THEMIS

Bottomline

White Paper

2025 FRAUD TRENDS

wearethemis.com

bottomline.com/risk-solutions

CONTENT

Executive Summary

Our White Paper

Banks today face intense pressure to keep pace with rapidly evolving fraud trends, balancing an increasingly complex internal and external threat landscape with changing customer needs, market dynamics, and regulatory demands. Staying on top of the latest fraud trends is paramount. This white paper outlines the most pressing fraud risks on the horizon for 2025, providing insights into the tactics, vulnerabilities, and strategic priorities that will affect the banking industry over the coming year.

Taking a focused industry perspective, we have looked specifically at the challenges faced by commercial banks today, exploring the dual role of technology in both driving and deterring fraud, as well as the interplay between insider and external fraud risks, and traditional and emerging payment types. Our research included an industry-wide survey of **over 90 banking professionals** from across North America and the UK, in a range of target roles, including senior management, information security, fraud, and compliance **(shown in Figure 1)**.

Despite the threat-oriented analysis covered by much of this white paper, there is much to be hopeful about as we kick off 2025. The commercial banking sector is one of the most proactive in terms of recognizing fraud threats as they emerge and using the latest technology to prevent and mitigate these threats. The key findings from our research can serve as an important guide for banks looking to understand and address the shifting dynamics of their fraud threat exposure based on feedback from peers.

