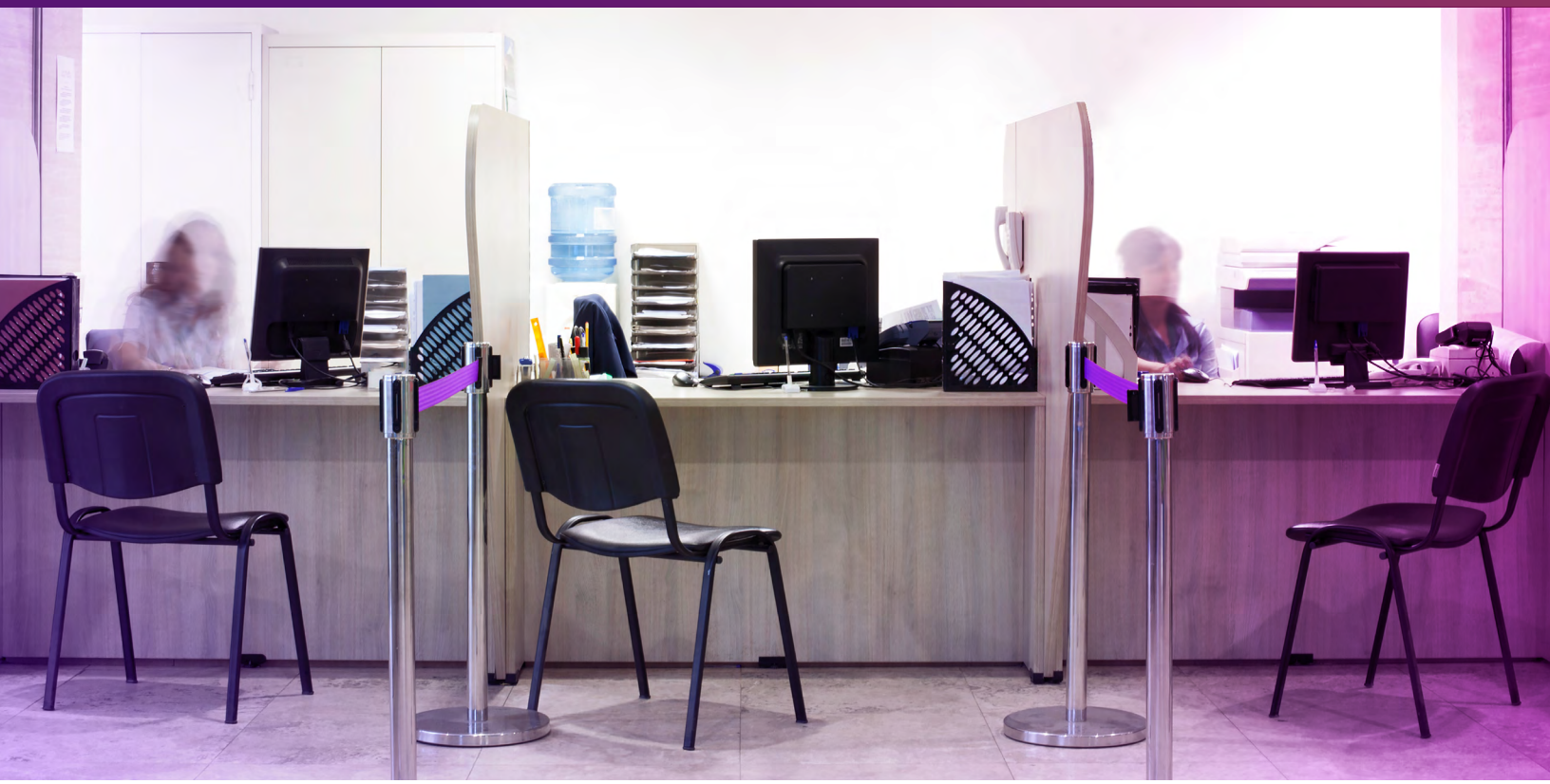
AICPA

FVS Eye on Fraud

The AICPA Forensic and Valuation Services quarterly report on fraud trends and topics



Banking on Vigilance: Modern Fraud Trends and Prevention Strategies for Financial Institutions

Issued by the AICPA® FLS Fraud Task Force
Lead author: **David Stone, CPA, MBA, CFE**

Winter 2026, Issue 2

Inside this issue

Introduction 1
History of banking fraud 2
Occupational fraud 2
Asset misappropriation 2
Financial statement fraud 5
External fraud 8
Check fraud 8
ATM theft and card skimming 9
Social engineering fraud 10
Ransomware 12
Conclusion 12

Introduction

It began with a simple deception — fraudulent applications submitted to banks for merchant processing accounts. But behind the paperwork was a sprawling scheme that would siphon more than $128 million from the financial system. In January 2025, federal prosecutors unsealed indictments against four individuals, accusing them of orchestrating one of the most audacious bank fraud and money laundering conspiracies in recent memory. [1]

[1] Internal Revenue Service, "Four Indicted in Conspiracy to Commit Bank Fraud and Money Laundering Schemes Involving More Than $128 Million in Criminal Proceeds," news release, January 14, 2025, irs.gov/compliance/criminal-investigation/four-indicted-in-conspiracy-to-commit-bank-fraud-and-money-laundering-schemes-involving-more-than-128-million-in-criminal-proceeds.

Using stolen personal information, the group created a network of e-commerce operations that thrived on high-risk and deceptive sales tactics. These merchant accounts, obtained under false pretenses, allowed the group to process credit and debit card payments while shielding themselves from liability. The result: a digital facade that masked criminal intent behind legitimate-looking transactions.

But the fraud didn't stop at the point of sale. The proceeds were laundered through a web of conspirator-controlled bank accounts and used to pay for advertising and other services that fueled the scheme. Lavish homes, now subject to forfeiture, in Miami Beach, Florida, and in the U.S. Virgin Islands stand as monuments to the scale of the deception.

Still unfolding, this case is a stark reminder of how sophisticated fraudsters exploit digital infrastructure and regulatory deficiencies to build empires on stolen trust. It also signals a growing trend: the convergence of identity theft, e-commerce manipulation, and money laundering into a single, scalable fraud model — one that regulators and banks must urgently learn to detect and dismantle.

