risks. Confidence scams involve bad actors who engage in fraudulent activities designed to take advantage of a person's trust. Technology makes it easier for bad actors to impersonate trusted sources, and digital currencies and prepaid cards allow scammers to mask the movement of stolen funds, making it more difficult for victims' funds to be retrieved. This article discusses ways to increase community bankers' awareness of the various types of confidence scams and provides resources for bank staff and customers dealing with the consequences of such scams.

IMPACT OF CONFIDENCE SCAMS

Multiple databases maintain information on confidence scams, which are defined in the accompanying table "Common Types of Confidence Scams." Several federal government agencies maintain databases on consumer fraud, such as the Federal Trade Commission (FTC) Consumer Sentinel Network Data Book (Sentinel Data Book) and the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3). The Consumer Financial Protection Bureau (CFPB) also collects information on incidents of fraud that shows a greater and increasing number of reported fraud cases, including confidence scams.

According to the Sentinel Data Book, the FTC received over 2.5 million reports of consumer fraud in 2023. Imposter scams, which include confidence scams, were the second most prevalent category behind identity theft and had more than 853,000 reported incidents. As a result of imposter scams, consumers lost about $2.7 billion that year.[1] Bank transfers or payments of $1.8 billion were the largest dollar volumes of reported fraud payment methods, followed by cryptocurrency transactions ($1.4 billion).

The IC3 reported that the FBI received approximately 880,000 fraud-related complaints in 2023, with total losses exceeding $12.5 billion.[2] Compared with 2022, those figures represent a 10 percent increase in IC3 complaints and a 22 percent increase in losses. According to the IC3, investment scams resulted in the costliest losses in 2023 ($4.57 billion, representing a 38 percent increase from 2022).

The CFPB received nearly 22,000 complaints related to money services in 2023 and sent approximately 13,700 of them to companies for review and response. Of those complaints, the most common issue was frauds/scams (5,200; 39 percent),[3] and the monthly average volume of complaints related to frauds/scams had increased 11 percent over the prior two years. Complaints resulted from a variety of scams, including scammers posing as representatives of investment firms, financial institutions, or companies offering debt relief. As prevalent as these fraud cases are, they likely underestimate the number of actual scams because these figures only represent incidents in which a victim reported the scam.

HOW TO IDENTIFY A CONFIDENCE SCAM

Confidence scams include a variety of fraudulent activities that generally fall under the relationships and trust scam category within the Federal Reserve's ScamClassifier model.[4] With these types of fraud, scammers attempt to influence or deceive individuals into divulging personal or financial information through social engineering, whereby scammers build relationships with individuals to gain control over their bank funds or other financial assets. To help legitimize their requests, criminals are increasingly leveraging deepfake media

as a way of impersonating individuals or organizations that victims may trust, as highlighted in a 2024 FinCEN Alert.[5]

HOW CONFIDENCE SCAMS WORK

The time it takes to perpetrate a scam varies by the type of scam involved and how quickly a scammer can gain the confidence of a targeted individual. Some scams are executed in a matter of minutes, while others, such as romance and investment scams, may continue over several days or months. Confidence scams often follow a three-stage strategy.

Stage One: Trust

During the first stage, the scammer contacts an individual through a variety of communication platforms. Once the communication channel is established, the scammer begins to gain the individual's trust. Communication may be initiated on the pretense of a mistaken contact, such as a wrong telephone number or misdirected text, or it may be a seemingly random contact with a stranger in a public place. Some initial contacts are based on the scammer's awareness of a financial or technological problem that the individual might have, such as a computer virus. Scammers may use information from public data, social media, or dark web sources to tailor the initial contact to a personal event or situation, such as the recent death of a family member, a medical condition, or a criminal record. Some scammers use fake call centers and websites to boost the credibility of their claims. Confidence scams rely on an individual's willingness to continue the communication, in hopes of deepening the individual's trust.