Jurisdictional Breakdown

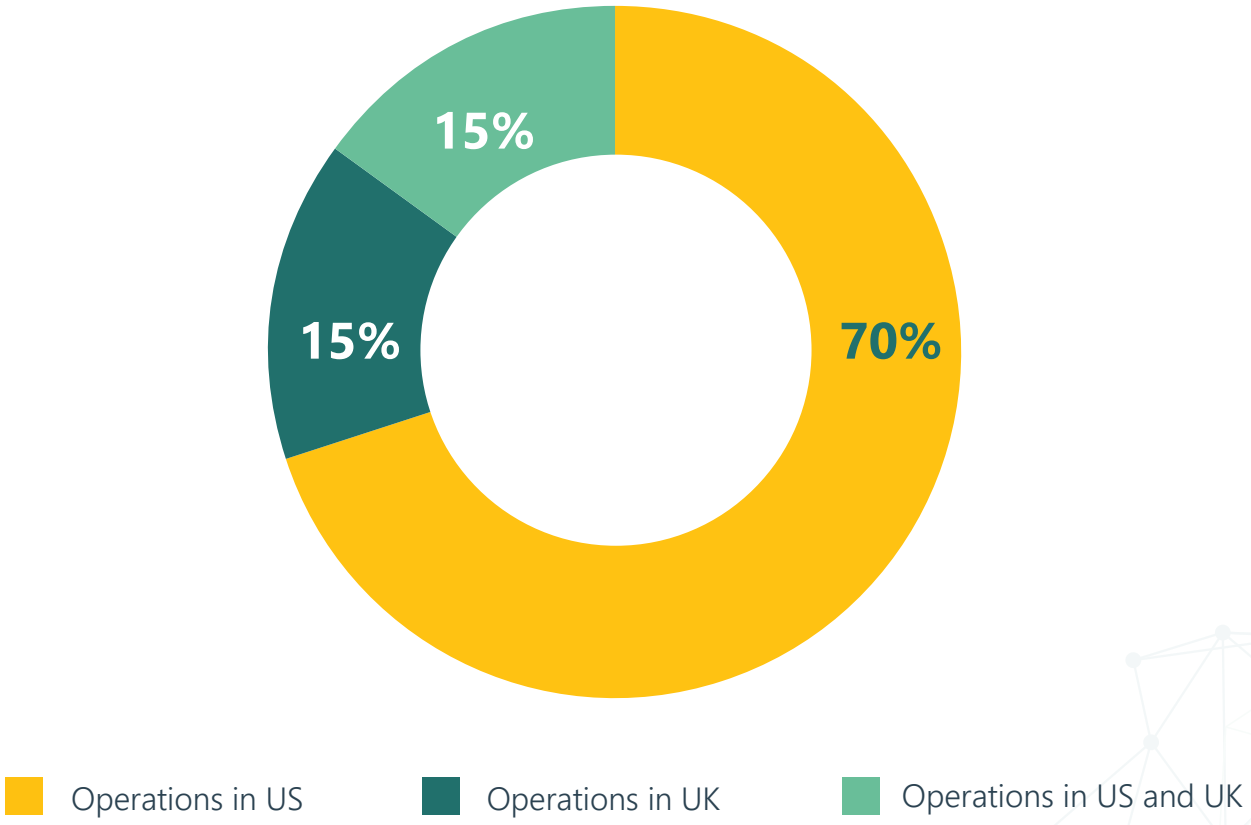


Figure 1*

*Of those surveyed, **70%** work at banks with operations in the US, **15%** at banks with operations in the UK, and another **15%** at banks with operations in both regions. In addition to commercial banking, other key services offered by the banks surveyed include financial technology services, money transfer services, trade finance, and investment banking.

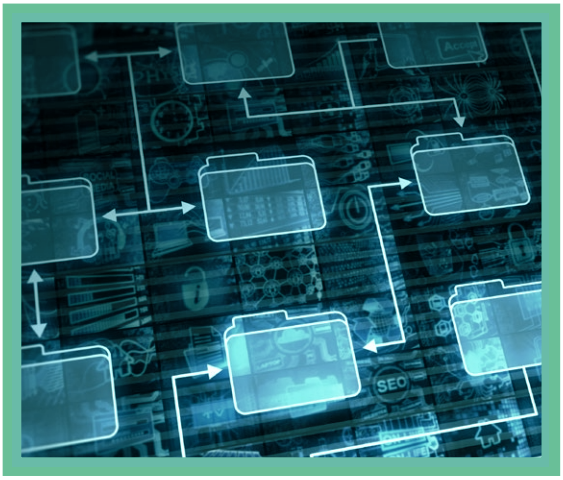
Key Takeaways: Fraud In Context

Fraudsters are exploiting new banking products and trends.

As banks continue to integrate new technology offerings and services, fraudsters are constantly looking to exploit these advancements to devise new methods of conducting fraud. Our research highlights the relationship between new banking products and services and the evolving strategies of fraudsters. **62%** of our survey respondents highlighted online account opening and client onboarding as a top banking trend impacting their bank's fraud exposure. This was followed by the rise of open banking at **59%** and increased automation of services at **55%**.

Bank fraud is growing and so are its costs.

Our research finds that banking fraud is on the rise, and with it, the financial toll on institutions continues to escalate. Over a quarter of our survey respondents attributed at least **10%** of their bank's operational losses in 2024 to fraud, with **50%** moreover saying their bank experienced an increase in fraud cases in 2024. On top of that, **66%** of respondents feel their bank is only somewhat prepared to address emerging fraud risks, with another **12%** feeling either underprepared or significantly underprepared.



Intersection of insider threats and external fraud.

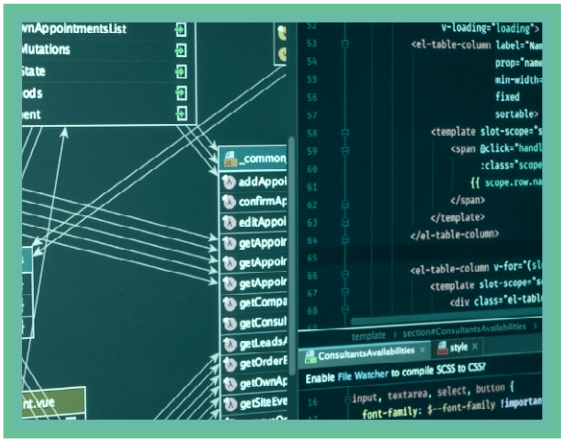
The risk of collusion between insiders and external fraudsters is a growing concern, underscoring the need for robust internal controls as banks rely more on digital systems and online workflows. Current fraud detection tools often focus on insider and external threats separately, leaving gaps in protection. Insider threat tools also tend to be reactionary versus proactive in nature.

Key Takeaways: Trends

Our research shows how the integration of cutting-edge technology into today's banking sector as well as fraud techniques is transforming today's fraud landscape.

Fraud techniques are growing in sophistication thanks to generative AI and increased automation.