History of banking fraud

The earliest recorded financial fraud case comes from ancient Greece around 300 B.C., involving a merchant named Hegestratos.[2] He took out a bottomry loan, a type of maritime insurance, against his ship and cargo, planning to sink the vessel after departure and keep both the loan and the goods. When the crew discovered his scheme, Hegestratos's attempt to escape by swimming away failed, and he drowned in the process. As this incident illustrates, exploiting financial systems for personal gain is as old as commerce itself.

From the Greek seas more than 2,300 years ago, to the emergence of the Ponzi scheme in the 1920s,[3] to check fraud in the mid-20th century, to the relatively recent onset of digital fraud schemes, it's clear that fraudulent activity in some shape or form is here to stay. Although *how* fraud is perpetrated changes and adapts, the essence of the schemes remains much the same. In this Eye on Fraud, we discuss all aspects of banking fraud, including common occupational fraud schemes; external threats, including those that affect bank customers; and, probably most importantly, effective measures that financial institutions can take to prevent fraud. We collectively refer to these prevention techniques (which appear throughout this issue) as "prevention recipes," collections of best practices that, when employed together, can help prevent fraudulent activity. As with all good recipes, these can be modified in whatever ways that work best for your organization.

This Eye on Fraud is organized into two primary sections: (1) occupational fraud and (2) external fraud.

Occupational fraud

Occupational fraud is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets."[4] It typically involves employees or executives who exploit their position of trust to commit fraud against the organization.

Occupational fraud falls into three main categories:

1. **Asset misappropriation.** Theft or misuse of an organization's assets (e.g., stealing cash, falsifying expense reports)

2. **Corruption.** Conflicts of interest, bribery, or extortion

3. **Financial statement fraud.** Intentional misrepresentation of financial information (e.g., overstating revenues or understating liabilities)

In this publication, we will focus on asset misappropriation and financial statement fraud.

Asset misappropriation

We begin with asset misappropriation, the most common but least costly of the three categories of financial institution occupational fraud.[5] Financial institutions are asset-intensive, with most of their assets held as loans to borrowers. Banks also carry substantial amounts of customer deposits, a liability on their balance sheets but also an area ripe for misappropriation.

---

[2] "The History and Evolution of Fraud," Fraud.com, n.d., fraud.com/post/the-history-and-evolution-of-fraud.

[3] Celeste Neill, "The Rise and Fall of Charles Ponzi: How a Pyramid Scheme Changed the Face of Finance Forever," *History Hit*, March 1, 2023, historyhit.com/the-rise-and-fall-of-charles-ponzi-how-a-pyramid-scheme-changed-the-face-of-finance-forever/.

[4] "Occupational Fraud — Everything About Detection and Prevention," Fraud.com, n.d., 7, fraud.com/post/occupational-fraud.

[5] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations®*, 2024, 4, 10, legacy.acfe.com/report-to-the-nations/2024/.

Mortgage fraud

Between 2018 and 2023, two mortgage loan originators operating in New Jersey engaged in a multiyear scheme to defraud banks through falsified loan applications. One was a top-producing originator who ranked fourth nationally in 2022, giving them significant influence over lending processes.[6]

The loan originators exploited vulnerabilities in mortgage underwriting by doing the following:

- **Misrepresenting occupancy status.** They claimed borrowers would occupy properties as primary residences when in fact the properties were intended for rental or investment purposes.
- **Fabricating documentation.** They submitted false statements and altered documents to secure loans under more favorable terms, such as lower interest rates.
- **Leveraging automation.** They relied heavily on automated approval systems, which allowed fraudulent applications to bypass manual checks.

This scheme enabled the originators to close more loans, earn higher commissions, and maintain top performance rankings. Because of inadequate internal controls and overreliance on automated verification, the fraud persisted for years.

Outside actors can also perpetrate mortgage fraud. For instance, journalist Hanna Guidry reported in 2025 on the guilty plea of a CPA who committed fraud while working as a financial manager. The CPA pled guilty to defrauding commercial lenders by providing false and fraudulent rent rolls and forged lease agreements to obtain loans for companies controlled by co-conspirators who then allegedly made some or no payments and ultimately defaulted on the loans. This caused losses to the financial institutions and commercial lenders totaling more than $19 million.[7]

The prevention recipe:

- **Strong tone at the top.** Tone at the top is one of the principles outlined in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control – Integrated Framework[8] and has thus been a pillar of strong internal control environments since the framework's inception (and likely long before then) in 1992.[9] If management establishes a strong tone at the top and leads by example, employees are likely to follow suit. Undue pressure on employees to meet sales goals, for instance, could lead them to rationalize fraudulent activity that they would not otherwise engage in.
- **Strengthen verification.** Implement multilayered checks for occupancy claims and borrower intent. Segregation of duties is always important, and when referencing a financial institution's largest asset, it likely carries more significance. Ensure that policies and procedures are in place to have a second review of critical loan documents. For instance, have someone independent from the loan call the borrower to verify pertinent borrower details. This may not be necessary for every loan origination but could be a good prevention technique for loans thought to carry more risk. Mortgage loan underwriters also often serve as an independent last line of defense. Therefore, ensure their processes also adequately consider document verification.
- **Monitor high-performing employees.** Exceptional production should trigger enhanced compliance reviews. Incorporate detailed reviews of your highest performers' loan portfolios. This could likely be completed after a loan has been originated. On a sample basis, originated loans could be selected for detailed testing.
- **Reduce automation blind spots.** Combine automated systems with periodic manual audits to detect anomalies. Technology can enable audits and oversight of problem areas as they are developing.[10] Although automated loan originations are becoming a necessity, as customers demand convenience, convenience is often at the sacrifice of consumer protection. In general, convenience versus protection is a "see-saw" financial institutions will need to balance on as emerging technologies are incorporated into operations. These automated systems require a "human-in-the-loop," not just to keep employees in check but also to ensure customers are not providing incomplete or inaccurate information, whether by error or for more nefarious reasons.