Stage Two: Control and Liquidation

By increasing an individual's trust, the scammer tries to isolate the individual from friends, family, and other trusted sources to prevent the individual from getting conflicting information or being alerted to the fact that they are being scammed. This isolation step is generally followed by the scammer insisting on some urgent action, usually claiming the action is necessary to protect the individual's financial interests or to continue their relationship. The scammer may tell the individual the steps to take to resolve the fictitious issue or problem, while the scammer continues to gather additional personal information regarding the individual's assets and resources. The scammer may ask for more personal information, more money, or more control of the individual's assets. In elder fraud cases, this may involve the individual signing a power of attorney or other legal documentation that gives the scammer control of the individual's real property and other assets (e.g., bank accounts or investments). Some investment scam victims are tricked into making payments to scammers and are then pressured to continue making payments to try to recover their losses. By the end of this stage — and unless the victim has caught on to the scam and sought help — the victim may have given the scammer all or a substantial part of their funds or assets during the scam.

"Scammers may use information from public data, social media, or dark web sources to tailor the initial contact to a personal event or situation, such as the recent death of a family member, a medical condition, or a criminal record."

Stage Three: Desertion

After the scammer has succeeded in gaining control of the individual's funds/assets or realizes that no additional funds are forthcoming, the scam and the relationship end. In most cases, even if the victim has the scammer's contact information, that contact information no longer works. Fear, denial, or shame may prevent the victim from reporting the

Common Types of Confidence Scams

Charity lotteries and sweepstakes: A scammer contacts an individual with the news that the person has won money or property and must submit personal information or money to receive the winnings.

Cryptocurrency scams: Scammers use cryptocurrency as the form of payment and the exchange of funds.[a] This type of fraud can take many forms; for example, scammers may threaten to expose harmful or embarrassing information unless an individual pays a ransom. This type of scam is often referred to as "pig butchering,"[b] referring to the way in which a pig is fattened before slaughter, and it is associated with romance and investment scams.

Elder financial exploitation scams: A scammer contacts an older individual and pretends to be the victim's grandchild or other relative who needs financial assistance; the scammer convinces the victim to remit funds to the scammer to provide that assistance.

Government and financial institution impersonation scams: A scammer claims to be affiliated with a government agency or financial institution in order to obtain an individual's passwords or credentials to gain access to the individual's computer or bank account.

Investment scams: A scammer convinces an individual that they have privileged financial knowledge that will produce profitable investments, often with the promise of unusually high returns, and convinces the victim to remit funds or provide access to the individual's bank and investment accounts.

Online shopping scams: A scammer uses a fake website to make an individual believe that they are buying merchandise from a legitimate merchant in order to obtain the victim's debit and credit card payment information.

Romance scams: A scammer feigns admiration for a potential victim to gain access to the individual's personal information or to induce the individual to give funds to the scammer.

Tech support scams: A scammer uses fake caller ID numbers, pop-up messages, or email to contact an individual, telling the individual that the technology company has detected a hardware or software problem and that the individual needs to provide the scammer with passwords, access credentials, or other personal information to allow tech support to correct the problem.

---

[a] For more information on cryptocurrency scams, see Anthony DeVita, "Crypto Scams and Related Fraud," *Community Banking Connections*, Sixth Release 2024.

[b] Because *pig butchering* is increasingly common, there are several resources dedicated to informing consumers and businesses about the risks, such as the Federal Deposit Insurance Corporation Office of the Inspector General Pig Butchering Scams page.

fraud immediately, which can hinder a bank from helping the customer recover lost funds or assets and law enforcement from pursuing criminal charges against the scammer.

DEVELOPING AN ACTION PLAN

Community banks can consider the following steps to help prevent or remediate confidence scams against their customers.

- Ensure that effective board and senior management governance is in place for detecting, monitoring, and addressing fraud in a timely manner.[6]
- Ensure that bank systems are equipped to detect unusual or suspicious account activity and file Suspicious Activity Reports (SARs).[7]
- Train frontline staff to recognize and respond when customer interactions suggest that a customer may be reacting to potential fraud, including how to alert the customer to a potential scam, when to escalate the issue at the bank for further investigation, and when to follow up with a potential report to law enforcement.
- Ensure board, senior management, and frontline staff are aware of elder financial exploitation, any state and local reporting requirements, and available resources[8] because senior citizens are often the target of confidence scams.
- Educate bank customers and their caregivers on detecting confidence scams, verifying the legitimacy of contacts, and expeditiously reporting suspicious activity to the bank and law enforcement when fraud is suspected or has been committed.[9] Additionally, reporting suspected scams and fraud to the FTC database can help law enforcement identify trends, educate the public, and bring cases against scammers.

