Lisa Rosenfeld

Stonier Graduate School of Banking, Capstone Project

Submission date: March 2026

Title of Project: How Banks Can Help Detect and Prevent Authorized Push Payment Fraud

DISCLAIMERS

The views expressed in this article, and any references provided, are for informational purposes only and do not necessarily represent the views, official positions, endorsement, or guarantee of accuracy or reliability by the FDIC or the United States. Statements of fact, opinions, and views expressed are solely those of the author and do not represent official positions.

Contents

Executive Summary

What is Authorized Push Payment (APP) Fraud?

APP fraud is when bad actors trick customers, often using a scam or another type of social engineering, into instructing their financial institution to initiate payments from their accounts to the bad actors. Despite the common myth that only the elderly or gullible individuals become victims of APP fraud, anyone can become a victim. APP fraud is highly prevalent in the United States and throughout the world. APP fraud has significant negative impacts on victims, causing financial and psychological harm. It also harms banks and the overall financial system by undermining trust and reducing the amount of legitimate funds available. Additionally, APP fraud harms society since the proceeds are often used to fund illicit activities, such as human trafficking and terrorism. APP fraud is challenging for banks to combat due to the rapid pace of fraud evolution, the tendency for social engineering to make customers less communicative or honest with their bank, and the customer's role in making transactions.

How Can Banks Help Detect and Prevent APP Fraud?

Measures that banks can take to detect and prevent APP Fraud generally fall into three broad categories:

- Fostering a culture of APP Fraud risk management,
- Gathering, using, and sharing data effectively, and
- Engaging with customers.

Fostering a culture of APP Fraud risk management includes:

- Corporate support,
- APP fraud risk assessment and strategy, and
- Well-trained and engaged workforce.

Gathering, using, and sharing data effectively includes:

- Effective “know your customer” (KYC),
- Ongoing monitoring,
- APP Fraud Reporting,
- Using consistent and useful definitions,
- Avoiding data silos, and
- Leveraging information sharing with other institutions.

Engaging with customers includes:

- Customer education,
- Slowing down payments,
- Trusted contact, and
- Communicating with victims.

How Can Regulators Use This Research?

U.S. government agencies have been seeking ways to help mitigate payments fraud, including APP fraud. Regulatory agencies can use the research in this paper to educate financial institutions about how they can help prevent and detect APP fraud.

Introduction/ Problem Statement/ Hypothesis

APP fraud is a significant and increasing risk to the financial industry. Community banks in the U.S. can and should act to help combat APP fraud.

General Background

What is APP Fraud?

According to the Federal Reserve, each piece of the term “APP Fraud” can be defined separately as:

- Authorization: The explicit instructions, including timing, amount, payee, source of funds, and other conditions, given by the payer to the payee to transfer funds on a one-time or recurring basis.
- Push Payment: A payment made when the payer sends the payment instruction to the payer's account to transfer the payer's funds to the payee.
- Fraud: An action taken with dishonest intent to take something valuable from a payment system participant.

(The Federal Reserve)

Taken together, APP fraud is when bad actors trick victims, often using a scam or other type of social engineering, into instructing their financial institution to initiate payments from their accounts to the bad actors.

What Types of Scams are Associated with APP Fraud?

Bad actors use a variety of scams when conducting APP fraud. Many of these scams are relationship/trust scams, where the bad actor develops a relationship with the victim or pretends to be an authority or reputable entity. Some examples are:

- Romance Scam – In this type of scam, the bad actor uses a fictitious online identity to establish a trusted relationship with the victim. The bad actor requests money by using false situations to create a sense of urgency (Federal Reserve). According to the Federal Bureau of Investigation (FBI), Americans lost over $672 million to romance scams in 2024 (Internet Crime Complaint Center).
- Government Imposter Scam – In this type of scam, the bad actor poses as a government agency employee or member of law enforcement. The bad actor uses potential negative consequences like arrest, financial penalties, or reputational harm to convince the victim to make payments (Federal Reserve). According to the FBI, Americans lost over $405 million to government imposter scams in 2024 (Internet Crime Complaint Center).
- Investment Scam – In this type of scam, bad actors deceive victims into making purchases based on false information, usually by offering large returns with minimal risk (Internet Crime Complaint Center). According to the FBI, Americans lost over $6.5 billion to investment scams in 2024 (Internet Crime Complaint Center).

How is APP Fraud Different from Unauthorized Push Payment (UPP) Fraud?

In APP fraud, the victim makes the payment, while in UPP fraud, the bad actor makes the payment. When bad actors use scams with UPP fraud, they intend to trick a victim into giving the bad actors access to the victims' accounts, and the bad actors make payments using the victims' account (Toh).

Bank's controls are often designed for catching UPP fraud, but they may not be suitable for identifying APP fraud (Marek). For example, banks may flag potential UPP fraud if a transaction is initiated from an unfamiliar physical location or device; however, these flags are not present in APP fraud (TransUnion). Also, victims of UPP fraud are more likely to report the fraud to their bank than victims of APP fraud. According to a Pew Research Center poll, 74% of U.S. adults who lost money from an online scam or attack did not report the loss to law enforcement, including over half of the respondents who said that their finances were hurt a great deal or fair amount by the fraud (Gottfried, Park and Anderson). A victim of UPP fraud, when seeing an unfamiliar transaction in their account, may contact their financial institution, while a victim of APP fraud initiates the transaction and believes it is legitimate. Victims of APP fraud are also often coached by the bad actor to lie to the bank, so the bank may not get accurate information from the customer (Greenstein).

The U.S. legal system is more developed for addressing UPP fraud than APP fraud. Regulation E requires banks to reimburse customers when an unauthorized electronic funds transfer (EFT) occurs in their account, even if the customer is negligent (CFPB). However, it does not cover transactions that the customer authorizes. Victims of APP fraud often have little or no recourse, with no liability protection (Toh).

How Prevalent is APP Fraud?

While the exact level of APP fraud in the U.S. is difficult to measure and is underreported, it is highly prevalent in the U.S. While not all scams result in APP fraud, they can be a helpful proxy for estimating APP fraud prevalence. According to the Pew Research Center, 73% of U.S. adults have been the victim of an online scam or attack, with 21% losing money because of an online scam or attack (Gottfried, Park and Anderson). This study also found that 68% of U.S. adults receive scam phone calls at least weekly, and 61% receive scam text messages at least weekly (Gottfried, Park and Anderson). As seen in Figure 1 below, the FBI received thousands of scam complaints, corresponding to billions of dollars in losses in 2024.

Figure 1

Scam Type	**Age Under 20**	**Age 20 – 29**	**Age 30 – 39**	**Age 40 – 49**	**Age 50 - 59**	**Age 60+**
Confidence / Romance	Count: 272 Losses: $759 thousand	Count: 1,219 Losses: $11 million	Count: 1,814 Losses: $31 million	Count: 2,056 Losses: $46 million	Count: 2,365 Losses: $82 million	Count: 7,626 Losses: $389 million
Government Impersonation	Count: 161 Losses: $2 million	Count: 1,462 Losses: $34 million	Count: 1,894 Losses: $30 million	Count: 1,818 Losses: $21 million	Count: 1,711 Losses: $19 million	Count: 4,521 Losses: $208 million
Investment	Count: 399 Losses: $14 million	Count: 3,453 Losses: $154 million	Count: 6,822 Losses: $541 million	Count: 6,873 Losses: $616 million	Count: 5,797 Losses: $872 million	Count: 9,448 Losses: $1.8 billion

(Internet Crime Complaint Center)

APP fraud is becoming increasingly prevalent. Deloitte measured total APP fraud losses in the U.S. at $8.3 billion in 2024 and projects that APP fraud losses in the U.S. will reach between $12.4 billion and $18.2 billion by 2028 (Lalchand, Srinivas and Wadhwani). The increasing level of APP fraud follows a general trend of increasing fraud losses in the U.S. According to

data from the Federal Trade Commission (FTC), there have been more fraud losses via payment app/service, cryptocurrency, and bank transfer/payment in the first half of 2025 than there was in all of 2020, and fraud losses via wire transfer are on track to exceed 2020 numbers (Figure 2).

Figure 2

Fraud Payment Method	**Losses 2020**	**Losses 1st and 2nd Quarter 2025**
Payment App or Service	$87.3 million	$234.8 million
Wire Transfer	$312.4 million	$180.3 million
Cryptocurrency	$131.6 million	$939.1 million
Bank Transfer or Payment	$319.6 million	$1.2 billion

(Federal Trade Commission)

A significant reason for the increase in APP fraud is that it is becoming easier for bad actors to conduct increasingly sophisticated scams. Artificial intelligence (AI) and deepfake technology have made scams, especially impersonation scams, easier and faster to perpetrate (Chainalysis). Bad actors can purchase kits to assist in their crimes, so they do not need as much technical knowledge (Chainalysis). In addition, the vast amount of personal data available, whether shared voluntarily through social media (Rust) or stolen in data breaches (McDade), makes it easier for bad actors to specifically target vulnerable individuals. Technology has also made it easier for bad actors to receive funds from victims, as consumers are more familiar with making transactions online, and crypto ATMs make it easier for consumers to transact with digital assets (Rust)

Who are the Bad Actors in APP Fraud?