Generative AI can facilitate the execution of key types of fraud including account takeover and business email compromise fraud. Criminals can use generative AI to carry out more sophisticated phishing schemes or create malicious malware and other cyber-techniques.



Traditional risks persist alongside newer threats, driving a global rise in fraud.

Fraud targeting more traditional payment forms such as checks and credit cards is again on the rise, highlighting how banks are dealing with fraud from all sides. Moreover, criminals can now leverage new technologies to enhance their effectiveness at targeting these traditional payment types, combining familiar methods with newly enhanced tools and tactics.

The rise of open banking creates new threats.

The rise of open banking is transforming the financial landscape in incredibly positive ways, but it does bring with it new fraud challenges. These include new risk exposure for banks relating to data breaches, identity fraud, and cross-border fraud.

Deepfakes and synthetic identities are growing tactics of choice.

With just last month FinCEN issuing an alert for financial institutions on deepfake-based fraud, it is clear this fraud type is here to stay. 50% of our survey respondents identified generative AI-driven fraud as the trend posing the greatest threat to their bank in 2025, with deepfake-based fraud appearing more often across a range of fraud types. Nearly 40% of our survey respondents also believe synthetic identity fraud will pose one of the greatest threats to their bank in 2025, highlighting the complexities these technologies present in biometric authentication protocols.

The rise of Fraud-as-a-Service (FaaS), automated fraud, and AI-enabled cyberattacks are also of key concern.

Our research finds that bot-driven and automated fraud techniques are rapidly increasing, significantly escalating both the scale and speed of attacks. Another associated risk that is also emerging comes from the rise of FaaS and AI-enabled cyberattacks, which allow for less experienced and knowledgeable criminals to carry out fraud attempts more successfully.

What Does This All Mean?

In the face of today's escalating fraud threats, adopting cutting-edge technology that is fully tailored to your organization's specific needs is no longer a matter of choice but an essential component of fighting fraud in commercial banking. Advanced tools, covering both proactive and reactive detection and mitigation, enable banks to more effectively detect, investigate, and prevent both internal and external fraud threats. It is also important for banks to adopt a multi-pronged approach to fraud prevention to keep pace with emerging trends and risks, including more effective industry collaboration and awareness building. We can use the insights gained in this white paper as a crucial first step.

Chapter 1: Introduction

An Evolving Threat Landscape

Today's fraud landscape is increasingly defined by sophisticated threats that outstrip dated defenses, such as ones that rely on static rules or legacy systems. Criminals both inside and outside of banks, and sometimes in coordination (as we have seen with recent AML fraud), are using new technologies to carry out large-scale, complex fraud schemes, taking advantage of vulnerabilities in a more digital and interconnected banking environment. Traditional risks persist alongside these newer threats, driving a global rise in fraud. To stay ahead of the curve and protect against fraud, commercial banks must invest in the latest anti-fraud strategies and technologies that fit their specific risk profile, which requires a strong understanding of emerging fraud trends. The pace of innovation among criminals demands equally agile and anticipatory responses from banks. As such, banks must ask themselves what key threats and challenges they need to prepare for in 2025.

Why Fraud Demands Our Attention

In 2023, fraud schemes reached an estimated $485 billion in global losses, with banks bearing the bulk of this, since $442 billion of these losses were across payments, checks, and credit card fraud. In fact, payment fraud is one of the fastest-growing business threats, with a recent study finding that an alarming 80% of organizations were hit by payment fraud attacks in 2023. In the US alone, total estimated fraud losses reached $138 billion, with banks incurring $127 billion of that total. The UK also faced steep losses, with customer fraud estimated at £1.17 billion.

All of this highlights a stark reality: fraud remains as pervasive as ever. Moreover, as the line between fraud and cybercrime is increasingly blurred, we are seeing a rise in sophisticated cyber tactics used to carry out fraud across the financial sector. Fraud also intersects with other serious crimes, including corruption and transnational organized crime, and is a predicate crime to money laundering. These overlapping threats create a fraud ecosystem today that extends far beyond one industry or victim type. Banks today face heightened fraud risks that extend from other sectors as well, especially as their business customers contend with their own challenges.