CONCLUSION

Banks are on the front line in encountering confidence scams, which often result in their customers suffering significant financial losses. Everyday bank staff interactions with customers, strong customer relationships, and effective oversight and implementation of fraud mitigation controls can help community banks identify fraud attempts early and help protect their customers from fraud. Specific issues or concerns should be discussed with your primary federal regulator. ■

Endnotes**

* Alinda Murphy, a former lead examiner, retired from the Federal Reserve Bank of Kansas City in January 2025.

1 See page 4 in the *2023 Consumer Sentinel Network Data Book*.

2 See the Internet Crime Complaint Center *2023 Internet Crime Report*.

3 See pages 47–48 in the *2023 Consumer Response Annual Report*.

4 See the Federal Reserve's ScamClassifier model.

5 See FIN-2024-Alert004, FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, November 13, 2024.

6 See Julie Williams, "Fraud Risk Management for the Ever-Present and Evolving Threat to the Payment Systems," *Community Banking Connections*, First Issue 2021.

7 See FIN-2023-Alert005, FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering," September 8, 2023.

8 See Jeanne Rentezelas and Larry Santucci, "Prepare Your Community Bank to Surf the Silver Tsunami," *Community Banking Connections*, First Issue 2020; Laura Gleason and Emily Rosenblum, "Combating Elder Financial Abuse," *Consumer Compliance Outlook*, First Issue 2017; FIN-2022-A002, FinCEN's Advisory on Elder Financial Exploitation, June 15, 2022; and Supervision and Regulation letter 24-8/Consumer Affairs letter 24-6, "Interagency Statement on Elder Financial Exploitation."

9 The CFPB site on fraud and scams contains educational resources that can help bank staff, customers, and caregivers.

** Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

Agencies Request Comments on Ways to Address Check and Payment Fraud

In response to a significant increase in check and payment fraud, the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Board), and the Office of the Comptroller of the Currency (OCC) (agencies) published a request for information in the *Federal Register* on June 20, 2025, to help the agencies explore ways they can exercise their various authorities to mitigate these risks.[1]

The agencies noted these statistics on the increase in payment and check fraud:

- Losses for noncard payment fraud increased 271 percent between 2020 and 2024, according to the Federal Trade Commission.[2]
- The number of Suspicious Activity Reports (SARs) filed related to check, ACH, and wire fraud increased 489 percent between 2014 and 2024, according to the Financial Crimes Enforcement Network.[3]
- Check fraud in the United States has risen 385 percent since the COVID-19 pandemic, according to the Department of the Treasury.[4]

Regarding check fraud, checks can be stolen, altered, or forged. While products and services are available to detect altered or forged checks when processed, they have varying degrees of effectiveness. Another risk is that checks display the payor's name, account number, routing number, address, and signature, which criminals can use to conduct other forms of payment fraud.

Payment fraud schemes can involve multiple institutions and payment methods, for which different federal and state agencies may have jurisdiction. As a result, no single agency or private-sector entity can address payment fraud on its own. But the agencies may be able to take action individually or working together to mitigate payment fraud. In addition, the Federal Reserve Banks may be able to further support the industry because of their role as payments system operator and payments improvement catalyst.

To inform their understanding of the issues and the actions that may be taken, the agencies requested comment on the following questions, by September 18, 2025:

Collaborating with Industry Stakeholders

1. What actions could increase collaboration among stakeholders to address payment fraud?
2. What types of collaboration, including standard setting, could be most effective in addressing payment fraud? What are some of the biggest obstacles to these types of collaboration?
3. Which organizations outside of the payments or banking industry might provide additional insights related to payment fraud and be effective collaborators in detecting, preventing, and mitigating payment fraud?
4. Could increased collaboration among federal and state agencies help detect, prevent, and mitigate payment fraud? If so, how?