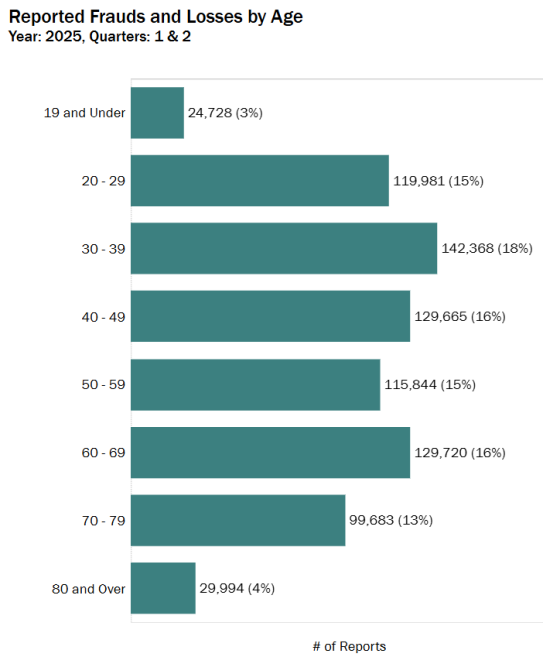
Bad actors in APP fraud can be domestic or foreign individuals or entities. While law enforcement has made arrests both within the U.S. (United States Attorney's Office Southern District of New York) and abroad (U.S. Department of the Treasury), foreign organized crime groups are increasingly involved in larger APP fraud schemes.

One prominent type of investment scam run by foreign organized crime is “pig butchering,” a virtual currency investment and relationship scam. It gets its name from the practice of bad actors “fattening up” victims before “slaughtering” them. In a typical pig butchering scam, the bad actor sends an initial message to the victim via texting, social media, or another communication platform under the guise of a wrong number or trying to reconnect with an old friend. After the victim responds, the bad actor communicates with the victim over time to build a relationship. Once the victim begins to trust the bad actor, the bad actor tells them about a supposedly lucrative virtual currency investment opportunity and introduces them to virtual currency websites that appear legitimate but are controlled by the bad actor. The bad actor encourages the victim to “invest” more money through these websites until the victim is unable or unwilling to pay more into the scam (Financial Crimes Enforcement Network). Usually, the individuals who are communicating with victims in pig butchering scams are victims of human trafficking. Organized crime organizations in Southeast Asia trick job seekers using authentic-looking job offers on constructed websites. Once these job seekers arrive, their passports are seized, and they are forced to live and work in compounds in violent conditions. (Rogin and Mufson).

Who are the Victims of APP Fraud?

Anyone can become a victim of APP fraud. While the elderly are the age group that lost the most money in aggregate to APP fraud and scams in 2024, the victims of APP Fraud can be any age (Internet Crime Complaint Center). According to a Deloitte survey, individuals born between 1997 and 2009 are more than twice as likely than those born between 1947 and 1965 to have a social media account hacked, fall for an online scam, have their identity stolen, or have a device hacked over the past year (Deloitte). FTC data show that, in the first half of 2025, the number of reported fraud losses is similar across ages between 20 and 79, with the most reports from individuals aged 30 to 39 (Figure 3).

Figure 3



(Federal Trade Commission)

While individuals of any age can become a victim of APP fraud, bad actors use different scams to target individuals of different age groups. Older individuals are more likely to be victims of investment, romance, or tech support scams, while younger individuals are more likely to be victims of employment scams, advance-fee credit scams, and online shopping fraud (Lalchand, Srinivas and Wadhwani).

What are the Impacts of APP Fraud?

APP fraud has negative impacts on victims, banks, the overall financial system, and society.

For the victim, there can be significant negative consequences beyond the direct monetary impact from losing assets. Victims lose time, with approximately 30% of victims spending more than 10 hours dealing with the consequences of APP fraud, including trying to recover funds, and 70% spending at least 1 hour (Board of Governors of the Federal Reserve System). Fraud can also cause lasting trauma for victims (Commonwealth Fraud Prevention Centre). Impacts can include psychological effects, reduced mental and physical health, harm to relationships, and changes in behavior (Low and Lally). Older adults who lose money may have limited opportunities to recover from financial loss, which can lead to a loss of independence (James, Boyle and Bennett). Additionally, victims could unknowingly be perpetrating a crime. Sometimes bad actors trick victims into acting as a money mule, meaning the victim is moving money through their account for the bad actor and helping them launder the money. Acting as a money mule is illegal and punishable, even if the individual does not know they are taking part in a crime (FBI).

When a bank customer becomes a victim of APP fraud, the bank may lose customer relationships as a result. One study found that 52% of victims stop engaging with emails and 42% keep less money in their accounts after being a victim of APP fraud (PYMNTS). Another study found that 31% of customers are more likely to leave a bank or credit union after a fraud event, even if the financial institution is not at fault (Luttrell). Additionally, when a customer is a victim of APP fraud, they are unknowingly funding illegal activities through the financial institution, which can have regulatory implications for the institution (Luttrell).

APP fraud is detrimental to a safe, accessible, and efficient financial system. It has the potential to undermine trust in the payments systems that the financial system depends upon (Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation). APP fraud can also harm local economies through its impact on small businesses and community groups. For example, the CEO of Heartland Tri-State Bank, a small community bank in Kansas, fell victim to a pig butchering scheme and sent funds from the bank and community organizations to the bad actor as part of the scheme. The $47.1 million in bank funds that he sent via wire transfers resulted in the bank entering receivership in 2023 (Office of Inspector General).

There are also larger societal impacts from APP fraud. The proceeds from fraud support the illicit activities of criminal organizations, including human trafficking and terrorist activities (Ryder). For example, the terrorist organization Isis has used romance scams to fund its activities (Flanagan).

How is APP Fraud Evolving?

APP fraud is constantly evolving. Technological advances have made it easier for bad actors to conduct increasingly convincing scams. Some technologies that bad actors can leverage include:

- AI – Bad actors can use deepfakes, image and text generation, and automation to easily create more convincing fake identities and documents (Wilder).
- Caller ID Spoofing – Bad actors cans manipulate the information transmitted to potential victims' caller IDs to display fake numbers or identities (Toh).
- Encrypted and Anonymous Messaging Platforms – Messaging platforms, such as Telegram, provide bad actors with encryption and anonymity and allow bad actors to use group-based fraud tactics (Corrons).
- Digital Assets – Transnational organized criminals can use digital asset service providers in jurisdictions with weak anti-money laundering standards to launder and cash out their illicit proceeds (United States Secret Service).
- Fast/Real Time Payments – The speed and irrevocable nature of transactions in most fast and real time payment systems makes these systems attractive to bad actors (Toh).

Hypothesis

Banks are critical in the fight against APP fraud. While a single bank cannot eradicate APP fraud on its own, each bank can act to reduce the impact of APP fraud through detection and prevention measures. These measures fall into three broad categories:

- Fostering a culture of APP Fraud risk management,
- Gathering, using, and sharing data effectively, and
- Engaging with customers.

Expected Discoveries and Potential Benefits and Impacts

This paper will identify best practices for U.S. banks in detecting and preventing APP fraud. While there is a significant body of research on APP fraud, the information is dispersed, and there is no easily accessible resource for U.S. banks that consolidates the information. Additionally, as APP fraud and methods to combat APP fraud are constantly evolving, attempts to consolidate this information become outdated quickly. Given the time and resource constraints that regulators and bankers face, this paper is intended to become a resource for examiners and bankers by presenting actionable steps that financial institutions can take to improve APP fraud detection and prevention processes.

If institutions implement the recommendations in this paper, they could develop more robust and efficient APP fraud detection and prevention programs, leading to a decline in the levels of fraud losses. Reduced levels of fraud would improve customer wellbeing, increase funds

and trust in banks and the payments system, and reduce funding to criminal and terrorist organizations.

Future Opportunities

APP fraud is constantly evolving. When financial institutions, as an industry, implement stronger controls, bad actors innovate to evade those controls or discover alternative methods to perpetrate fraud. In response, financial institutions develop new methods to detect and prevent the bad actor's methods, and the cycle continues. Due to the constant evolution, there are consistently opportunities for expanded research into new fraud and anti-fraud techniques.

Additionally, individual banks are just one type of entity fighting against APP fraud. There are opportunities for expanded research into how other entities can prevent and detect APP fraud in concert with banks, including:

- Governments and regulators,
- Banking industry groups,
- Other industries that are impacted by APP fraud, such as telecommunications and social media companies, and
- Charitable organizations and other groups that support vulnerable populations.

Research Methodology – Data Sources & Analysis

The research in this paper relies on published sources and secondary data. These sources include industry white papers and other publications, government research and advisories, and academic research.

Research is limited by the inability to gather non-public bank data about APP fraud. Further, suspicious activity reports (SARs) are confidential and are not available for public research and analysis.

Research methodologies consist of using publicly available publications from reputable sources to develop a list of best practices, challenges in implementing the best practices, and ways to implement the best practices more effectively based on common recommendations.

Findings and Conclusions

There are numerous measures that banks can take to help detect and prevent APP fraud. These actions generally fall into three broad categories:

- Fostering a culture of APP Fraud risk management,
- Gathering, using, and sharing data effectively, and
- Engaging with customers.

Fostering a Culture of APP Fraud Risk Management

As discussed below, fostering a culture of APP Fraud risk management includes:

- Corporate support,
- APP fraud risk assessment and strategy, and
- Well-trained and engaged workforce.

Corporate Support

What is it?

The board of directors and management team set the bank's cultural environment and corporate values (CFI Team). A corporate culture that values and rewards APP fraud prevention can make anti-APP fraud efforts more effective. Efforts to develop and maintain a culture of APP fraud prevention could include making fraud prevention part of the bank's brand; highlighting when employees protect customers from APP fraud; devoting time and

resources to APP fraud prevention efforts, such as quality employee training; and establishing metrics for employee success (Federal Trade Commission).

What Implementation Challenges do Banks Face?