Commercial banks are keenly aware of the potential impact of fraud on their own bottom lines. As financial services continue to face tough macroeconomic and geopolitical conditions in 2025, understanding and combating the dynamics of fraud is critical to prevent additional fraud-related losses. Moreover, small businesses are increasingly concerned about payment fraud, as a recent survey by KeyBank indicates. The survey found that the top concern among small-to-medium size businesses was payment fraud of various types, including unauthorized transactions, identity theft, malware and ransomware, and phishing and email scams. The role of technology driving an uptick in these fraud types was equally highlighted by our survey respondents.

Indeed, our survey results show that fraud is as costly as ever:

- Over a **quarter** of our survey respondents attributed at least **10%** of their bank's operational losses in 2024 to fraud **(shown in Figure 2 below).**
- Furthermore, nearly **50%** of our respondents said their bank experienced an increase in fraud cases in **2024**, and only **17%** of respondents saw a decrease in fraud cases **(shown in Figure 3).**
- On top of that, **66%** of respondents feel their bank is only somewhat prepared to address emerging fraud risks, with another **12%** feeling either underprepared or significantly underprepared **(shown in Figure 4 below).**

Together, these insights emphasize the urgent need for banks to enhance their fraud detection and prevention strategies.

Estimated Percentage of Operational Looses Attributable to Fraud in 2024

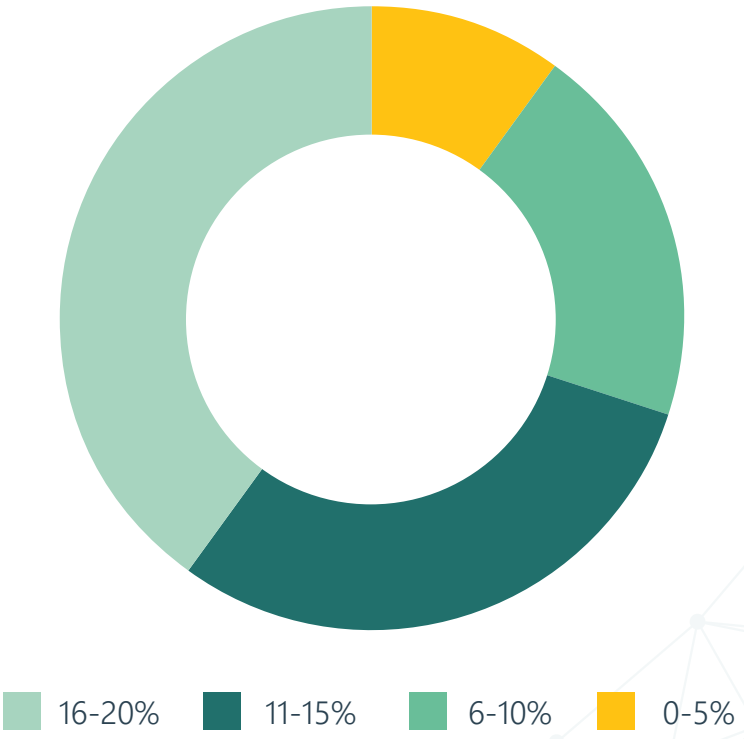


Figure 2

Change In Fraud Cases 2023 Vs 2024

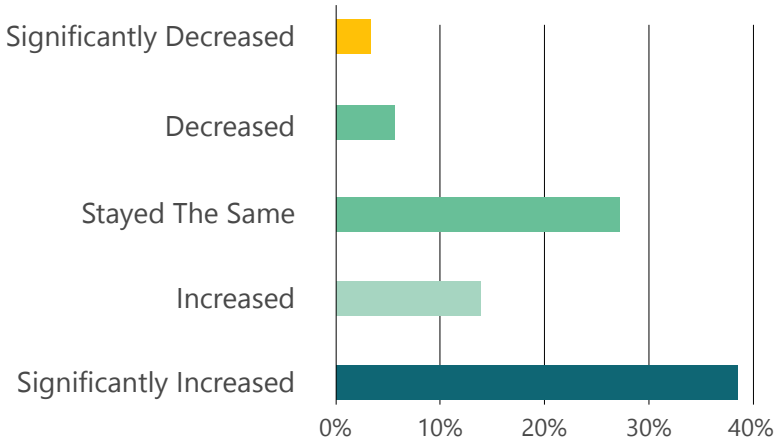


Figure 3

Fraud Preparedness Hierarchy

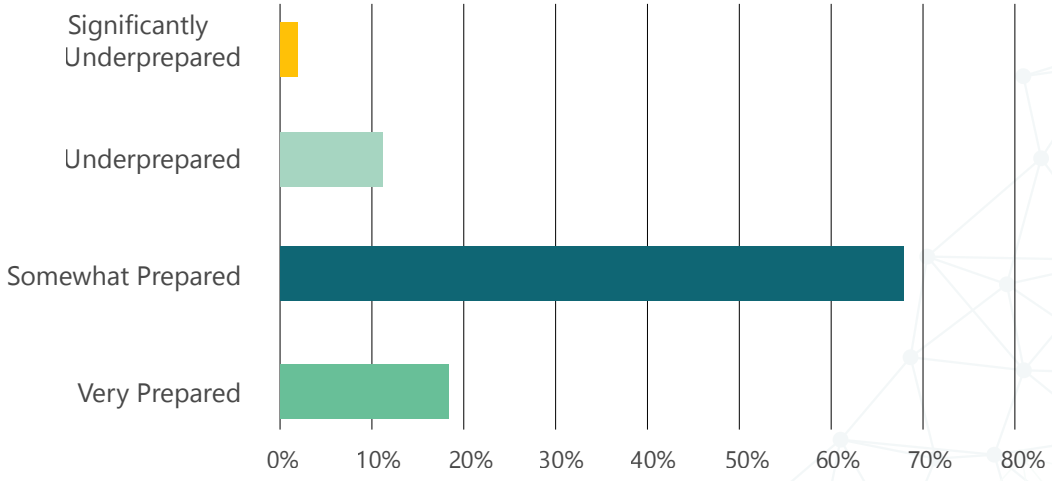
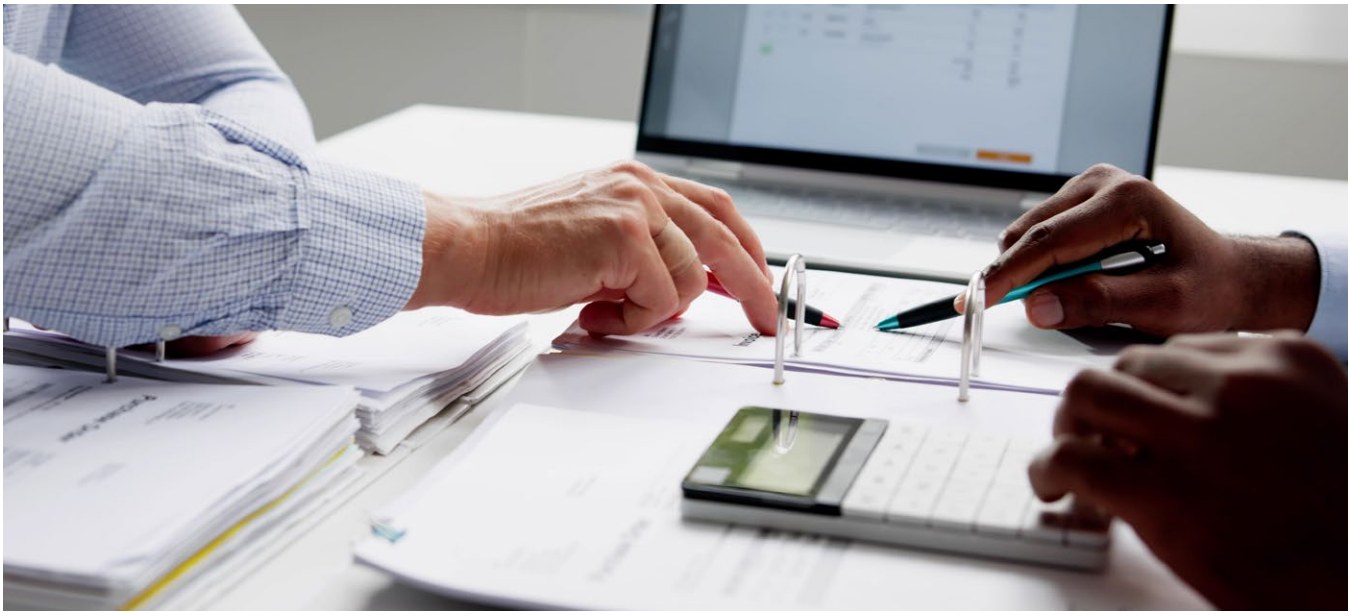