Consumer, Business, and Industry Education

5. In general, what types of payment fraud education are most effective, and why? Would different audiences (for example, industry and consumers) benefit from different types of payment fraud education?
6. Would additional education informing consumers and businesses about safe payment practices be helpful to reduce payment fraud and promote access to safe, secure payment options?
7. Which approaches could make existing payment fraud education more effective? For example, would targeting outreach to particular audiences or conducting additional education in collaboration with other key stakeholders be effective?

Regulation and Supervision to Mitigate Payments Fraud

8. Are current online resources effective in providing education on payment fraud? If not, how could they be improved?
9. What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payment fraud and mitigate the harms from payment fraud to consumers, businesses, and supervised institutions?
10. The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payment fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payment fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?

11. How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payment fraud?

12. What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payment fraud? (Regulation CC's "reasonable cause to doubt collectability" exception is discussed separately below.)

    (a) For instance, how frequently are consumers and businesses affected by holds, delays, or account freezes, and how responsive are supervised institutions to inquiries from consumers and businesses regarding these issues?

    (b) Do current disclosure requirements effectively address consumer and business concerns when supervised institutions hold customer funds due to suspected payment fraud? For example, should changes be considered with respect to permissible customer communications under SAR confidentiality rules?

13. The Board, FDIC, and OCC have received complaints from supervised institutions regarding challenges in resolving disputes about liability for allegedly fraudulent checks. What is the experience of supervised institutions when trying to resolve these types of interbank disputes regarding allegedly fraudulent checks? Do these types of interbank disputes arise more frequently in connection with certain types of checks or parties? What actions could the Board, FDIC, and OCC consider, including potential amendments by the Board to Regulation CC, that could improve supervised institutions' ability to resolve interbank disputes over liability for allegedly fraudulent checks?

14. Regulation CC seeks to balance prompt funds availability with the risk of checks being returned unpaid for reasons that include fraud. What potential amendments to Regulation CC would support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payment fraud?

    (a) Have technological advancements in check processing reduced the time it takes for depository institutions to learn of nonpayment or fraud such that funds availability requirements for local checks and nonproprietary ATMs should be shortened?

    (b) What effects would shortening funds availability requirements have on payment fraud, consumers who rely on timely access to funds, and depository institutions?

    (c) Are there any changes the Board should consider to the expeditious return requirement to better balance providing expeditious notice to the receiving depository institution with ensuring adequate time for the paying depository institution to investigate potentially fraudulent checks?

15. Regulation CC provides six exceptions that allow depository institutions to extend deposit hold periods for certain types of deposits, including deposits for which the depository institution has reasonable cause to doubt the collectability of a check. Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds? Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception? What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?

Payments Fraud Data Collection and Information Sharing

16. Broadly, how could payment fraud data collection and information sharing be improved?

17. What barriers limit the collection and sharing of payment fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilateral or multilateral payment fraud data collection and information sharing? What changes would address these barriers?

18. What role should the Federal Reserve System, FDIC, or OCC take in supporting further standardization of payment fraud data? For instance, can the System better leverage or improve the FraudClassifier and ScamClassifier models?

19. What types of payment fraud data, if available, would have the largest impact on addressing payment fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?

20. Is there a need for centralized databases or repositories for the sharing of payment fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?

Federal Reserve Bank Tools and Services to Reduce Payments Fraud

21. How can the Reserve Banks enhance their existing risk management tools and services, operations, rules, or

procedures to better meet the needs of participating financial institutions in addressing payment fraud? For example, should the Reserve Banks consider requiring fraud reporting for payment rails (as they already do for the FedNow Service) or adopting any particular payment fraud standards?

22. Are there risk management tools or services that the Reserve Banks should consider offering or expanding, such as (a) developing a payment fraud contact directory for financial institutions, (b) offering tools that can provide notification of atypical payment activity, or (c) introducing confirmation of payee services to help mitigate fraudulent payment origination?