Getting board or management buy-in can be challenging, especially because quantifying the impact of APP fraud to an institution is difficult. In the U.S., financial institutions are not required to reimburse victims of APP fraud or report losses that don't meet SAR reporting requirements. Customers may not report APP fraud to their financial institution due to embarrassment or a belief that there is no benefit to reporting. These challenges can make it difficult to help directors and executives understand the scale of the concern with APP fraud and how it impacts their financial institution. (The Knoble)

How Can Banks Respond to These Challenges?

To make a business case for combatting APP fraud, bankers can use the data they have available to estimate the cost of APP fraud. Some data that may be available include:

- Current and proposed operational costs for identifying, investigating, and reporting APP fraud.
- The attrition rate among APP fraud victims and the resulting deposit loss value or acquisition cost to replace the customer.
- Amount that the bank has voluntarily reimbursed for APP fraud.
- Any legal costs associated with cases that resulted in litigation, settlements, or fines.

(The Knoble)

To make the business case stronger, bankers can work with the marketing department to advertise their bank's anti-APP fraud practices. A 2025 study found that 97% of consumers say that fraud prevention and security are very or somewhat important when choosing where to bank (Alloy). For these consumers, strong anti-APP fraud practices can be a competitive advantage that can be marketed to potential and existing customers. For example, Santander Bank has widely publicized its Break the Spell Team, a team within the bank that is focused on helping APP fraud victims realize that they are victims of a scam (Ainsley and Pilsworth). In another example, a group of small banks in Missouri were able to take out a large, discounted ad in the local newspaper to educate the public about APP fraud and how to identify and avoid scams (Robb).

APP Fraud Risk Assessment and Strategy

What is it?

A risk assessment helps bank management and boards of directors identify where risks lie in an institution. As part of the process of creating and updating risk assessments, the board and management determine the risk profile of the institution and identify the risk appetite. The risk assessment can be a tool to focus resources where they are needed most by helping the bank conduct risk-based monitoring and measure outcomes. (Thackeray)

A written strategy is based on the risk assessment and outlines the approach to APP fraud prevention, detection, disruption, and response. The strategy should be specific to APP fraud rather than addressing fraud in general, as APP fraud requires different prevention strategies than other types of fraud (America's Credit Unions).

What Implementation Challenges do Banks Face?

One challenge banks face is the rapid rate of change in APP fraud methods, which can make risk assessments and strategies become outdated. Bad actors adapt quickly and target developments in technologies and markets (The Treasury).

Another challenge is implementation of the risk assessment. If there is a lack of management buy-in, or if there are not adequate methods of measuring compliance, risk assessments and strategy documents may be ignored or not used properly.

How Can Banks Respond to These Challenges?

Banks should develop flexible frameworks that can quickly respond to changes in APP fraud practices (The Treasury). Banks should regularly review the effectiveness of the strategy against the risk assessment (The Treasury). Some entities recommend a review at least annually (BioCatch).

Additionally, the risk assessment and strategy documents should get high-level sign-off within the business from the board or similar level of governance. The board and management should make it clear that there is a high level of priority and oversight. Additionally, there

should be ongoing monitoring and reporting to senior levels, to ensure the strategy is being effectively implemented. (The Treasury)

Well-Trained and Engaged Workforce

What is it?

A well-trained and engaged workforce has:

- Position-based training,
- Clear procedures and reporting lines to support staff that identify potential APP fraud and ensure that the proper personnel get involved,
- Employee empowerment to act when APP fraud is suspected, and
- Incentives that align with the bank's anti-APP fraud strategy.

In a well-trained and engaged workforce, all bank staff are knowledgeable about APP fraud, especially customer-facing staff and individuals who are responsible for fraud prevention. Employees know how to identify APP fraud, report and act when they identify potential APP fraud, and feel empowered to do so, even if there is a chance they are mistaken (Regions Bank).

What Implementation Challenges do Banks Face?

Banks face various challenges when training employees. Employees may not be engaged during the training, especially when communication is unclear or lacks interaction. The

workforce may be geographically dispersed and have a variety of backgrounds and ages, with a variety of communication style preferences. Staff may have time constraints due to other obligations. Additionally, tracking and measuring training effectiveness can be difficult. (TriNet)

Setting up clear procedures, processes, and reporting lines is time consuming, and documents may become out of date as changes occur at the bank or in the fraud or banking environment. Additionally, these measures may be less effective without support from the Board and management and ways to measure compliance.

Incentives, such as bonuses, may be focused on priorities that conflict with anti-APP fraud strategies. For example, if incentives are based on unrealistic sales goals, employees may prioritize opening accounts, even if opening the account would harm the customer (CFPB).

How Can Banks Respond to These Challenges?

To mitigate training challenges, banks should ensure that training is clear and engaging. If the workforce is comprised of individuals of different generations, geographic locations, or backgrounds, multiple formats of training may be necessary, including virtual training. Micro-courses and training bursts that are short but frequent can be effective for employees with limited time. As part of training development, banks should determine which metrics are most relevant for the APP fraud prevention and detection process. Banks should use these metrics to gauge whether the training is effective or if changes or further training are necessary. Training should be designed to meet the needs of each job category. (TriNet)

Management should regularly revisit procedures, processes, and reporting lines to ensure they are meeting the bank's needs. Management should develop clear ways to ensure they are implemented properly.

When designing incentives, such as bonuses, management and the board should consider the APP fraud strategy and reward anti-fraud behavior. Incentives should be based on realistic goals.

Gathering, Using, and Sharing Data Effectively

As discussed below, gathering, using, and sharing data effectively includes:

- Effective "know your customer" (KYC),
- Ongoing monitoring,
- APP Fraud Reporting,
- Using consistent and useful definitions,
- Avoiding data silos, and
- Leveraging information sharing with other institutions.

Effective KYC

What is it?

KYC is a catchall term used to refer to the process of understanding the identity and characteristics of a customer and the nature and purpose of a customer relationship (Gentenaar, Rowland and Davidson). KYC includes regulatory requirements, such as customer

identification program and customer due diligence requirements, and additional processes that institutions implement to better understand their customers. Some information is gathered at account opening, such as name, date of birth, social security number, physical address, and intended use of the account. Other information is gathered as the customer uses the account, such as account usage patterns. When bankers have a clear idea of who their customers are and what type of activity is normal for each customer, they are better able to identify when activity is abnormal or potentially fraudulent and to tailor their communications with customers. They are also better able to allocate resources to customers who are at higher risk (Ibitola).

What Implementation Challenges do Banks Face?

Challenges for KYC include:

- Friction: Initial KYC can introduce friction into opening accounts. Institutions may be hesitant to collect enough information at account opening to fully understand the customer's fraud risk profile to avoid causing the customer annoyance during the account opening process.
- Data silos and quality: Some institutions gather KYC information to meet anti-money laundering (AML)/countering the financing of terrorism (CFT) regulatory requirements without consideration for gathering enough information to capture the full APP fraud risk profile of a customer. Additionally, the information may not be fully available to anti-fraud employees.

(FinScan)

How Can Banks Respond to These Challenges?

Banks can lessen the friction from KYC by leveraging external resources and recognizing that KYC is an ongoing process. While some information must be gathered from the customer at account opening, other information can be gathered from other sources, such as credit reports, or during the life of the account with little or no impact on the customer's experience. Throughout the life of the account, banks can use transaction data and behavioral biometrics to determine what types of activity are usual for the customer.

Individuals with knowledge of APP fraud can help shape KYC practices at the institution. There should be processes for communication between AML/CFT and anti-fraud staff, whether they are informal conversations at less complex institutions or formal information flow processes at more complex institutions. The section below on avoiding silos has additional suggestions for improving systems, data quality, and data availability.

<u>Ongoing Monitoring</u>

What is it?

At many institutions, ongoing monitoring focuses on transaction monitoring. Transaction monitoring can be performed in multiple ways. Smaller, less complex banks may be able to rely on manual processes, such as reviewing system reports and speaking with customers and

customer-facing employees. Larger, more complex institutions generally use more automated solutions, such as transaction monitoring software, to help monitor transactions.

What Implementation Challenges do Banks Face?

Challenges for transaction monitoring include:

- Cost: Monitoring systems can be costly in terms of money, time, and other resources.
- Talent: To use monitoring systems properly, banks need individuals who can effectively implement and understand the systems.
- Poor data quality/lack of integration: Transaction monitoring models rely on quality data to determine if activity is potentially suspicious or indicates potential fraud. Organizational or system silos can prevent these models from having all the access to the data they need (Arora, Hui and Leong). Additionally, other technical or training issues can cause data within internal systems to be incomplete, inaccurate, or in an unusable format.
- Poor KYC: KYC helps banks understand what activity should be expected for a customer. Without effective KYC, ongoing monitoring may not identify activity as potentially suspicious or fraudulent.
- Evolution of APP fraud: APP fraud techniques and typologies are constantly evolving, which may change the transaction or behavioral patterns that monitoring systems and employees need to look for.

How Can Banks Respond to These Challenges?

More sophisticated banks can leverage machine learning and AI in transaction monitoring. Machine learning may be faster to adapt to changing fraud tactics and be able to identify suspicious patterns that would not be identified by traditional transaction monitoring (Armstrong). It can also allow for real time analysis and alerts, alerting the bank and the customer to potentially fraudulent activity as it is occurring (Fraud.com). Some considerations when selecting a machine learning system include accuracy, flexibility, speed, explainability, cost, scalability, and integration (Harris)

Banks may also monitor accounts using behavioral biometrics, which monitors customers' behavior when using digital banking tools on banks' websites or mobile apps. Customers' behaviors change when they have strong emotions or are under the influence of another person. For example, a customer who is receiving instructions from a bad actor over the phone may have a more segmented typing pattern and have more mouse "doodling" (random mouse movement) (BioCatch). Banks may also be able to use banking apps to determine if the customer has an active phone call while performing a transaction, which may also be indicative of a scam situation if it is a longer inbound call (Palla, ZELLE FRAUD: Top Ten Controls Banks Can Deploy Today to Protect Consumers).