Figure 4



Moreover, compliance costs are also on the rise. A recent study by LexisNexis revealed that compliance costs have increased for almost all financial institutions. While anti-fraud measures are only one component of overall financial crime compliance costs, this trend reflects the increasingly demanding and complex nature of compliance strategies for banks and other financial institutions. Moreover, as various financial crimes often overlap, it is hard to fully separate out compliance costs as only relating to one specific crime type or regulatory demand. This issue is particularly salient today, with banks facing increasing risks and demands on their operational resilience.

The legal repercussions associated with fraud can be just as severe, especially in today's world of increasingly stringent regulatory pressures. Furthermore, the impact of fraud can go beyond such direct financial and legal ramifications, spilling over into reputational damage and customer relationships. This is because fraud can impact customer perceptions and trust, as well as investor confidence, which in turn can lead to declining customer bases. Some estimates have found that more than half of victims consider switching banks after being scammed, with 30% actually leaving. With many corporate customers spreading their banking relationships across several banks, reputation is paramount to keep customers on board.

A large enough fraud event can also have a sizeable impact on the banking sector as a whole, extending beyond the direct impact on the implicated bank. For instance, research by the IMF found that AML/CFT deficiencies are associated not only with large drops in stock prices for the most directly affected banks but also declines in share prices of other lenders who simply happen to be in the same country, as well as banks in the region that have similar cross-border exposures.

When Fraud Goes Viral

In today's world of social media, a single fraud incident can have lasting reputational damage that can take years to rebuild. Once a financial crime scandal breaks, social media can play a significant role in amplifying public outrage. For instance, when a large US bank was revealed to have engaged in unethical customer practices, whistleblowers took to platforms like Twitter, Facebook, and LinkedIn to share their experiences. Hashtags related to the scandal trended widely, attracting media and public attention.

All this demonstrates the vested interest the banking sector has in fighting fraud, given the significant potential repercussions. Understanding the latest fraud risks is therefore crucial, if banks are to build the best defenses to thrive in an evolving threat landscape. Keeping banks and their customers safe demands a multifaceted approach that blends risk identification and understanding with advanced technology and forward-thinking collaboration and governance. Bad actors don't operate in isolation, and risk management strategies shouldn't either.

Chapter 2: Today's Fraud Threat Landscape

Banking Service Trends Shaping Today's Fraud Landscape

The financial services sector has been defined in recent years by transformative technologies and innovative services. From the rise of mobile banking and real-time payment options, commercial banks face a starkly different operational landscape than even 10 years ago. With innovation, however, comes new challenges and vulnerabilities. The increasing digital and open nature of banking today creates vulnerabilities in the security and compliance measures of banks, and the integration of next-generation technologies is creating an even more complex threat landscape to navigate.

We asked our survey respondents which banking service trends they believe have the highest potential to increase their bank's fraud exposure. The answers were very telling.