23. What types of payment fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payment fraud?

24. What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payment fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?

25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payment fraud?

26. Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?

Comments can be submitted electronically or by mail:

- https://www.regulations.gov/commenton/OCC-2025-0009-0001
- Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, 400 7th Street SW Suite 3E-218, Washington, DC 20219 ■

Endnotes*

1 90 FR 26293 (June 20, 2025).

2 90 FR at 26295, footnote 3.

3 90 FR at 26294, footnote 4.

4 90 FR at 26295, footnote 5.

* Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

Interested in reprinting a *Consumer Compliance Outlook* Article?

Please contact us at outlook@phil.frb.org. We generally grant requests to reprint articles free of charge provided you agree to certain conditions, including using our disclaimer, crediting *Consumer Compliance Outlook* and the author, and not altering the original text.

Cybersecurity Resources for Community Banks

This is a voluntary resource providing a non-exclusive compilation of publicly available content for convenience and informational purposes only. The Federal Reserve neither endorses the information, content, presentation, or accuracy nor makes any warranty, expressed or implied, regarding the organizations sponsoring linked websites and does not endorse the views they express or the products or services they offer. This resource does not have the force or effect of law and does not prescribe any specific practices or standards nor establish any safe harbors for compliance with laws or regulations. While it is intended for use by community banks, other banks may find it useful.

POTENTIAL SOURCES OF INFORMATION

Federal Financial Institutions Examination Council (FFIEC)

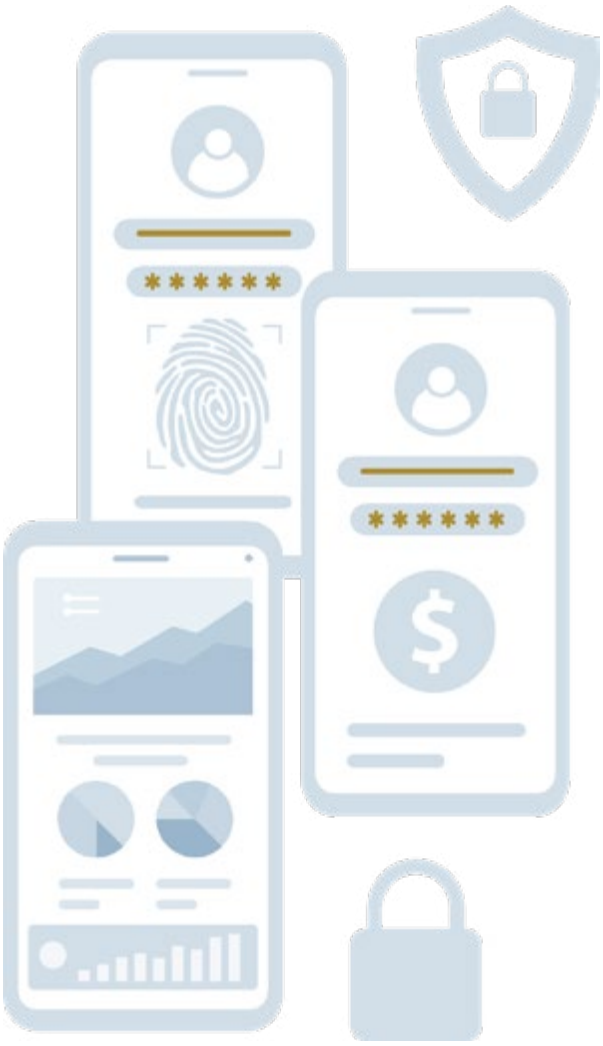
FFIEC members are taking a number of initiatives to raise the awareness of financial institutions and their third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

Content: The referenced resource guides and alerts pertain to cybersecurity awareness and various joint agency statements and can be found at www.ffiec.gov/.

Notifications: Sign up for alerts at www.ffiec.gov/.