[6] Joe Wilson and Sarah Atkinson, "The Escalating Threat of Mortgage Fraud," blog, Bradley, May 6, 2024, bradley.com/insights/publications/2024/05/the-escalating-threat-of-mortgage-fraud

[7] Hanna Guidry, "Public Accountant Pleads Guilty $19,000,000 Bank Fraud," Western Mass News, June 16, 2025, westernmassnews.com/2025/06/17/public-accountant-pleads-guilty-19000000-bank-fraud/.

[8]

[9] "Guidance [Internal Controls]," COSO, coso.org/guidance-on-ic.

[10] "Guidance [Fraud Deterrence]," COSO, coso.org/frauddeterrence.

Dormant and employee accounts

Deposit accounts are a prime area for fraudulent activity, especially that perpetrated by bank employees. Employees looking to steal cash from depositor accounts will likely turn their attention to dormant accounts. As the name implies, these are accounts that have been inactive for a specified period. In this case, *inactive* means they have had no activity (deposits, withdrawals, etc.) whatsoever for a period of time. If an employee can transact on these accounts, they could steal the funds, either withdrawing the cash altogether or transferring it to their own bank accounts. Although this could be perpetrated by employees, an outside actor could use dormant accounts to their advantage, especially if they've stolen an individual's identity. The idea is that, if there has been no activity on these accounts, the account owners are unlikely to be closely monitoring them.

The prevention recipe:

- **Automated dormant-account controls.** Most banking systems have built-in controls when an inactive account goes into dormant status (usually triggered after one year of inactivity). When an account goes into dormancy, it is included on a deposit file maintenance report, which tracks changes on deposit accounts (address changes, interest rate changes, status changes, etc.). This file maintenance report should be reviewed daily by someone who does not have the ability to make deposit account changes but is knowledgeable of the financial institution's depositors. Particular attention should be given to changes of address, as these could indicate an employee attempting to reroute depositor notifications and statements to conceal fraudulent activity.

- **Dormant-account reactivation controls.** Once an account is in dormant status, there should be a higher barrier to transact on the account. For instance, the account owner should be required to visit a branch and show proof of identification, which the branch should maintain a copy of. Security questions, likely established by the customer on opening the account, could also serve as a form of multifactor authentication. As when an account goes into dormant status, an account coming out of dormant status will also show up on the deposit file maintenance report. Review of this change (account reactivation) is arguably more essential than that when the account goes into dormant status. The file maintenance report reviewer should obtain proof of identification from the individual requesting account reactivation and match it to other documents on file for the account. This independent review will help detect if an employee or even an outside actor is trying to access dormant accounts.

- **Employee account controls.** Ideally, employees should be unable to transact on their own accounts. This should be a built-in limitation where the system disallows them to post any activity to their own account without a second approval, ideally that of a supervisor. However, there may be instances where the banking system is unable to prevent employees from transacting on their own accounts. In such cases, it is important to establish through policy that employees are prohibited from transacting on their own accounts. However, beyond establishing policy, management should also review employee account activity at least monthly. Although this might not be a full review of all employee accounts, it could be a sample of employees that rotates each month.

  This is also a good opportunity to use existing software solutions. Many financial institutions now incorporate fraud detection software as part of their anti-money laundering and Bank Secrecy Act efforts. This software analyzes both customer and employee activities and identifies anomalies in individual customers' transaction activity. The software first establishes each customer's baseline behavior, which then allows it to promptly identify suspicious activity.

  As an example, let's say we have a small business owner who owns a restaurant. The restaurant owner typically deposits cash once a week, in person, at their bank's local branch. The merchant also deposits credit card sales once per week. Weekly deposits for cash and credit card sales are generally $40,000–$50,000. If there were suddenly a series of $5,000–$10,000 transactions occurring daily, that would likely be flagged for further review. Bank management, possibly a compliance or risk officer, could then review the activity. To tie this example to dormant and employee accounts, let's say the restaurant owner's spouse is a branch teller at the same bank and is thus possibly transferring dormant account funds into their spouse's restaurant account.

- **Data analytics.** Data analytics are becoming an increasingly effective tool in identifying potentially fraudulent activity.[11] In the case of dormant accounts, consider running monthly analysis. This analytical equation could be as follows:

$$\frac{\text{\$ Value of Dormant Accounts}}{\text{\# of Dormant Accounts}}$$

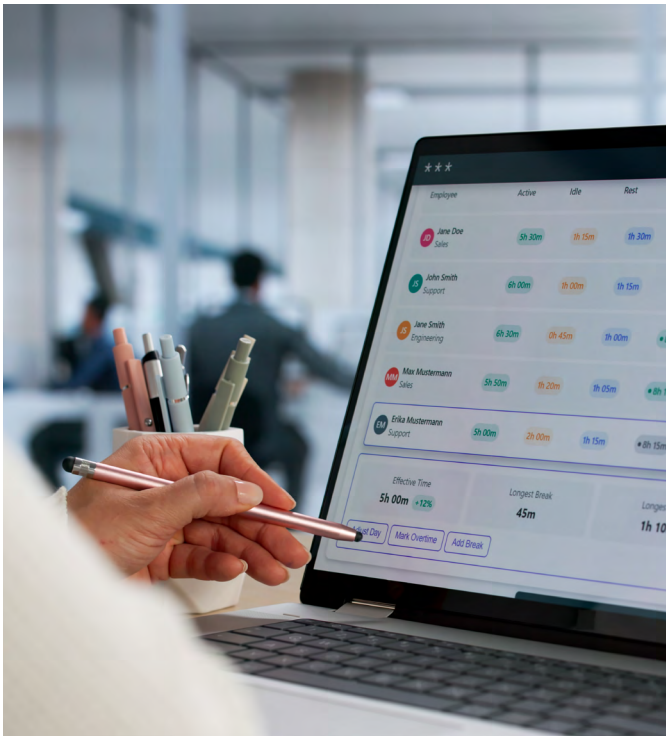
  A significant decline in this data point, or a significant decline in both the numerator and denominator, could indicate suspicious activity. The same equation could also be performed for employee accounts.