Top Banking Service Trends Perceived to Increase Fraud Exposure

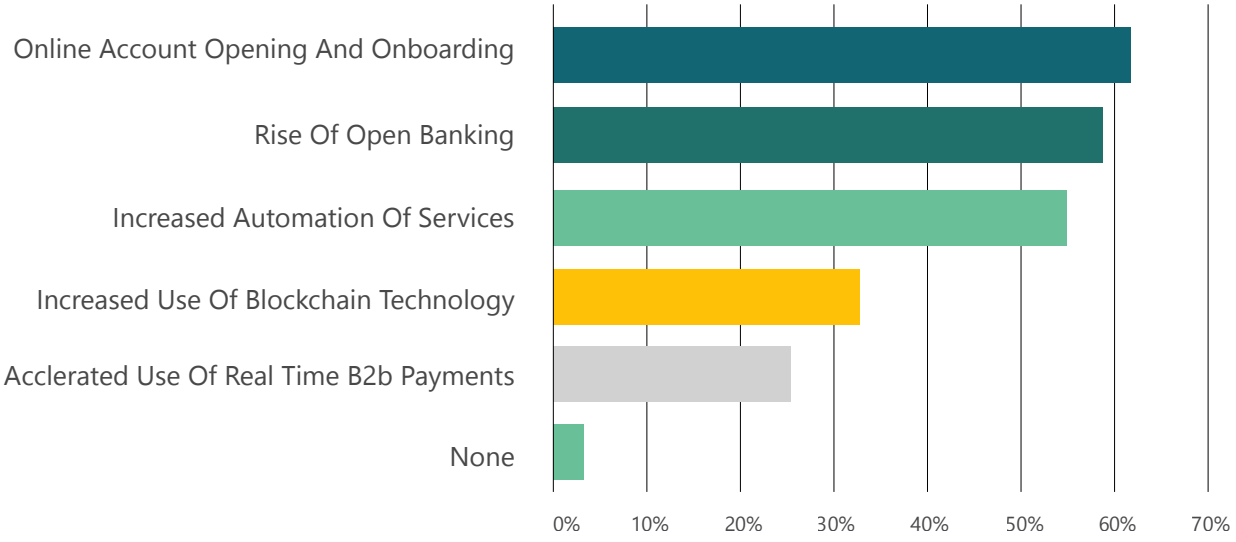


Figure 5

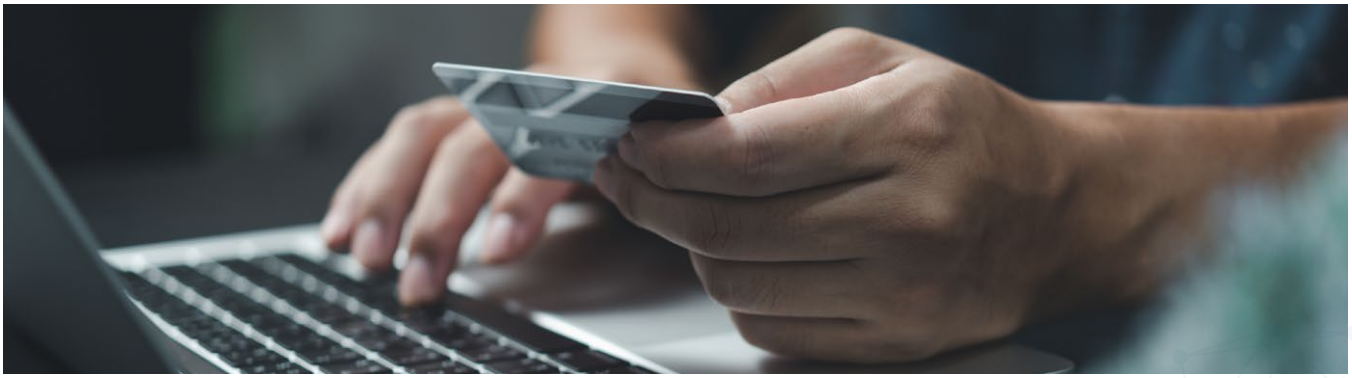
* Survey respondents were able to select up to three top trends.

Online Account Opening & Client Onboarding

The largest number of our survey respondents, at **62%**, believe that online account opening and client onboarding have the highest potential of all banking services to increase their bank's fraud exposure **(shown in Figure 5 above).** Online account opening and client onboarding has increased exponentially with the rise of online and mobile banking. Today, more Americans prefer banking via a phone app or website than in person. Many banks are also embracing AI chatbots and other technology to further digitalize customer experiences. All this lends itself to the continuation of more bank accounts and customer relationships being established without any in-person verification. This creates many notable fraud risks, which this report will go into in detail. Of particular concern, the rise of deepfake technology leaves banks with even the most advanced "liveness test" and biometric protocols vulnerable.