While smaller or less sophisticated financial institutions may not have the resources to implement machine learning or behavioral biometrics, they often have the advantage of a lower risk profile and more personal interactions with customers. Well-trained and

empowered front line staff can help mitigate shortfalls in transaction monitoring in a smaller, less digital institution.

APP Fraud Reporting

What is it?

Clear and user-friendly fraud reporting methods are a useful tool for gathering information about APP fraud. Reporting can be from internal or external parties.

Internal reporting methods involve bank employees reporting when they suspect a customer may be a victim of APP fraud. Effective internal reporting allows the appropriate personnel to be involved and data to be more centralized, with information bypassing the silos that employees generally work in.

External reporting methods involve customers contacting their bank when they believe they are a victim of APP fraud. Some banks have established methods, such as designated phone numbers and email addresses, for customers to report suspected fraud (Bank of America). Easy and accessible reporting methods make customers more likely to report fraud to their bank, which improves the quality of banks' APP fraud data.

What Implementation Challenges do Banks Face?

For internal reporting, employees may not feel empowered to report potential APP fraud, especially if they are not completely sure that the customer is a victim of APP fraud (Regions

Bank). Additionally, employees may not have the incentive to report or may not know how to report potential fraud.

For external reporting, victims may face psychological and practical barriers to reporting APP fraud. Victims may be reluctant to report due to shame, stigma, or fear of retaliation (Houtti, Roy and Gangula). Also, they may not report APP fraud if they feel that the fraud is not important enough to report or if they believe that reporting will not achieve anything (Harvey, Kerr and Keeble). Victims may find it difficult to trust others, even their bank, after being a victim of APP fraud (Harvey, Kerr and Keeble). Practically, victims may not report due to not knowing how to report the APP fraud or due to the time and effort involved in reporting (LaFleur). According to a 2025 study, 63% of consumers reported to their financial institution after being targeted by a scam (Alloy).

How Can Banks Respond to These Challenges?

Training, corporate support, and employee empowerment can make employees feel more comfortable reporting potential APP fraud. Additionally, clear procedures make it easier for employees to understand what reporting methods are available and how and when to use them.

Banks can help victims overcome psychological and practical barriers by:

- Making the reporting process as simple and streamlined as possible, with multiple reporting channels to meet the needs of customers with different needs (LaFleur).

- Using customer education to help customers understand how to report in case of fraud and promoting anonymized success stories where customers reported fraud and had positive outcomes (LaFleur).
- Trying to make victims feel like their case is being taken seriously and recognizing that the victim was the victim of a crime (Harvey, Kerr and Keeble).
- Using behavioral nudges, such as pop-ups with reporting instructions, when APP fraud is suspected (LaFleur).

Using Consistent and Useful Definitions

What is it?

APP fraud and the scams associated with it do not have consistent terminology across the financial industry. For example, some sources refer to APP fraud as "APP scams" or just "scams." Similarly, "pig butchering" scams are called by a variety of names, including "romance baiting," "financial grooming," and "hybrid romance-investment scam." Financial institutions may also use a variety of terms to refer to APP fraud or specific scams internally. Lack of consistent terminology can lead to inconsistent metrics (Segner). When financial institutions use consistent definitions throughout the organization, it is easier to collect data, develop useful metrics, and communicate and share information across different functions within the organization (Woolley).

What Implementation Challenges do Banks Face?

Defining APP fraud and scams can be challenging because APP fraud typologies are constantly evolving. Definitions that are too rigid or prescriptive may frequently become out of date. Additionally, ensuring that all departments within an organization use the same terminology involves a coordinated effort, which can be difficult if there is a lack of support from within the organization.

How Can Banks Respond to These Challenges?

One way that financial institutions can quickly develop consistent and useful definitions or taxonomies for APP fraud is leveraging existing models, such as the Scam Classifier and Fraud Classifier models promoted by the Federal Reserve. The Scam Classifier model involves a four-step process:

1. Determining if the incident meets the definition of a scam (the use of deception or manipulation intended to achieve financial gain),
2. Determining whether an authorized party was tricked into making the payment (APP fraud) or the authorized party was tricked into giving the bad actor access to the account (UPP fraud),
3. Determining how the authorized party was deceived or manipulated, and
4. Classifying the scam type based on the type of deception (Federal Reserve).

This model provides flexibility by not relying on the communication method, payment application or payment type to classify a scam (Federal Reserve).

Avoiding Silos

What is it?

Silos occur when parts of an organization do not share information with other parts effectively. Sometimes the silos are the result of organizations using a “divide and conquer” mentality where processes are optimized without regard for how they impact other processes (Ribeiro, Giacoman and Trantham). Data may be stored in different systems or formats across various departments, making it difficult to create a unified view of the risks and patterns within the customer base (FinScan).

What Implementation Challenges do Banks Face?

Different areas within the bank may have different priorities and needs that make removing silos impractical (Ribeiro, Giacoman and Trantham). There may be a lack of technology platforms that work well with all the systems that a bank needs to work together (McHugh). It can also be expensive to move systems, as integrating new data, services, or signals into a system can be costly (Leyva, Katkov and Perez).

Sometimes confidentiality concerns present barriers. Some information is confidential and should only be shared on an as-needed basis (Leyva, Katkov and Perez). There may also be regulations limiting sharing certain information. For example, if a bank has its transaction monitoring team outside the U.S., certain information, such as SAR filings, may not be shared with this offshore team (Financial Crimes Enforcement Network).

How Can Banks Respond to These Challenges?

Banks should encourage a culture of sharing and focus on technology with the right data capabilities (McHugh). Some banks have begun combining AML/CFT, anti-fraud, and cyber units into unified anti-financial crime units to facilitate sharing data and other information between personnel (PWC Canada).

For information confidentiality, banks should consider whether there is a way to separate confidential information from information that can be shared. For example, while disclosure of a SAR outside the U.S. is prohibited, the bank can still share underlying facts, transactions, and documents upon which a SAR is based (Financial Crimes Enforcement Network).

<u>External Information Sharing</u>

What is it?

Bad actors often use the same tactics across different financial institutions and payment types. Sharing information allows banks to learn from other financial institutions' experiences to improve their own anti-APP fraud processes. Banks can share information about the general types, typologies, and prevalence of APP fraud their customers are experiencing, and best practices for combating APP fraud. Banks that participate in information sharing under Section 314(b) of the USA PATRIOT Act have a safe harbor to voluntarily share information with other participants about individuals, entities, organizations, and countries for the

purpose of identifying and reporting money laundering and terrorist activities (Financial Crime Enforcement Network).

The benefits of sharing information include:

- Improving countermeasures and controls,
- Better APP fraud prevention,
- Better understanding of the level and types of APP fraud,
- Identification of mule accounts that bad actors use to move money.

(Federal Reserve)

What Implementation Challenges do Banks Face?

In the U.S., APP fraud information sharing is fragmented, with no single forum for sharing information (Federal Reserve). Even when there are registries to connect banks, such as the Nacha registry, the contact information on the registries may only include general customer service lines that do not lead directly to anti-fraud personnel (Marek). Additionally, when banks do not participate in information sharing under Section 314(b) of the USA PATRIOT Act, there are substantial legal limits on the customer information that can be shared.

How Can Banks Respond to These Challenges?

Banks should report scams to appropriate authorities when applicable and encourage victims to report as well. This information will improve law enforcement and industry knowledge

about scams. There are several government organizations that collect data and share aggregated data with the public, including FinCEN, FTC, and the Financial Services – Information Sharing and Analysis Center (FS-ISAC) (Information Sharing Working Group). There are also industry organizations that facilitate information sharing, such as the American Bankers Association (ABA) (American Bankers Association) and Nacha (Nacha). When possible, banks should put direct lines in these registries to make contact easier (Marek).

Banks should consider participating in information sharing under Section 314(b) of the USA PATRIOT Act. Section 314(b) allows banks to voluntarily share information with other institutions participating in Section 314(b) that would assist in identifying money laundering or terrorist activities (FFIEC). Institutions have used Section 314(b) to get information to help validate information and activities and identify fraud (FinCEN's Office of Special Programs Development).

Engaging with Customers

As discussed below, engaging with customers includes:

- Customer education
- Slowing down payments
- Allowing customers to name a trusted contact
- Communicating with victims,
- Combating bank imposter scams.

Customer Education

What is it?

Customer education can take many forms. Banks can provide anti-fraud education via their websites and mobile apps, social media, emails to customers, pamphlets available in person or by mail, awareness events, messages on ATMs, conversations between bank personnel and customers, and any other way that customers interact with the banks (Financial Conduct Authority). The content of the education generally helps customers understand what fraud is, how to identify fraud, how to report fraud, and what to expect from the institution once they report fraud (Financial Conduct Authority).

One innovative example of this control is Starling Bank in the United Kingdom. Starling Bank implemented a new tool in their app that allows customers to upload images of items, ads, and other communication from online marketplaces before making a transaction. The tool uses AI to identify and educate customers about potential signs of fraud in the uploaded images (Starling Bank).

What Implementation Challenges do Banks Face?

There are numerous challenges that banks need to overcome to implement effective customer education. Due to optimism biases and stereotypes of fraud victims, people often think they are less likely to become fraud victims than other people (Scam Prevention

Research Committee). As a result, customers often ignore education campaigns (U.S. Government Accountability Office).