[11] "Guidance [Fraud Deterrence]," COSO, coso.org/frauddeterrence

Payroll-related fraud

Payroll tends to be the largest expense for any financial institution and thus tends to be a target area for unscrupulous employees. Although it was not at a financial institution, the lead author of this report once worked with a small not-for-profit (NFP) that lacked any segregation of duties for its payroll processes. In conducting a forensic review of the NFP's bank account activity, he discovered that one employee — who had the ability to process, approve, and distribute payroll — had received more than 70 paychecks in one fiscal year. The NFP had a weekly payroll cycle — that's a lot of off-cycle bonuses! The employee made no effort to conceal their fraud — all 70-plus checks were written to them. Given the small size of the organization, even a simple review of monthly bank statements could have sufficed as a mitigating control.

Similarly, inadequate controls around payroll onboarding of new employees could enable the creation of fictitious employees, which could in turn allow for an employee to receive more than one paycheck per pay period. A fictitious employee scheme might be difficult to pull off in a small organization (if proper review controls are in place), where an unfamiliar name on the payroll would likely catch the attention of management. For a large organization, however, with hundreds if not thousands of employees, such a scheme would be more difficult to detect.



The prevention recipe:

- **New-employee onboarding.** Onboarding new employees is critical for many reasons, but one item that might be overlooked is the ability of an effective onboarding process to prevent fraud and, specifically, to prevent the creation of fictitious employees. Recall the banking systems referenced earlier that create file maintenance reports; an organization's payroll provider should, along similar lines, provide an employee change report every pay period. This report should detail any new employees added to payroll as well as any changes to existing employees' payroll information (such as a change to their mailing address, deductions, direct deposit routing, etc.). An employee who has no role (including entering the new employee into the payroll system) in the onboarding process should review the employee change report and corroborate changes with source documentation. For new employees, that could mean reviewing a signed I-9 or W-4 to verify that the new employee is legitimate. Missing documentation, such as missing I-9s, W-4s, or even background checks, may be indicative of a fictitious employee.
- **Employee terminations.** Terminated employees can be used to perpetrate fraud. On termination and final payment, such former employees should be immediately disabled in payroll systems. Failure to do so could allow an employee to make a quick change to address info or to direct-deposit routing and, if they have the ability to process payroll, direct paychecks to the terminated employee (which would ultimately go to the nefarious employee). Combining strong segregation of duties with an efficient termination process makes these schemes significantly harder to carry out. Such a process probably requires coordination across multiple departments. The terminated employee's department must initiate the process, which should involve notifying IT (to disable access to systems) and HR/payroll. As with onboarding, an employee independent from the process should review the employee change report, ensuring that all employees terminated during that pay period appear on the report.
- **Analytics.** Analytics again prove to be useful in detecting potentially fraudulent activity. Although a simple comparison of payroll expense from one pay period to the next may not (unless there's significant change) be precise enough to identify potentially fraudulent activity, looking at nonfinancial trends, such as new and terminated employees per month or new and terminated employees by location, could help discern unusual activity that warrants further investigation. For instance, if a location has unusually large turnover, that may be indicative of payroll manipulation.

Financial statement fraud

Although it's the least common type of occupational fraud, financial statement fraud is the costliest for financial institutions.[12] Any industry has specific areas prone to financial statement fraud. Accounting estimates, given the judgment and subjectivity involved, tend to be among the areas most vulnerable to financial statement fraud. Financial institutions arguably have one of the most significant and complex accounting estimates: the allowance for credit losses on loans and off-balance-sheet credit exposures. It should be noted that not every misstatement is necessarily indicative of fraudulent activity; after all, intent matters. The areas we discuss here are highly complex and nuanced. Thus, it is possible a misstatement is simply due to error.

Allowance for credit losses

Although the allowance for credit losses for financial institutions serves the same purpose as an allowance for credit losses for (let's say) a manufacturer, the duration of the underlying assets — trade receivables in the case of a manufacturer — tend to be shorter-duration assets than loans, which tend to have longer durations, sometimes staying on the balance sheet for upwards of 30 years. These longer durations inherently require a much more complicated estimation process than a shorter-duration financial asset does.

The current expected credit loss (CECL) standard overhauls the previous incurred loss model.[13] Where the incurred loss model required that a loss be probable of having been incurred before being recorded, CECL allows an institution to record expected losses before the probable threshold has been met. In this way, CECL effectively lowers the threshold that must be met to record a loss in the financial statements. This was largely the result of the Great Recession, where many financial institutions wanted to proactively record losses but could not because the probable threshold had not yet been met.[14] As a result, CECL incorporates a forecasting component whereby financial institutions must forecast losses over a reasonable and supportable period. Thus, there are a multitude of inputs that need to be assessed and determined by management periodically, such as the expected life of the loans being assessed, loss rates used in the calculation, forecasting techniques, and qualitative factors (adjustments outside of the quantitative model), to name a few. The allowance for credit losses is complicated, has many rules, and requires subjective judgment. Because of this, it is a prime area for malevolent actors to target and exploit.

A principal concern related to financial statement fraud is changes in these inputs from one period to the next without adequate documentation. Given the possible inputs, of primary concern is manipulation of earnings. If a financial institution is doing well financially, it might unjustifiably change these inputs in a manner that inflates the allowance for credit losses. Because this would reduce earnings, this might seem counterintuitive. But by inflating the allowance for credit losses, the financial institution could increase earnings by releasing this excess reserve (again, by changing its inputs) in periods that prove financially challenging. This is sometimes referred to as creating "cookie jar reserves." A change in the allowance for credit losses directly affects earnings, as the sample journal entry that follows demonstrates:

To increase the allowance for credit losses (the entry would be the opposite to reduce the allowance for credit losses):

DEBIT: Credit loss expense	$XXX	
CREDIT: Allowance for credit losses		$XXX

Specific reserves

When a loan does not share the risk characteristics of other loans within the bank's portfolio, it must be individually evaluated. Individual evaluation can occur using one of two methods: (1) calculating the present value of the expected future cash flows and comparing it to the loan balance, or (2) comparing the value of the loan's collateral to the loan balance. Any shortfall resulting from either method is recorded as an allowance for credit losses. Specific to the latter evaluation method (often referred to as "the collateral method"), the appraisal of the underlying collateral is a significant input in determining the collateral value and, therefore, in determining the allowance for credit losses (if any). Inflating property values, whether through collusion with appraisers or fraudulent appraisals, will have a direct impact on the allowance for credit losses.