FFIEC resources related to cybersecurity:

- Cybersecurity Awareness Webpage
- Cybersecurity Assessment Tool Sunset Statement
- FFIEC Cybersecurity Resource Guide for Financial Institutions
- FFIEC Statement on Security in a Cloud Computing Environment
- FFIEC IT Examination Handbook



United States Treasury's Project Fortress

U.S. Department of the Treasury established Project Fortress to improve the security and resilience of the financial services sector through forward-leaning public-private information sharing mechanisms. Project Fortress includes a mix of proactive defensive and offensive measures to help secure the financial sector. For more information, please see https://home.treasury.gov/.

Cybersecurity Infrastructure and Security Agency (CISA)

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. CISA is designed for collaboration and partnership with a mission to reduce risk to the nation's cyber and physical infrastructure.

Content: The programs and services offered by CISA seek to help organizations better manage risk and increase resilience using all available resources.

Notifications: Sign up for alerts at www.cisa.gov.

CISA cybersecurity resources and services available at www.cisa.gov:

- Cyber Hygiene Services
- Free Cybersecurity Services and Tools
- Tabletop Exercise Packages

CYBERSECURITY SELF-ASSESSMENT TOOLS

National Institute of Standards and Technology (NIST)

NIST is part of the U.S. Department of Commerce. NIST developed the Cybersecurity Framework, which provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks.

The Cybersecurity Framework is available at www.nist.gov/cyberframework.

Center for Internet Security (CIS)

CIS is an independent, nonprofit organization. CIS developed the Critical Security Controls (CIS Controls) as a prescriptive, prioritized, and simplified set of cybersecurity posture best practices.

CIS Controls are available at www.cisecurity.org/controls.

CISA

CISA developed the Cross-Sector Cybersecurity Performance Goals (CPGs), which are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. Financial Services Sector-Specific Goals are expected to be released soon.

CISA CPGs are available at www.cisa.gov/cross-sector-cybersecurity-performance-goals.

Cyber Risk Institute (CRI)

CRI is a not-for-profit coalition of financial institutions and trade associations. CRI developed the Cyber Profile as a global standard for cyber risk assessment. It consists of a list of assessment questions based on the intersection of global regulations and cyber standards, such as the International Organization for Standardization and NIST.

The Cyber Profile is available at https://cyberriskinstitute.org/the-profile/.

FEDERAL RESERVE

Supervision and Regulation Letters

Supervision and Regulation (SR) letters address significant policy and procedural matters related to the Federal Reserve System's supervisory responsibilities.

Content: SR letters cover a variety of topics including: information technology guidance, information technology examination process, cybersecurity, business continuity/disaster recovery, and operational resilience.

Notifications: Active SR letters are available at www.federalreserve.gov/supervisionreg/srletters/srletters.htm. Additionally, topical supervisory policy and guidance is located on the Information Technology Guidance webpage.

SR letters related to cybersecurity:

- SR 24-7: FFIEC Cybersecurity Assessment Tool Sunset Statement
- SR 22-4: Contact Information in Relation to Computer-Security Incident Notification Requirements
- SR 21-14: Authentication and Access to Financial Institution Services and Systems
- SR 05-23: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- SR 01-15: Standards for Safeguarding Customer Information

Federal Reserve webpages of interest:

- Operational Resilience, at www.federalreserve.gov/supervisionreg/topics/operational-resilience.htm.
- Cybersecurity and Operational Resilience, at www.federalreserve.gov/supervisionreg/cybersecurity-and-operational-resilience.htm.

Community Banking Connections

Community Banking Connections is a source for information on guidance, resources, and tools that help community banks across the United States.

Content: Information technology, information security, and cybersecurity are often covered. Articles on these topics can be found at www.communitybankingconnections.org/topical-index.

Notifications: Sign up to receive notifications at www.communitybankingconnections.org.

***Community Banking Connections* articles related to cybersecurity:**

- Security in the Cloud: A Discussion with the Regulators
- 2024 Midwest Cyber Workshop Recap
- Ransomware: A Multifaceted Menace
- Ransomware Defense: A Discussion with the Regulators
- Endpoint Security: On the Frontline of Cyber Risk
- Maintaining Strong Cybersecurity Controls Is Imperative as Online Threats Increase
- Notifying Primary Federal Regulators About Computer-Security Incidents

Ask the Fed

Ask the Fed is a program for officials of banks and bankers' associations to address new or important regulatory issues or supervisory guidance.