Even if customers pay attention to fraud education campaigns, they may not remember what they have learned when faced with a real fraud situation. In studies, participants only retained information from training for two weeks to six months, depending on the study. Bad actors also frequently try to create a heightened emotional state in their victims, which can disrupt victims' ability to remember prior education and warnings. (Scam Prevention Research Committee)

Additionally, even if customers retain what they learn from fraud education campaigns, the information they learn may become outdated as APP fraud schemes change. The pace of change in APP fraud schemes is accelerating, and bad actors are increasingly using AI to perpetrate APP fraud (NICE Actimize).

How Can Banks Respond to These Challenges?

Education campaigns should seek to reduce customers' perceptions that they are less likely to become fraud victims. Messaging should avoid fraud victim stereotypes and should not imply that victims are unintelligent, uneducated, naïve, or gullible. Giving customers personal experience with scams by simulating the experience of being scammed (such as using fake scam emails) or giving second-hand experience through messaging with vivid stories of people's experiences with scams may also help (Scam Prevention Research Committee). Additionally, messaging should not just focus on one age group. While there is a popular

perception that fraud victims are typically elderly, younger adults are also highly susceptible to fraud due to overconfidence in technological skills, high social media exposure, and high levels of data sharing online (A+ Federal Credit Union).

There are various ways to make training more memorable. Messages are more memorable when they are easy to understand, are well organized and clear, have exciting and vivid details, and provoke thought and emotion (Schraw, Bruning and Svoboda). Trainings are also easier to remember when they use visuals, use concrete language that evokes a mental image, or are interactive, which makes it easier for the customer to visualize themselves taking the steps that the training is trying to convey (Scam Prevention Research Committee).

Training should be actionable. It should be clear what actions individuals should take to reduce their risk and what the potential benefits of action or consequences of inaction would be (Scam Prevention Research Committee). One way to make education more actionable is putting interactive training messages immediately before or during a transaction, so the customer can immediately put their learning to use (Palla, ZELLE FRAUD: Top Ten Controls Banks Can Deploy Today to Protect Consumers).

Consumer education should evolve as scams evolve to ensure information is current and accurate (Low and Lally). For bankers with limited time to create and update consumer education messages and training, there are numerous external resources that can be leveraged. Some organizations that offer free customer training resources to banks include the ABA (Safe Banking for Seniors | American Bankers Association), AARP (AARP BankSafe:

Protection Against Financial Exploitation), the Customer Financial Protection Bureau (CFPB) (Resources for Financial Practitioners, Educators & Professionals | Consumer Financial Protection Bureau), the FDIC (Money Smart | FDIC.gov), and Nacha (Consumer Financial Exploitation Project Team | Nacha).

Other steps for making consumer education more effective include seeking feedback on training materials and making improvements based on the feedback, partnering with organizations or trusted individuals within the community to increase the reach of education campaigns, and considering the learning style, native language, age, and culture of the target audience (Federal Trade Commission). One study found that marketing-inspired call-to-action messaging was more effective than messaging that relied on loss aversion or fear appeals (Akesson, Gathergood and Quispe-Torreblanca).

Slowing Down Payments

What is it?

As of January 2025, about half of U.S. states have laws allowing banks to hold or deny suspicious transactions involving older customers and/or other vulnerable individuals (ABA Foundation). However, there are many ways banks can slow down payments without needing to hold or deny payments. They can institute transaction size limits and daily transfer limits, require a waiting period before using a new payment method (such as Zelle), or delay all or specific transactions, such as transactions that present red flags or that are intended for a new payee (Palla, Faster Payments: Is Adding Sand in the Gears Necessary?). Additionally, a

bank can force customers to acknowledge pop-ups or answer questions about the payment before the customer can make the transaction. (U.S. Government Accountability Office). These methods can also be used for instant payments, since these payments only have to be instant once the payment instruction has been issued (Tapling, The power of a pause: Can a small delay prevent big fraud losses?).

Use of fast payments and real time payments has increased, with one survey finding that 91% of consumers have sent a real time payment in 2024 (Cobb). As use of these services increases, the time banks have to intervene in a potentially fraudulent transaction has shortened. Additionally, bad actors frequently create a false sense of urgency when perpetrating scams to make the victim act more quickly and have less time to think about the validity of the requests (Tapling, Authority, Urgency, Action: The Financial Scammer's Recipe). The purpose of slowing down payments is to give customers more time to think before sending funds and banks more time to detect and potentially prevent payments to bad actors.

One example of a bank using this control is Santander's dynamic fraud warnings. Santander introduced a dynamic fraud warning on mobile and online banking that asked customers a series of tailored questions when they purchased items on Facebook Marketplace. Between December 2023 and May 2024, 439 customers (less than one percent of customers who attempted to use a bank transfer to purchase an item through Facebook Marketplace) reported falling victim to a scam, with 1,889 customers not proceeding with their transaction after receiving the warning. (Santander)

What Implementation Challenges do Banks Face?

Slower payments or friction in the payment process may cause customer dissatisfaction. When making legitimate payments is more difficult, banks can experience reduced customer satisfaction, lower customer loyalty, and increased churn rate (Kuhrt). Forty-five percent of banks that responded to a 2025 survey said that customers have a negative reaction to a delayed disbursement, transaction refusal, or hold on their account (ABA Foundation). In a 2024 Federal Reserve study, customers using instant payments were found to be 8% more satisfied with their financial institution, and slow speed of funds was the second-most reported consumer payment challenge (Federal Reserve).

Another challenge is that bank's efforts to make customers stop and think may not work consistently. Customers become habituated to warnings, meaning they pay less attention to warning labels and pop ups over time (Scam Prevention Research Committee).

How Can Banks Respond to These Challenges?

To avoid customer dissatisfaction, banks can strengthen customers' trust and knowledge about why the bank is slowing down payments, so that customers realize that the bank is acting in their best interests (ABA Foundation). Many consumers will accept more friction in payments if there is trust and adequate information (FICO). Additionally, banks can give customers the option to slow down payments themselves, such as including an in-app "freeze switch" that customers can use to pause payments when they realize that they may be a victim of fraud (The Treasury).

To combat habituation, banks can vary warning messages and make them more interactive and less generic. Studies show that warning messages that change in format, color, and design may be more resistant to habituation (Scam Prevention Research Committee). Another study found that warnings that interrupt a task and require the user to make a decision are more effective than passive dialogue box warnings (Egelman, Cranor and Hong). Increasing the font size may also make warnings more effective (Ebert, Ackermann and Bearth). Additionally, a study found that people are more likely to pay attention to warnings that appear specific to the individual and are less generic (Wen, Wu and Wang).

Trusted Contact

What is it?

When customers name trusted contacts, they provide consent for the financial institution to contact specific individuals if there is concern that the customers may be at risk of financial exploitation (CFPB). Generally, when contacting a trusted contact, the bank will only disclose that there is reason to suspect that the customer may be a victim of financial exploitation and will not disclose any confidential personal or financial information (State of Wisconsin). While use of trusted contacts is a more recent development for banks, brokerage firms have been required to ask retail customers to name trusted contacts since 2018 (Office of Investor Education and Advocacy).

What Implementation Challenges do Banks Face?

Banks' abilities to implement a trusted contact procedure may be limited by the laws of the jurisdictions they operate in. Based on the states that banks operate in, they may have restrictions on when they are legally allowed to share information about an older or vulnerable account holder, who they can share information with, and how much they can share (CFPB).

This control is reliant on voluntary customer participation. As with customer education, people often think they are less likely to become fraud victims than other people due to optimism biases and stereotypes (Scam Prevention Research Committee).

If not handled well, conversations about trusted contacts can cause conflicts with customers. Customers could perceive bankers' suggestions to name trusted contacts as violating their privacy or questioning their competency (Place).

Sometimes the trusted contact is the one exploiting the customer. However, when this situation occurs, having the bad actor named as a trusted contact can make it easier to identify who the bad actor is (Place).

How Can Banks Respond to These Challenges?

Banks should establish clear written procedures regarding trusted contacts to ensure that the control is used properly. These procedures should discuss the process of offering customers the opportunity to consent to sharing information with a trusted contact, circumstances in which trusted contacts will be contacted, and information that can be shared with trusted

contacts (CFPB). Banks should also provide training for personnel who will be communicating with customers about naming a trusted contact. This training should include how to communicate with the customer, such as focusing on the skill of bad actors rather than the vulnerability of the customer when talking to customers about naming a trusted contact (Place).

Banks should develop customer consent forms written in plain language. These forms should address:

- When the bank may communicate with trusted contacts,
- A statement that, notwithstanding the consumer's consent, the financial institution will not disclose nonpublic personal information to a designated third party if the financial institution reasonably believes that the third party has engaged in, is engaging in, or will engage in financial exploitation of the consumer,
- An acknowledgment that the consumer has a right to revoke the consent and/or execute new consent naming a different trusted third party.

(CFPB)

Bankers should not assume that older customers will be more open to naming a trusted contact than other customers. A study of key determinants for naming a trusted contact for U.S. brokerage accounts found that investors aged 65 or older were less likely to name a trusted contact than those aged 18 to 34 (Sommer and Lim).

Communication with APP Fraud Victims

What is it?

When banks determine that a customer is likely the victim of an APP fraud, effective communication is key to help minimize losses to the customer and avoid damaging the relationship between the customer and the bank.

The way banks communicate with customers after they have discovered that they have been a victim of APP fraud is important for both the bank and the customer. Studies have found that informing individuals that they have been a fraud victim and providing fraud awareness information can reduce the likelihood that they will become victims again in the near term (DeLiema). Studies have also found that customer retention may be stronger after a fraud event if the financial institution is able to communicate well with the customer and provide a resolution that involves blame attribution (Somanchi, Kanuri and Telang).

What Implementation Challenges do Banks Face?