[12] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations®*, 2024, 4, 10, legacy.acfe.com/report-to-the-nations/2024/.

[13] FASB Accounting Standards Update (ASU) No. 2016-13, *Financial Instruments — Credit Losses (Topic 326): Measurement of Credit Losses on Financial Instruments.*

[14] ASU No. 2016-13.

Delayed loan charge-offs

Once a loan is deemed uncollectible, it should be promptly charged off. A loan that carried an inadequate allowance for credit losses will result in increased credit loss expense and thus reduce earnings. Therefore, to prevent reduced earnings in one period, management might wait to charge off a loan until a subsequent period.

To charge off a loan that has been deemed uncollectible:

DEBIT: Allowance for credit losses	$XXX	
CREDIT: Loans receivable		$XXX

To adjust the allowance for credit losses to actual (when running the allowance calculation):

DEBIT: Credit loss expense	$XXX	
CREDIT: Allowance for credit losses		$XXX

Non-accrual accounting

Typically, loans 90 or more days past due are placed on non-accrual status. This means that any interest income on the loan ceases to accrue (meaning it's also not recorded as interest income in the financial statements), and any previously accrued interest should be reversed against interest income.

To reverse previously accrued interest on the day a loan goes on non-accrual status:

DEBIT: Interest income	$XXX	
CREDIT: Accrued interest		$XXX

When this loan subsequently goes back onto accrual status (typically after at least six months of sustained payments), any previously reversed interest *cannot* then be recorded into interest income. Rather, it must be either accounted for on either a cash or cost recovery basis. Given this summary of proper accounting, the following are a few ways management could incorrectly conduct non-accrual accounting for the purpose of inflating earnings:

1. Not putting a loan on non-accrual status if it is 90 or more days past due (some exceptions do exist)
2. Not reversing accrued interest when a loan is put on non-accrual status
3. Prematurely putting a non-accrual loan back on accrual status
4. Re-recording previously reversed accrued interest when a loan returns to accrual status.

Fair value — Investments and derivatives

Certain items within a financial institution's financial statements are required to be marked to fair value. Some notable examples are investments and derivatives. Outside of the allowance for credit losses, determining the fair value of investments and derivatives is likely the most significant accounting estimate in a financial institution's financial statements. Most financial institutions use independent third parties to assist in determining the fair value of investments and derivatives. However, manual adjustments from third-party-provided reports could indicate intentional misstatement.

The prevention recipe:

- **Strong governance framework.** The few CECL inputs mentioned earlier are only a subset. And although it may seem simple to follow along, it can be easy (given everything else happening on a day-to-day basis), to miss something. A strong governance framework over the allowance for credit losses calculation is essential. Consider providing a "key input matrix" to those charged with governance, whereby they can see the key inputs that are being utilized in the institution's allowance calculation, including what changed since the last calculation. Also, given that the allowance for credit loss estimate now often relies on complex modeling techniques, financial institutions should refer to the federal banking agencies' model risk management guidance and should consider getting models periodically validated by an independent party.[15]

  Similarly, any adjustments made to fair values obtained from third-party reports for investments and derivatives should be thoroughly documented; moreover, those charged with governance should demand the rationale for such adjustments.

[15] Board of Governors of the Federal Reserve System, SR 11-7: Guidance on Model Risk Management, April 4, 2011, federalreserve.gov/supervisionreg/srletters/sr1107.htm.

- **Appraisal review.** Given the significance of the appraisal when analyzing individual loans for a specific reserve under the collateral method, financial institutions should ensure significant (likely determined via a dollar threshold or property type) appraisals are reviewed by someone knowledgeable enough to challenge an appraisal that seems inaccurate. When using the appraisal in the allowance for credit losses calculation, there should be another independent check to ensure the correct value was used.

- **Loan charge-off checklists.** As a best practice, we frequently see a checklist utilized as part of the loan charge-off process. Such checklists are loan-specific and are often created well before a charge-off decision is made. For instance, a checklist may be started once a loan, as part of the specific reserve process discussed earlier, is individually evaluated. The checklist is thereafter referred to each time the loan is reevaluated. If it is ultimately decided to charge off a loan, the appropriate approvals and routing instructions would be entered in a dedicated area of the checklist to timely alert the accounting department of the charged-off loan.

- **Non-accrual loan review.** A delinquency report showing all loans 30 or more days past due should be run on a periodic basis, with any loans 90 or more days past due cross-referenced to a non-accrual report. If any loans 90 or more days past due are still accruing, the reviewer should ensure there is appropriate documentation supporting this decision. For loans new to the non-accrual report, the reviewer should check the loan details to ensure that any previously accrued interest was reversed; for loans removed from the non-accrual report since the last such report was generated, the reviewer should check to ensure that any previously accrued interest wasn't immediately recorded as interest income.

External fraud

To this point, our primary focus has been on fraud schemes that start inside the organization. As if that's not enough to worry about, there is also a plethora of external fraud threats to guard against. In this section, we examine some of the most common threats as well as some emerging threats.

Check fraud

You may see "check fraud" and think, "That's one of the oldest tricks in the book." And you're right: in the 1970s, check fraud surged in the United States, hitting $4 billion in 1976.[16] However, check fraud remains prevalent and, despite the decline in the use of checks, they are still a common payment method, making them a target for fraudsters. Check fraud can take several forms, including forgery, alteration, and counterfeiting. For instance, check washing involves stealing a check, erasing the original details, and altering the payee name and amount before cashing it. Another method is creating counterfeit checks using real account numbers but depositing them under fake identities.