Content: Sessions can be viewed at https://bsr.stlouisfed.org/askthefed. For past information technology content, select the "All Calls" tab.

Notifications: Register for an account on the Ask the Fed site, then opt in to communications under "My Account."

Ask the Fed sessions related to cybersecurity:

- Sunset of the FFIEC CAT Session 2: A Discussion with the Cyber Risk Institute (CRI) (April 2025)
- Sunset of the FFIEC CAT Session 1: A Discussion with the Center for Internet Security (CIS) (March 2025)
- Insights with the Cybersecurity and Infrastructure Security Agency (CISA) Part II (December 2024)
- Insights with the Cybersecurity and Infrastructure Security Agency (CISA) (February 2024)
- Maturing Your IT Risk Management and Governance Framework (December 2022)
- Ask the Regulators: Computer-Security Incident Notification Rule (April 2022)
- For more information about Ask the Fed: Questions@AsktheFed.org

The Supervision Contact System

The Supervision Contact System (SCS) is used by the Federal Reserve Bank (FRB) supervision functions to communicate Board of Governors supervisory guidance and other information in a timely manner to the financial institutions they supervise.

Content: SCS is used primarily to distribute information needed by financial institutions within the scope of the FRB's supervision. Such regulatory information includes SR letters, Consumer Affairs letters, and other supervisory guidance.

Notifications: Individuals from supervised institutions create a profile on the SCS website (a secure website hosted by the FRB of St. Louis) at https://supervisioncontactsystem.org and follow the prompts on https://Login.gov.*

If you have any questions, please contact the SCS Support Center at: 855-727-5919 or supervision.contact@stls.frb.org.

The Emergency Communications System

The Emergency Communications System (ECS) is a free service that is a means for state supervisory agencies and FRB supervision functions to communicate with financial institutions they regulate in an emergency situation.

Content: ECS is only used to contact institutions during real emergencies and during semiannual tests. The following situations might necessitate the use of ECS:

- Natural disasters
- Man-made disasters: Chemical biological events or threats
- Events affecting the financial markets
- Cyber events

Notifications: Individuals from supervised institutions create a profile on the ECS website (a secure website hosted by the Federal Reserve Bank of St. Louis) at https://bsr.stlouisfed.org/ecs and follow the prompts on https://Login.gov.*

If you have any questions, please contact the ECS Support Center at: 855-327-5333 or ecs.support@stls.frb.org.

LAW ENFORCEMENT CONTACT INFORMATION

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) has 55 field offices (also called divisions) centrally located in major metropolitan areas across the United States and Puerto Rico. Field offices carry out investigations, assess local and regional crime threats, and work closely with partners on cases and operations.

Find a field office near you at www.fbi.gov/contact-us/field-offices.

The United States Secret Service

With local field offices across the United States, the Secret Service also has a Cyber Fraud Task Force staffed with special agents, technical experts, and forensic analysts.

Find a field office near you at www.secretservice.gov/contact/field-offices.

*Institutions should add Frb.org and Stls.frb.org email domains to their safe-sender list to ensure receipt of SCS and ECS communications.

REGULATORY CALENDAR

Rules Currently in Effect or Proposed
Final and proposed rules that have not been affected by the ongoing regulatory review