Customers who are victims of an ongoing APP fraud may not believe that they are a victim of fraud. While customers may know not to send money to individuals they don't know, by the time they are sending money to bad actors, the customer may think that they know the bad actor personally (Ainsley and Pilsworth). Victims of APP fraud are also often coached by the bad actor to lie to the bank, so the bank may not be getting accurate information from the customer (Greenstein).

Customers who have learned that they have been the victim of APP fraud may not willingly share information with banks or law enforcement. The social engineering used in APP fraud and the stigma of being a fraud victim often prevents the victim from openly communicating about the fraud. According to a Pew Research Center poll, 74% of U.S. adults who lost money from an online scam or attack did not report the loss to law enforcement, including over half of the respondents who said that their finances were hurt a great deal or fair amount by the fraud (Gottfried, Park and Anderson). Even when customers are willing to share the fact that they have been an APP fraud victim with banks, they may not be in a state where they are receptive to what the bank communicates back. After discovering that they are APP fraud victims, customers may be too anxious or upset to absorb anything that bankers communicate to them (LSB Insight).

How Can Banks Respond to These Challenges?

While the APP fraud is ongoing, communication with APP fraud victims by knowledgeable and well-trained staff should include:

- Non-judgmental language,
- Asking open-ended questions,
- Gently challenging inconsistencies,
- Providing a safe space for conversation,
- Offering discreet methods to reach out for follow-up discussions and resources.

(Lovesaid)

Customers may not realize that they are APP fraud victims and may be resistant to suggestions that they are involved in a scam. When possible, staff should aim for the customer to come to their own conclusion about being an APP fraud victim. More than one conversation with the customer may be necessary. (Ainsley and Pilsworth)

After the APP fraud has concluded, communication with APP fraud victims by knowledgeable and well-trained staff should include:

- Patiently answering the customers' questions and explaining how to avoid future scams,
- Asking open- and close-ended questions and listening to the customer's description of what happened,
- Providing advice and support at a time when the customer is more open to receiving this information, rather than when they have just learned of the APP fraud and are still feeling intense emotions,
- Providing reassurance and being empathetic, including discouraging self-blame and informing the customer of the prevalence of APP fraud, and
- Referring the customer to external organizations that can provide further support. (LSB Insight)

Banks should encourage their customers to report fraud to law enforcement organizations such as IC3 to help these organizations investigate and track APP fraud (Internet Crime

Complaint Center). Banks should also leverage information learned during post-fraud conversations to improve anti-APP fraud measures (ACAMS).

Conclusion

Regulators should discuss the above actions with financial institutions. Although there are challenges associated with each of these controls, there are actions that financial institutions can take in response to many of these challenges. Banks cannot combat APP fraud alone, but encouraging bankers to adopt the controls that best fit their institution can be a good start.

Recommendations

U.S. government agencies, such as the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation, have been seeking ways to help mitigate payments fraud, including APP fraud (Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation). While these agencies are limited in the actions they can take by their specific roles and authorities, one tool that they have at their disposal is industry education. Regulatory agencies can use the research in this paper to educate financial institutions about how they can help and detect APP fraud.

How Examiners Can Use This Research

Examiners may find opportunities during examinations to educate bankers about APP fraud. These opportunities may come from examiner observations or questions or requests for advice from bank AML/CFT or fraud personnel. In those cases, examiners can have informal discussions with bank personnel about opportunities to improve anti-APP fraud measures. Examiners should use their knowledge of the financial institution to determine how the measures in the Findings and Conclusions section can be adapted to meet the needs of the institution and which of the measures are most important. For example, if an examiner is examining a bank whose customer base conducts transactions frequently using the bank's mobile app, the examiner could encourage the bank to consider behavioral biometrics. However, if the bank's customer base instead primarily conducts transactions in person, an

examiner would likely not consider this suggestion the best use of the bank's resources and might instead focus on the training, reporting, and empowerment of frontline staff.

Examiners will likely be unable to make formal supervisory recommendations, even in cases where banks make little or no effort to detect or prevent APP fraud. While there have been multiple bills introduced in Congress relating to APP fraud prevention, as of February 2026, there are no regulatory requirements for banks to detect or prevent APP fraud in the United States (119th Congress) (118th Congress) (Bennett). However, examiners can hold informal discussions to educate bankers about the risks that APP fraud present to financial institutions and the measures they can take to combat APP fraud. Additionally, if the APP fraud results in the facilitation of money laundering or terrorist financing, such as APP fraud leading to customers setting up mule accounts at the bank, examiners may be able to use AML/CFT regulations to support the need for action.

How Other Regulatory Staff Can Use This Research

There are many individuals within regulatory agencies who may be able to leverage this research in their role. Individuals who organize or design banker outreach programs can use this information to educate bankers on the impact of APP fraud and the measures that banks can take to detect and prevent it. Individuals who have policy responsibilities can use this research to inform policy recommendations and decisions. While preventing APP fraud cannot be accomplished by regulating banks alone, financial institutions' actions are

important to APP fraud prevention, and this research can help inform policy makers on actions that banks can take independently from other banks or industries.

In conclusion, regulators can help combat APP fraud by using this research to educate themselves and banks on the measures that they can take to detect and prevent APP fraud.

Works Cited

118th Congress. "H.R.5808 - Preventing Deep Fake Scams Act." 28 Setember 2023. 27 February 2026. <https://www.congress.gov/bill/118th-congress/house-bill/5808/text?s=3&r=3&q=%7B%22search%22%3A%22scam+banks%22%7D>.

119th Congress. "S.3355 - National Strategy for Combating Scams Act of 2025." 4 December 2025. 26 February 2026. <https://www.congress.gov/bill/119th-congress/senate-bill/3355/text>.

A+ Federal Credit Union. "Gen Z Fraud: Tips For Fighting It." 28 May 2025. 27 February 2026. <https://aplusfcu.org/blog/gen-z-fraud-tips-for-fighting-it>.

ABA Foundation. "State 'Hold' Laws and Elder Financial Exploitation Prevention." January 2025. 2 March 2026. <https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/State%20Hold%20Laws%20and%20Elder%20Financial%20Exploitation%20Prevention%20%282025%29.pdf>.

ACAMS. "AFC Briefing: Fraud Planning Assumptions 2026-2030." 15 August 2025. 25 February 2026. <https://www.acams.org/en/resource/afc-briefing-fraud-planning-assumptions-2026-2030>.

Ainsley, Chris and Michelle Pilsworth. *The Bank that Breaks the Spell* Paul Benda. 12 November 2025. <https://bankingjournal.aba.com/2025/11/aba-fraudcast-the-bank-that-breaks-the-spell/>.

Akesson, Jesper, John Gathergood and Edika Quispe-Torreblanca. "Preventing Payments Fraud in the FinTech Era: New Evidence from a Behavioural Experiment." 7 August 2023. 26 February 2026. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4532757>.

Alloy. "2025 State of Scams Report." n.d. 4 March 2026. <https://www.alloy.com/reports/2025-scams-report>.

American Bankers Association. "ABA Fraud Contact Director." n.d. 3 March 2026. <https://www.aba.com/banking-topics/risk-management/fraud/directory>.

America's Credit Unions. "Australian credit unions achieve breakthrough results by separating fraud from scams." 8 January 2026. 1 March 2026.

<https://www.americascreditunions.org/blogs/americas-credit-unions/australian-credit-unions-achieve-breakthrough-results-separating-fraud>.

Armstrong, Iain. "Transforming KYT: The use of AI and machine learning in transaction monitoring." 13 January 2026. 4 March 2026. <https://complyadvantage.com/insights/transforming-kyt/>.

Arora, Shipla, Florence Hui and Caryn Leong. "Best Practice Guide: Transaction Monitoring - Effectiveness Matters." n.d. 1 March 2026. <https://www.acams.org/sites/default/files/2025-11/Best-Practice-Guide-Transaction-Monitoring.pdf>.

Balcombe, Luke. "The Mental Health Impacts of Internet Scams." 14 June 2025. Ed. Amal Mitra. 3 March 2026. <https://pmc.ncbi.nlm.nih.gov/articles/PMC12192844/>.

Bank of America. "Report Suspicious Activity." n.d. 2 March 2026. <https://web.bankofamerica.com/en/security/report-suspicious-activity>.

Benda, Paul. "Testimony of Paul Benda on Behalf of the American Bankers Association Before the Subcommittee on Oversight and Investigations of the House Financial Services Committee." 18 September 2025.

Bennett, Karen. "What is Regulation E? Protect yourself from electronic banking fraud and errors." 15 September 2025. Ed. Marc Wonjo. 27 February 2026. <https://www.bankrate.com/banking/checking/regulation-e/#types-of-transactions-covered>.

BioCatch. "Scams Mandetory Industry Codes Consultation Paper - BioCatch Response." January 2024. 2 March 2026.

—. "Spot the Impostor: Tackling the Rise in Social Engineering Scams." 2023. 1 March 2026. <https://www.biocatch.com/hubfs/WP-Spot-The-Impostor-Tackling-Social-Engineering.pdf>.

Board of Governors of the Federal Reserve System. "Economic Well-Being of U.S. Households in 2024." May 2025. 2 March 2026. <https://www.federalreserve.gov/publications/files/2024-report-economic-well-being-us-households-202505.pdf>.

CFI Team. "Tone at the Top." 11 January 2020. 4 March 2026. <https://corporatefinanceinstitute.com/resources/management/tone-at-the-top/>.

CFPB. "CFPB Warns Financial Companies About Sales and Production Incentives That May Lead to Fraud or Consumer Abuse." 28 November 2016. 1 March 2026. <https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-financial-companies-about-sales-and-production-incentives-may-lead-fraud-or-consumer-abuse/>.