The statistics are alarming. According to the Financial Crimes Enforcement Network (FinCEN), in 2022 there were 680,000 reports of check fraud, nearly double the number reported in 2021. The surge in mail-theft-related check fraud has also been significant, with a 161% increase in reports of mail theft complaints from March 2020 to February 2021. Criminals have even resorted to armed robberies of postal carriers to obtain master keys that open mailboxes, providing easy access to checks. A recent investigation revealed that criminal rings, including street gangs, used sham bank accounts and insider help to launder stolen checks. In one case, insiders opened hundreds of accounts using fake IDs, enabling a criminal ring to deposit over $1.7 million in checks stolen from church mailboxes.[17]

The federal banking agencies are taking notice. On June 16, 2025, the Federal Reserve Board, along with the FDIC and the Office of the Comptroller of the Currency, issued a joint request for public comment on strategies to mitigate payments fraud, with a particular emphasis on check fraud. The agencies highlighted that *payments fraud*, defined as "illegal means used to make or receive payments for personal gain," often spans multiple institutions and payment systems, making collaborative efforts essential. They are seeking input on five key areas: interagency and industry collaboration, consumer and business education, regulatory and supervisory measures, improved data collection and information sharing, and enhancements to Federal Reserve Banks' operational tools. The American Bankers Association has publicly welcomed the initiative, calling for a coordinated national strategy to combat check fraud.[18]

[16] "Frank Takes: How Banks Solved the Check Fraud Boom of the 1970s," Point Predictive, November 1, 2024, pointpredictive.com/frank-takes-how-banks-solved-the-check-fraud-boom-of-the-1970s/.

[17] Financial Crimes Enforcement Network, "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail" [FIN-2023-Alert003], February 27, 2023, fincen.gov/news/news-releases/fincen-alert-nationwide-surge-mail-theft-related-check-fraud-schemes-targeting; David Maimon and Kurt Eichenwald, "Heists Worth Billions," The Conversation, June 21, 2023, theconversation.com/us/investigations/mailbox-robberies-drop-accounts-checkwashing-fraud-gangs-of-fullz.

[18] Board of Governors of the Federal Reserve System, "Federal bank regulatory agencies seek comment to address payments and check fraud," news release, June 16, 2025, federalreserve.gov/newsevents/pressreleases/bcreg20250616a.htm; "Banking agencies seek public comment on strategies to combat payments fraud," ABA Banking Journal, June 16, 2025, bankingjournal.aba.com/2025/06/banking-agencies-seek-public-comment-on-strategies-to-combat-payments-fraud/.

The prevention recipe:

Check fraud can be tough to identify, especially with a lack of continuity in customer-facing transactions due to the prevalence of mobile banking. However, there are some tools and techniques banks can employ to combat check fraud:

- **Positive pay.** Positive pay involves companies informing their bank about issued checks ahead of time, allowing the bank to verify the checks before processing them.[19] Any discrepancies (amount, payee, check number) trigger alerts for review. This is often seen as a great value-added service that financial institutions can often charge a fee for.

- **Automated signature verification.** Although financial institutions likely already verify signatures, the process tends to be manual and reliant on human review, which can be prone to error. Software now exists that can assist by comparing and matching signatures to customer source documents, such as a signed agreement. Any potential exceptions can then be reviewed further.

- **Real-time fraud monitoring.** As we mentioned earlier in the context of employee account review, software used for anti-money laundering compliance can serve multiple purposes. Indeed, such software can be an effective tool in monitoring for check fraud. These tools, which are starting to incorporate artificial intelligence (AI), can analyze transaction patterns and flag anomalies, such as unusual check amounts or altered payee names.

- **Data sharing and collaboration.** As alluded to in the federal banking agencies' request for public comment, data sharing, especially as it relates to check fraud and, more generally, to payments fraud, can be a powerful prevention technique. Fraudsters often conspire — there's no reason why financial institutions shouldn't also collaborate and compare notes on what they're seeing on the front lines.

ATM theft and card skimming

A surge in ATM thefts from New York City bodegas has emerged as a growing physical-security threat within the larger context of banking fraud, with crews using brute-force tactics to rip machines from storefronts. Dubbed the "Midnight Smashers," one group is suspected of targeting at least 49 locations across Brooklyn, Queens, and the Bronx between September and December 2024, often using stolen vehicles and disabling security systems before hauling away 200-pound ATMs.[20] These smash-and-grab heists, sometimes completed in under five minutes, have netted tens of thousands of dollars per incident and collectively cost small businesses hundreds of thousands. Such thefts underscore how, even as digital payments rise, cash-dependent communities and free-standing ATMs remain vulnerable, creating a lucrative niche for low-tech criminals in urban areas.

Somewhat more subtle than stealing an entire ATM, card skimming remains widespread. Card skimming is a type of financial fraud where criminals steal payment card information, such as credit or debit card numbers, by capturing the data stored on the card's magnetic stripe. A recent case in Texas highlights the growing sophistication of skimming operations. Investigators uncovered a large-scale criminal network that installed "deep skimmers" inside fuel-pump card readers to steal payment data; these were often paired with hidden cameras to capture PINs. These deep skimmers are a type of card skimming device designed to be hidden inside the card reader slot, making them almost impossible to detect visually. The group not only skimmed cards but also manufactured devices and trained others, fueling a black-market scheme centered on card theft. Authorities estimate one suspect earned over $400,000 in a year using stolen data. Ten men now face felony charges for organized criminal activity and unlawful interception of electronic communications, underscoring how skimming has evolved into a highly organized scheme. Although this example uses fuel-pump card readers, deep skimmers can just as easily be placed in ATMs, with the remaining details of the story remaining unchanged.[21]

[19] Office of the Washington State Auditor, "Positive Pay can help protect your organization from check fraud," The Audit Connection Blog, June 30, 2017, sao.wa.gov/the-audit-connection-blog/2017/positive-pay-can-help-protect-your-organization-check-fraud.

[20] Darla Miles, "Reward offered in search of New York City bodega ATM robbery suspects," ABC7 *Eyewitness News*, January 9, 2025, abc7ny.com/post/nyc-bodega-robberies-5000-reward-offered-search-atm-robbery-suspects-targeting-small-businesses/15783327/.

[21] Marco Bitonel, "10 Charged After FCIC Uncovers Card Skimming Operation Across Texas," *Fox 7 Austin*, September 13, 2025, fox7austin.com/news/10-charged-after-fcic-uncovers-card-skimming-operation-across-texas; Carolyn Richardson, "Understanding Deep Insert ATM Skimmers: Detection and Prevention," *Medium*, August 6, 2024, medium.com/@financial-strategies/understanding-deep-insert-atm-skimmers-detection-and-prevention-4364b7c26c50.