DATE†	REGULATION	REGULATORY CHANGE
06/18/25	§1071 (Reg. B)	Consumer Financial Protection Bureau (CFPB) issues interim final rule to extend compliance deadlines for its rule under Regulation B implementing §1071 of the Dodd–Frank Act
06/03/25	FHA regulation	Rescission of Affirmative Fair Housing Marketing Regulations (24 CFR Part 108 and 24 CFR §200.600–200.640)
10/01/25	Reg. Z	Agencies issue final rule on quality control standards for automated valuation models
07/01/25	Reg. CC	Agencies implement inflation-adjusted dollar thresholds for Regulation CC funds availability
01/01/25	Reg. Z	Agencies announce dollar thresholds for smaller loan exemption from appraisal requirements for higher-priced mortgage loans
01/01/25	Regs. M and Z	Agencies adjust dollar thresholds for consumer credit and lease transactions
12/13/24	Reg. V	Consumer Financial Protection Bureau (CFPB) issues an advance notice of proposed rulemaking for furnishing information about coerced debt
07/26/24	FHA, Regs. Z and B	Final Interagency Guidance on Reconsiderations of Value of Residential Real Estate Valuations
11/14/23	Reg. II	Federal Reserve issues proposal to lower the maximum interchange fee a large debit card issuer may charge
10/12/23	Reg. B	CFPB and Department of Justice issue Joint Statement on Fair Lending and Credit Opportunities for Noncitizen Borrowers Under the Equal Credit Opportunity Act

† Because proposed rules do not have an effective date, we have listed the *Federal Register* publication date.

REGULATORY CALENDAR

Rules Under Review

Prior proposed rules or final rules that were subsequently rescinded, stayed in litigation, or otherwise under review

DATE	REGULATION	REGULATORY CHANGE	STATUS
10/01/25	Regs. E and Z	CFPB issues final rule for overdraft fee for very large financial institutions	Repealed 05/08/25
03/17/25	Reg. V	CFPB issues final rule to limit the use of medical debt in underwriting consumer credit	Stayed in litigation
01/17/25	12 U.S.C. §1033	CFPB issues final rule on personal financial data rights	Stayed in litigation
01/09/25	12 C.F.R. §1090.109	CFPB issues larger participant final rule for the general-use digital consumer payment applications market	Stayed in litigation
12/13/24	Reg. V	CFPB proposes defining data brokers as consumer reporting agencies subject to the Fair Credit Reporting Act	Withdrawn 05/15/25
07/30/24	Reg. Z	CFPB issues interpretive rule applying certain provisions of Regulation Z to Buy Now, Pay Later loans	Withdrawn 05/12/25
05/14/24	Reg. Z	CFPB issues final rule for credit card penalty fees	Vacated 04/14/25
02/01/24	Reg. BB	Agencies issue final rule to modernize their implementing regulations for the Community Reinvestment Act	Withdrawn 07/16/25
01/31/24	12 C.F.R. §1042.2	CFPB issues proposal to prohibit fees for instantaneously declined transactions	Rescinded 01/14/25
10/30/23	n/a	Agencies issue principles for climate-related financial risk management for large financial institutions	OCC Withdrawal 03/31/25

How to Subscribe to *Consumer Compliance Outlook* and Outlook Live

CCO and Outlook Live are complimentary Federal Reserve System outreach platforms. *CCO* is a quarterly newsletter focusing on federal consumer compliance topics, while Outlook Live is a webinar series focusing on consumer compliance topics.

To subscribe to *CCO* and Outlook Live, please visit consumercomplianceoutlook.org. There, you can choose to receive future editions of *CCO* in electronic or print format. If you provide your email address while subscribing, we will also notify you by email of upcoming Outlook Live webinars.

Suggestions, comments, and requests for back issues are welcome in writing, by telephone (215-574-6500), or by email (outlook@phil.frb.org). Please address all correspondence to:

Kenneth Benton, Editor
Consumer Compliance Outlook
Federal Reserve Bank of Philadelphia
SRC 7th Floor NE
Ten Independence Mall
Philadelphia, PA 19106

Calendar of Events

October 9, 2025	Securing the Future: Fraud Trends, Lessons, and Insights Federal Reserve Bank of Philadelphia Virtual
November 6–7, 2025	New Perspectives on Consumer Behavior in Credit and Payments Markets Conference Federal Reserve Bank of Philadelphia Philadelphia, PA
November 16–19, 2025	CRA & Fair Lending Colloquium JW Marriott Los Angeles Los Angeles, CA

Scan with your smartphone or tablet to access *Consumer Compliance Outlook* online.

consumercomplianceoutlook.org