—. "Elder fraud prevention and response network stakeholders." 13 February 2024. 2 March 2026. <https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/resources/stakeholders/#:~:text=Financial%20institutions%20and%20financial%20service%20providers%20must,share%20with%20How%20much%20they%20c>.

—. "Electronic Fund Transfers FAQs." 16 January 2025. 2 March 2026. <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>.

—. "Financial institutions can help prevent elder financial exploitation with alerts to trusted contacts." n.d. 2 March 2026. <https://files.consumerfinance.gov/f/documents/cfpb_trusted-contacts-fis_2021-11.pdf>.

—. "Recommendations and Report for Financial Institutions on Preventing and Responding to Elder Financial Exploitation." March 2016. 2 March 2026. <https://files.consumerfinance.gov/f/201603_cfpb_recommendations-and-report-for-financial-institutions-on-preventing-and-responding-to-elder-financial-exploitation.pdf>.

Chainalysis. "The 2026 Crypto Crime Report." 2026. 5 March 2026. <https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-release.pdf>.

Cobb, Debbie. "Survey: Consumers Want Better Scam Prevention from Banks." 20 November 2024. 2 March 2026. <https://www.fico.com/blogs/survey-consumers-want-better-scam-prevention-banks>.

Commonwealth Fraud Prevention Centre. "Impacts of Fraud." n.d. 2 March 2026. <https://www.counterfraud.gov.au/learn-about-fraud/impacts-fraud>.

Corrons, Luis. "How Social Media Fuels Scams: Trends, Tactics, and Best Practices." 22 March 2025. 4 March 2026. <https://www.gasa.org/post/how-social-media-fuels-scams-trends-tactics-and-best-practices>.

DeLiema, Marti. "What works in scam prevention messaging? (And tips for supporting fraud victim-survivors)." n.d. 2 March 2026. <https://elderjusticemn.org/wp-content/uploads/2024/06/What-Works-in-Scam-Prevention-WEAAD-2024-_-DeLiema.pdf>.

Deloitte. "New Deloitte Survey: Increasing Consumer Privacy and Security Concerns in the Generative AI Era." 2 December 2024. 2 March 2026. <https://www.deloitte.com/us/en/about/press-room/increasing-consumer-privacy-and-security-concerns-in-the-generative-ai-era.html>.

Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation. "Request for Information on Potential Actions to Address Payments Fraud." 17 June 2025. 2 March 2026. <https://www.fdic.gov/request-information-potential-actions-address-payments-fraud.pdf>.

Ebert, Nico, Kurt A Ackermann and Angela Bearth. "When information security depends on font size: how the saliency of warnings affects protection behavior." 14 November 2022. 2 March 2026. <https://www.tandfonline.com/doi/full/10.1080/13669877.2022.2142952>.

Egelman, Serge, Lorrie Faith Cranor and Jason Hong. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings." 6 April 2008. 2 March 2026. <https://dl.acm.org/doi/10.1145/1357054.1357219>.

FBI. "Money Mules." n.d. 3 March 2026. <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules>.

Federal Reserve. "Consumer Payments Study." 2025. 5 March 2026. <https://fedpaymentsimprovement.org/wp-content/uploads/2024-consumer-payments-study.pdf>.

—. *Scam Classifier*. n.d. 2 March 2026. <https://fedpaymentsimprovement.org/wp-content/uploads/scamclassifier-model-and-definitions.pdf>.

—. "ScamClassifier Model." n.d. 3 March 2026. <https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/>.

—. "Scams Information Sharing Industry Work Recommendations." n.d. 2 March 2026. <https://fedpaymentsimprovement.org/wp-content/uploads/scams-information-sharing-industry-work-group-recommendations.pdf>.

Federal Trade Commission. "Fraud Reports." 16 December 2025. 2 March 2026. <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>.

—. "How to Help Older Adults Spot, Avoid, and Report Fraud." n.d. 2 March 2026. <https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/Guiding%20Principles%20to%20Help%20Older%20Adults%20Spot%20Fraud.pdf>.

—. "Principles for Effective Training to Help Employees Spot, Stop, and Report Scams Affecting Older Adults." n.d. 3 March 2026. <https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/Principles%20for%20Effective%20Training%20to%20Help%20Employees%20Spot%2C%20Stop%2C%20and%20Report%20Scams%20Affecting%20Older%20Adults.pdf>.

FFIEC. "SPECIAL INFORMATION SHARING PROCEDURES TO DETER MONEY LAUNDERING AND TERRORIST ACTIVITY." n.d. *BSA/AML Manual.* 15 February 2026. <https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/07>.

—. "Suspicious Activity Reporting—Overview." n.d. 5 March 2026. <https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04>.

Financial Conduct Authority. "3. What do firms do to educate their customers?" n.d. 27 February 2026. <https://www.fca.org.uk/data-visualisation/3-what-do-firms-do-educate-their-customers>.

—. "Anti-fraud controls and complaint handling in firms (with a focus on APP Fraud)." 11 July 2023. 1 March 2026. <https://www.fca.org.uk/publications/multi-firm-reviews/anti-fraud-controls-complaint-handling-firms-focus-app-fraud>.

Financial Crime Enforcement Network. "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime." 25 October 2016. 26 February 2026. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005>.

Financial Crimes Enforcement Network. "Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality." 5 September 2025. 4 March 2026. <https://www.fincen.gov/system/files/2025-09/Crossborderguidance-508C.pdf>.

—. *FIN-2023-Alert005*. 8 September 2023. 2 March 2026. <https://www.fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf>.

FinCEN's Office of Special Programs Development. "The 314(b) Program A Decade of Information Sharing: Stronger Than Ever." 2016. 20 February 2026. <https://verafin.com/wp-content/uploads/2016/09/FinCEN-The-314b-Program-A-Decade-of-Information-Sharing.pdf>.

FinScan. "Modernizing KYC: exploring the key challenges of ownership, data, and technology." 17 September 2024. 3 March 2026. <https://www.finscan.com/post/modernizing-kyc-key-challenges-ownership-data-technology>.

Flanagan, Jane. "Isis funds terror with 'Tinder' love scams." 14 November 2022. *The Times.* 3 March 2026. <https://www.thetimes.com/world/africa/article/isis-funds-terror-with-tinder-love-scams-nv08xnbcz>.

Fraud.com. "Application Fraud Detection." n.d. 2 March 2026. <https://www.fraud.com/application-fraud-detection>.

Gentenaar, Kelly, Sepideh Rowland and John Davidson. *It's Not KYC: The Truth About Identity Verification* 7 March 2023. <2f8vp46shv0f-ACAMSWebinars_03.07.2023_ItsNotKYCTheTruthAboutIdentityVerification.pdf>.

Gottfried, Jeffrey, Eugenie Park and Monica Anderson. "Online Scams and Attacks in America Today." 31 July 2025. 2 March 2026. <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>.

Greenstein, Melissa. "FBI says in some scams, scammers are 'coaching' victims." 30 August 2016. 2 March 2026. <https://www.kshb.com/money/consumer/fbi-says-in-some-scams-scammers-are-coaching-victims>.

Harris, Robert. "How Banks Can Detect and Prevent Scams." 24 March 2023. 5 March 2026. <https://live.handelsblatt.com/how-banks-can-detect-and-prevent-scams/>.

Harvey, Shannon, et al. "Understanding victims of financial crime: A qualitative study with people affected by investment fraud." 3 March 2014. 2 March 2026. <https://www.fca.org.uk/publication/research/qual-study-understanding-victims-investment-fraud.pdf?utm_source=chatgpt.com>.

Houtti, Mo, et al. "A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries." July 2024. 2 March 2026. <https://arxiv.org/pdf/2407.12896>.

Ibitola, Joseph. "Understanding Customer Risk Profiling." 16 September 2023. 1 March 2026. <https://www.flagright.com/post/customer-risk-profiling-a-key-to-aml-compliance>.

Information Sharing Working Group. "Key Fraud Information Sharing Mechanisms." n.d. 1 March 2026. <https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/SSSATech_InfoSharingMechanisms.pdf>.

Internet Crime Complaint Center. *Federal Bureau of Investigation Internet Crime Report 2024*. n.d. 2 March 2026. <https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf>.

—. "Welcome to the Internet Crime Complaint Center." n.d. 1 March 2026. <https://www.ic3.gov/>.

James, Bryan D, Patricia A Boyle and David A Bennett. "Correlates of Susceptibility to Scams in Older Adults Without Dementia." 1 January 2015. 3 March 2026. <https://pmc.ncbi.nlm.nih.gov/articles/PMC3916958/>.

Kuhrt, Matt. "Exclusive research: Embedding fraud prevention in the customer experience." 15 July 2025. 2 March 2026. <https://www.americanbanker.com/research-report/embedding-fraud-prevention-in-the-customer-experience>.

LaFleur, Michael. "Why Underreporting Holds Back Fraud Prevention." 7 February 2025. 2 March 2026. <https://www.threatmark.com/why-underreporting-holds-back-fraud-prevention/>.

Lalchand, Satish, et al. "Forecasting the rise of push payment scams—the fraud consumers are tricked into authorizing." 9 October 2025. *Deloitte Center for Financial Services.* 4 March 2026. <https://www.deloitte.com/us/en/insights/industry/financial-services/authorized-push-payment-fraud.html>.

Leyva, Shana, et al. *Merging Forces: Why More U.S. Banks are Converging AML and Fraud* 26 June 2025.

Lovesaid. "Romance Fraud Response Toolkit for Frontline Staff & Fraud Teams." n.d. 2 March 2026. <https://lovesaid.org/frontline-staff-and-fraud-team/>.

Low, Natalie and Clare Lally. "Social and psychological implications of fraud." 29 April 2024. 4 March 2026. <https://researchbriefings.files.parliament.uk/documents/POST-PN-0720/POST-PN-0720.pdf>.