The prevention recipe:

ATMs provide great convenience to customers but, as is often the case, convenience comes at a cost. Here are some prevention techniques to consider:

- **Upgrade ATM hardware.** This is likely the simplest and most obvious prevention technique, but make sure ATM hardware is up to date. For instance:
  - Ensure ATMs support Europay, Mastercard and Visa (EMV) chip cards, which are harder to clone than magnetic stripe cards.
  - Install jamming or detection devices inside card readers to prevent external skimmers from functioning.
  - Use card readers and keypads that make it difficult to attach overlays or hidden cameras.
- **Use emerging technologies.** Incorporate real-time monitoring, allowing for the detection of unusual transaction patterns and device-tampering alerts. Geo-blocking and velocity checks can also serve as good preventive measures. *Geo-blocking* refers to limiting transactions in unexpected locations, while *velocity checks* are more concerned with rapid withdrawals. When combined, these tools can be quite powerful in identifying potentially fraudulent activity. Lastly, consider incorporating biometric authentication into ATMs — using, for instance, a fingerprint or facial recognition for ATM access. This becomes even more powerful if used as a form of multifactor authentication, with the customer still using a PIN but also needing to be biometrically verified.
- **Customer education.** Customer education will surface as a common theme throughout the external fraud portion of this publication. It's important to remind customers of the risks of using an ATM as well as common red flags that they should look for (such as the presence of skimming devices) when using one. Also, customers should know whom to contact at the bank if they suspect an ATM has been tampered with.
- **Physical security measures.** The positioning of ATMs can dramatically affect a fraudster's ability and willingness to access it. Try to put ATMs in well-lit, high-traffic areas or inside bank branches to reduce tampering risk. Surveillance cameras should be installed around ATMs so that they allow for easy viewing of the ATM and surrounding area. Staff should routinely inspect the ATMs, looking for loose parts or evidence of tampering. If the ATMs are equipped with GPS tracking (highly recommended), test this feature periodically to ensure it can be accessed if needed.

Social engineering fraud

On the website for its Information Security Office, Carnegie Mellon University succinctly defines *social engineering* as "the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information."[22] Social engineering can lead to a criminal's access to a person's mobile banking and to identity theft, synthetic identify theft (a more complex form of fraud where criminals create a new, fictitious identity by combining real and fake information), and full-on account takeovers.

A notable recent example of social engineering fraud involved the digital wallets of a bank's customers. Fraudsters used persuasive tactics to trick cardholders into revealing sensitive information, including one-time passcodes. This allowed unauthorized access to accounts and enabled fraudulent transactions.[23]

Social engineering can take many forms:

- **Phishing** is a type of cyberattack where attackers impersonate a legitimate entity (such as a bank, company, or trusted person) to trick individuals into revealing sensitive information like passwords, credit card numbers, or personal details. This is usually done through emails, text messages, or fake websites (known as website "spoofing").
- **Spear phishing** is a more targeted form of phishing. Instead of sending mass emails to random people, attackers focus on a specific individual or organization. Attackers often use personalized details (like your name, job title, or company) to make the message appear credible and increase their odds of success.
- **Technical support scams** are a type of fraud where scammers impersonate legitimate tech support representatives — they usually claim to be from well-known companies like Microsoft, Apple, or antivirus providers — to trick individuals into believing their computer or device has a problem (such as viruses, malware, or performance issues). In this way, they persuade the target to grant the scammer remote access to their device to "fix" it, at which point they install malware.
- **Impersonation of bank staff** is just as it sounds: someone pretends to be a bank employee to deceive customers or other employees.

[22] "What is Social Engineering?" Carnegie Mellon University, accessed February 4, 2026, cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.

[23] "Case study: How One Bank Is Fighting Back Against Social Engineering," TSYS, July 22, 2025, tsys.com/insights/2025/07/22/how-one-bank-is-fighting-back-against-social-engineering

Although anybody can be susceptible to social engineering fraud, social engineering tactics tend to be deployed especially against senior citizens. The AICPA has written extensively on elder fraud, and we encourage you to refer to those publications.[24] Bank employees should be alert to elderly clients acting frightened, confused, secretive, or suddenly transacting large amounts to foreign locations.

Furthermore, the attacks are getting more sophisticated, especially with the use of AI. In July of last year, Sam Altman, OpenAI's CEO, voiced his concerns during a conference held at the Federal Reserve, where he stated that AI "has fully defeated most of the ways that people authenticate currently, other than passwords."[25] However, even passwords could soon prove useless with the onset of quantum computing, which is also thought to be potentially disastrous for blockchain technology.[26] Financial institutions are taking notice, with generative AI–enabled fraud losses in the United States projected to grow from $12.3 billion in 2023 to $40 billion by 2027.[27]

The phenomena Sam Altman referred to are called deepfakes — AI-generated replicas designed to mimic real individuals, whether it be through voice or video. In one of the most alarming cases of deepfake fraud to date, a multinational corporation was defrauded of $25.6 million after a finance employee was tricked into joining a video call with what appeared to be several senior colleagues, including the CFO. Unbeknownst to the employee, every participant on the call was a deepfake. Convinced by the realism of the interaction, the employee authorized a massive transfer of funds. The fraud was only uncovered after the transaction was verified with the actual head office.[28]

The prevention recipe:

- **Employee and customer training and awareness.** Employees and customers tend to be the weakest links when it comes to many fraud schemes, particularly social engineering attacks. Consider the following:
  - **Regular training sessions.** Teach staff to recognize phishing and other attempts. Include examples of real-world scams and evolving tactics like AI-generated emails (which often have fewer grammatical errors than human-generated emails).
  - **Simulated attacks.** Conduct periodic phishing and social engineering simulations to test readiness and identify vulnerable employees.
  - **Emphasis on critical thinking.** Encourage skepticism toward urgent or unusual requests, especially those involving financial transactions or credentials.
  - **Clear messaging.** Inform customers that the bank will never request passwords via email or phone.
  - **Fraud alerts.** Share examples of common scams (e.g., fake QR codes, spoofed websites) and provide guidance on safe practices.
- **Technical safeguards.** Consider the following:
  - **Email filtering and anti-phishing tools**. Deploy advanced filtering to block suspicious emails and links.
  - **Transaction verification.** Implement dual approval for high-value transfers and vendor-payment changes.
  - **Behavioral analytics.** Use fraud detection models to flag unusual patterns in account activity.
- **Deepfake prevention.** Consider combining multifactor authentication with the use of deepfake-detection technologies, which help detect whether a voice or video has been created with AI.