LSB Insight. *Aftercare, Not an Afterthought*. n.d. 2 March 2026. <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2023/01/Aftercare-not-an-afterthought.pdf>.

Luttrell, Terri. "The real cost of fraud for financial institutions explained." 23 July 2025. 3 March 2026. <https://www.abrigo.com/blog/blog-the-true-cost-of-fraud/>.

Marek, Lynne. "Banks struggle to talk about fraud." 15 May 2025. 5 March 2026. <https://www.paymentsdive.com/news/banks-credit-unions-communication-payments-fraud/748226/>.

McDade, Patrick. "Testimony of Patrick McDade - Hearing Entitled “Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial." 5 March 2026. 9 March 2026. <https://docs.house.gov/meetings/BA/BA20/20260305/119023/HHRG-119-BA20-Wstate-McDadeP-20260305.pdf>.

McHugh, Brian. "How to identify and break down IT silos." 16 May 2024. 3 March 2026. <https://www.advsyscon.com/blog/break-down-silos-in-it/>.

Nacha. "New IAT Exception Request Available in Nacha’s Risk Management Portal." 28 October 2024. 4 March 2026. <https://www.nacha.org/news/new-iat-exception-request-available-nachas-risk-management-portal>.

NICE Actimize. "2025 Fraud Insights U.S. Retail Payments Edition." n.d. 4 March 2026. <https://info.niceactimize.com/rs/338-EJP-431/images/2025-Fraud-Insights-Report-U.S.-Retail-Payments-Edition.pdf?utm_source=marketo&utm_medium=email&utm_region=amer&utm_campaign=701Vo00000Z7BU3IAN&aliId=eyJpIjoiV1I1bE5PelU2bjlpbTJsVCIsInQiOiJFTHFQQjNBM3FZa>.

Office of Inspector General. "Material Loss Review of Heartland Tri-State ." 7 February 2024. 3 March 2026. <https://oig.federalreserve.gov/reports/board-material-loss-review-heartland-tri-state-bank-feb2024.pdf>.

Office of Investor Education and Advocacy. "Investor Bulletin: FINRA’s New Account Protection Rule - Trusted Contacts." 8 May 2018. *Investor.gov.* 2 March 2026. <https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins-30>.

Palla, Ken. "Faster Payments: Is Adding Sand in the Gears Necessary?" n.d. 2 March 2026. <https://www.biocatch.com/blog/faster-payments-sand-in-the-gears>.

—. "ZELLE FRAUD: Top Ten Controls Banks Can Deploy Today to Protect Consumers." April 2025. 4 March 2026. <https://www.biocatch.com/hubfs/White%20Papers/WP-Top-Ten-Zelle-Fraud-Controls.pdf>.

Place, Nathan. "'Trusted contacts' provide banks new fraud bulwark." 8 September 2025. 2 March 2026. <https://www.americanbanker.com/news/trusted-contacts-provide-banks-new-fraud-bulwark>.

Powerful Partners in Prevention, Break Out Session Recording - FICO World 2024. Perf. FICO. 2024. YouTube. 2 March 2026. <https://www.youtube.com/watch?v=lhWcSL9fSU0>.

PWC Canada. "Breaking down the silos to combat financial crimes." n.d. 5 March 2026. <https://www.pwc.com/ca/en/services/deals/breaking-down-the-silos-to-financial-crimes.html>.

PYMNTS. "Block Chief Risk Officer Says Scams Test Trust After the Damage Is Done." 11 December 2025. 3 March 2026. <https://www.pymnts.com/news/security-and-risk/2025/block-chief-risk-officer-says-scams-test-trust-after-the-damage-is-done/>.

Regions Bank. "How to create an anti-fraud training program." 7 February 2025. 4 March 2026. <https://www.regions.com/insights/small-business/article/anti-fraud-training>.

Ribeiro, Frank, Augusto Giacoman and Maureen Trantham. "Dealing with market disruption & Seven strategies for breaking down silos." n.d. 3 March 2026. <https://www.strategyand.pwc.com/gx/en/insights/2016/dealing-market-disruption/dealing-with-market-disruption.pdf>.

Robb, Dan. *One Community Bank's Fight Against a Mass Text Scam* Paul Benda. 14 January 2025. <https://bankingjournal.aba.com/2025/01/aba-fraudcast-one-community-banks-fight-against-a-mass-text-scam/>.

Rogin, Ali and Claire Mufson. "How human trafficking victims are forced to run 'pig butchering' investment scams." 4 January 2025. *PBS News Weekend.* 2 March 2026.

Rust, Adam. "Statement for the Record - “Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."." 5 March 2026. 9 March 2026. <https://docs.house.gov/meetings/BA/BA20/20260305/119023/HHRG-119-BA20-Wstate-RustA-20260305.pdf>.

Ryder, Nic. "Written Evidence Submitted by Professor Nic Ryder (Cardiff University)." October 2023. 1 March 2026. <https://committees.parliament.uk/writtenevidence/125617/pdf/>.

Santander. "Over 1,800 customers saved from potential Facebook Marketplace scams by new Santander Fraud Protections." 5 June 2024. 1 March 2026. <https://www.santander.co.uk/about-santander/media-centre/press-releases/over-1800-customers-saved-from-potential-facebook>.

Scam Prevention Research Committee. "A Review of Scam Prevention Messaging Research: Takeaways and Recommendations." April 2024. 2 March 2026. <https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/A%20Review%20of%20Scam%20Prevention%20Messaging%20Research.pdf>.

Schraw, Gregory, Roger Bruning and Carla Svoboda. "Sources of Situational Interest." 1995. 4 March 2026. <https://journals.sagepub.com/doi/epdf/10.1080/10862969509547866>.

Segner, Michael. "The Guide to Data Consistency: How to Find and Fix Data Consistency Issues." 16 June 2025. 5 March 2026. <https://www.montecarlodata.com/blog-data-consistency/>.

Somanchi, Sriram, Vamsi Kanuri and Rahul Telang. "Mitigating Churn After Online Financial Fraud: The Value of Blame Attribution." 23 March 2025. 2 March 2026. <https://journals.sagepub.com/doi/10.1177/10591478251331125>.

Sommer, Matthew and HanNa Lim. "Key Determinants of Naming a “Trusted Contact” for U.S. Brokerage Accounts." 27 September 2022. 2 March 2026. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4231059>.

Starling Bank. "Starling launches UK-first AI tool to combat scams." 27 October 2025. 4 March 2026. <https://www.starlingbank.com/news/scam-intelligence-launch/>.

State of Wisconsin. "2023 Wisconsin Act." 2023. 27 February 2026. <https://content.govdelivery.com/attachments/WIGOV/2024/03/20/file_attachments/2820960/sb628.pdf>.

Tapling, Peter. "Authority, Urgency, Action: The Financial Scammer’s Recipe." n.d. 1 March 2026. <https://www.biocatch.com/blog/authority-urgency-action-scammer-recipe>.

—. "The power of a pause: Can a small delay prevent big fraud losses?" n.d. 1 March 2026. <https://www.biocatch.com/blog/small-delay-prevent-fraud-losses>.

Thackeray, John. "A Framework for Effective Fraud Risk Management." August 2018. *ACFE Insights Blog.* 3 March 2026. <https://www.acfe.com/acfe-insights-blog/blog-detail?s=a-framework-for-effective-fraud-risk-management>.

The Federal Reserve. n.d. Website. 2 March 2026. <https://fedpaymentsimprovement.org/resources/educational/>.

The Knoble. "Measuring the Financial Impact of Authorized Push Payment Scams." n.d. 2 March 2026. <https://www.biocatch.com/wp-measure-impact-app-scams>.

The Treasury. "Scams – Mandatory Industry Codes." November 2023. 2 March 2026. <https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf>.

Toh, Ying Lei. "Combating Authorized Push Payment Scams in Fast Payment Systems." 15 November 2024. 2 March 2026. <https://www.kansascityfed.org/research/payments-system-research-briefings/combating-authorized-push-payment-scams-in-fast-payment-systems/>.

TransUnion. "Banking Fraud Detection." n.d. 2 March 2026. <https://www.transunion.com/business-needs/fraud-prevention/banking-fraud-detection>.

TriNet. "Common Challenges with Employee Training." 4 December 2023. 3 March 2026. <https://www.trinet.com/insights/common-challenges-with-employee-training>.

U.S. Department of the Treasury. "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia." 14 October 2025. 5 March 2026. <https://home.treasury.gov/news/press-releases/sb0278>.

U.S. Government Accountability Office. "Payment Scams: Information on Financial Industry Efforts." 24 July 2024. 3 March 2026. <https://www.gao.gov/assets/gao-24-107107.pdf>.

United States Attorney's Office Southern District of New York. "11 Members Of Money Laundering Ring Charged." 2 March 2020. 5 March 2026. <https://www.justice.gov/usao-sdny/pr/11-members-money-laundering-ring-charged>.

United States Secret Service. "Combating the Illicit Use of Digital Assets." n.d. 4 March 2026. <https://www.secretservice.gov/investigations/digitalassets>.

Wen, Xin, et al. "Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life." 7 July 2022. *International Journal of Environmental Research and Public Health.* 2 March 2026. <https://www.mdpi.com/1660-4601/19/14/8294>.

Wilder, Mason. "Top 5 Fraud Trends of 2025." January 2025. 1 March 2026. <https://www.acfe.com/acfe-insights-blog/blog-detail?s=top-fraud-trends-2025>.

Woolley, Rachel. "A Pandora’s Box of Money Laundering Crime." 8 February 2022. 5 March 2026. <https://www.acams.org/en/opinion/a-pandoras-box-of-money-laundering-crime>.