[24] *Elder Financial Abuse Trends*, FVS Eye on Fraud, February 28, 2017, aicpa-cima.com/resources/download/elder-financial-abuse-trends; *Investment Fraud Schemes Targeting Senior Citizens*, FVS Eye on Fraud, February 28, 2019, aicpa-cima.com/resources/download/investment-fraud-schemes-targeting-senior-citizens; *Medical and Insurance Fraud: A Prescription for Financial Loss*, FVS Eye on Fraud, August 19, 2021, aicpa-cima.com/resources/download/medical-and-insurance-fraud-fvs-eye-on-fraud; *Evolution of Elder Fraud in the Era of COVID-19*, FVS Eye on Fraud, September 30, 2023, aicpa-cima.com/resources/download/evolution-of-elder-fraud-in-the-era-of-covid-19-or-fvs-eye-on-fraud.

[25] Clare Duffy, "OpenAI CEO Sam Altman warns of an AI 'fraud crisis,'" CNN, July 22, 2025, cnn.com/2025/07/22/tech/openai-sam-altman-fraud-crisis.

[26] Skip Sanzeri, "The Password Era Is Over: What Comes Next In The Age Of AI And Quantum Threats," Forbes, Jul 23, 2025, forbes.com/councils/forbestechcouncil/2025/07/23/the-password-era-is-over-what-comes-next-in-the-age-of-ai-and-quantum-threats/; Bernard Marr, "Will Quantum Computing Kill Bitcoin?" Forbes, June 12, 2025, forbes.com/sites/bernardmarr/2025/06/12/will-quantum-computing-kill-bitcoin/.

[27] "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking," Deloitte, May 29, 2024, deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html.

[28] Dan Weckerly, "Deepfake Scam: $25 Million Fraud Highlights AI Banking Risks," Banking+, April 14, 2025, bankingplus.news/news/deepfake-bank-scam/.

Ransomware

In November 2023, a midsize U.S. bank fell victim to a sophisticated ransomware attack that disrupted its operations overnight.[29] Customers were locked out of their accounts, ATMs went offline, and internal systems displayed ransom demands. The attackers employed a double-extortion tactic, encrypting critical systems while stealing sensitive data, and threatened to leak confidential information unless a substantial Bitcoin payment was made within seven days. This incident highlights the growing complexity of ransomware in the banking sector. With ransomware attacks on financial institutions surging over 60% year-over-year in 2023, banks remain prime targets due to their high-value data and critical role in the economy. Some attackers have even started to employ triple-extortion tactics, which include encryption, data theft, and public outreach (regulators, journalists, or even the victim's clients).[30]

Not only is a ransomware attack or any cybersecurity incident traumatizing, but there are also stringent reporting requirements if a financial institution is subject to a cybersecurity incident. Under the Computer-Security Incident Notification Rule, banks regulated by the Office of the Comptroller of the Currency, Federal Reserve, or FDIC must notify their primary regulator as soon as possible and no later than 36 hours after determining that a significant computer-security incident has occurred. In accordance with the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, banks are also expected to notify affected customers as soon as possible.[31]

The prevention recipe:

- **Employee training.** Again, we come back to employee training. Because email remains a common ransomware entry point, conduct ongoing phishing-awareness programs.
- **Limit access.** Operate under the principle of least privilege, where user permissions are limited to only what is necessary for their role.
- **Network segmentation.** Separate critical systems from less sensitive networks to contain potential breaches and prevent lateral movement. As defined by Kurt Baker, "lateral movement refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets."[32]
- **System patches and updates.** Regularly apply security patches to operating systems, applications, and firmware to close known vulnerabilities.
- **Incident response planning.** Maintain a tested cyberattack (including ransomware) response plan that includes isolation procedures, law enforcement coordination, and communication protocols. Also, ensure that a sufficient backup strategy is in place and that backups are frequently tested.

Conclusion

Banking fraud continues to evolve, leveraging new technologies and exploiting both digital and human vulnerabilities. As this Eye on Fraud has shown, the convergence and enhancement of various fraud techniques present unprecedented challenges for financial institutions. However, history demonstrates that proactive governance, robust internal controls, and ongoing education — for employees and customers both — remain the most effective defenses. The financial services industry has often served as a role model for other industries when it comes to robust internal control environments. This is partly out of necessity, as financial institutions are entrusted with consumers' sensitive information. By adopting a layered approach to fraud prevention and staying vigilant against emerging threats, banks can protect their assets, reputation, and the trust of their customers. The fight against fraud is ongoing, but with the right strategies and a commitment to continuous improvement, financial institutions can stay one step ahead.

[29] Sean Lyngaas, "Brazen ransomware attack on US unit of Chinese banking giant has financial sector on alert," CNN, November 10, 2023, cnn.com/2023/11/10/tech/ransomware-attack-industrial-and-commercial-bank-of-china-financial-sector#:~:text=The%20hackers%20hit%20New%20York,US%20financial%20institution%20told%20CNN.

[30] Ankit Gupta, "Ransomware Attacks: The Evolving Extortion Threat to US Financial Institutions," CSO, August 4, 2025, csoonline.com/article/4032874/ransomware-attacks-the-evolving-extortion-threat-to-us-financial-institutions.html.

[31] "Computer-Security Incident Notification Final Rule," Financial Institution Letters, FDIC, November 18, 2021, fdic.gov/news/financial-institution-letters/2021/fil21074.html; "Information Technology (IT) and Cybersecurity," FDIC, fdic.gov/banker-resource-center/information-technology-it-and-cybersecurity.

[32] Kurt Baker, "Lateral Movement Explained," Crowdstrike, February 12, 2025, crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/.

aicpa-cima.com

2601-063458