Rise of Open Banking

A large majority of respondents, at **59%,** also believe the rise of open banking has high potential to increase their bank's fraud exposure **(shown in Figure 5 above).** Open banking is a key service trend to pay attention to as we enter 2025. Building on the broader introduction of real-time payments across the banking sector, open banking enables the sharing of bank account data with another financial service provider (for instance, another financial institution or a third party such as a digital platform). It is on the rise globally, especially in key markets such as the US and UK, with the technology already integrated into many popular financial tools and services. In fact, the global value of open banking transactions is expected to surpass $330 billion by 2027, up from $57 billion in 2023. While open banking allows individuals and small businesses to be more fully in charge of their own financial data, it also creates new challenges for banks navigating fraud risks. Open banking exposes data to third parties, for instance, thus potentially increases the risk of data breach driven fraud. Moreover, the relatively new nature of open banking means some regions lack consistent regulatory frameworks or oversight, which can lead to inconsistencies in security protocols, making it easier for fraudsters to find weaknesses to target.



Increased Automation of Services

Akin to online account opening and onboarding, increased automation of services is also increasing as banks embrace the digital banking movement. Banking automation uses technology such as AI to replace manual processes with automated ones, thus helping to reduce costs and increase efficiency. For instance, more banks are offering self-service portals and automated onboarding. There are some key benefits to automated services, such as their potential to enhance security measures and protect customer data. At the same time, the automation of services introduces several fraud risks, which is reflected by **55%** of our survey respondents highlighting automation's high potential impact on their organization's fraud exposure **(shown in Figure 5 above).** Key challenges such as increased exposure to account takeover fraud and weaknesses in biometric authentication are covered in this report.

Technology Trends Shaping Today's Fraud Landscape

In addition to asking which banking service trends are having the greatest impact on respondents' risk exposure, we also asked respondents which emerging technologies are having the greatest impact on the fraud risk profile of their organizations. Results were fairly evenly split as follows **(shown in Figure 6 below):**

- Technology related to open banking led the way at 66% of respondents.
- Biometric authentication was next at 57% of respondents.
- Generative AI followed at 48% of respondents.
- Blockchain and cryptocurrency were close by at 47% of respondents.

With open banking covered above, let's take a closer look at the other three technology types.

Impact of Emerging Technologies on Bank Fraud Risk

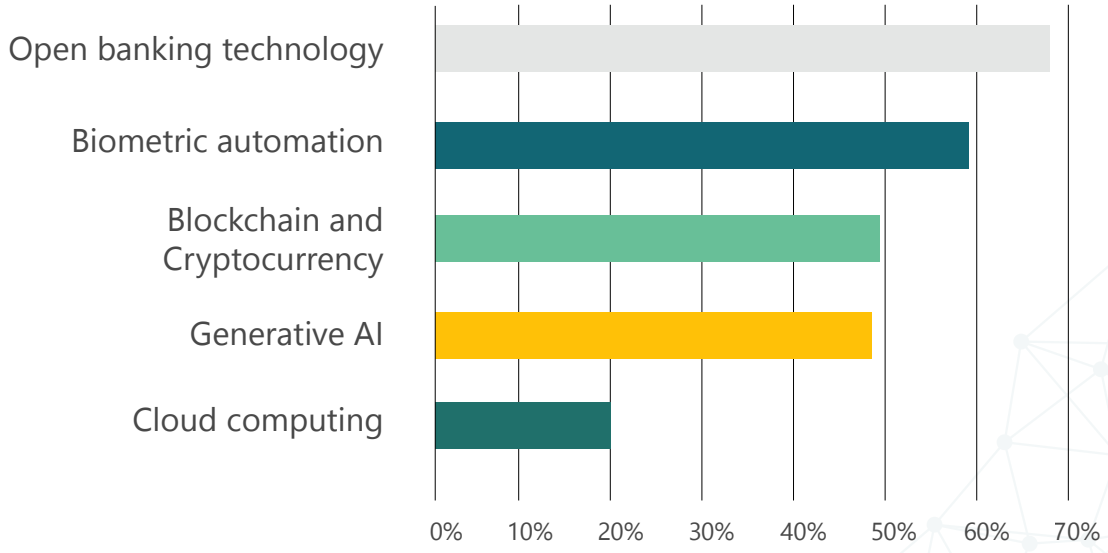


Figure 6 *

* Survey respondents were able to select up to three top emerging technologies.

Biometric Authentication

Biometric authentication uses unique physical or behavioral characteristics – such as fingerprints, facial recognition, voice patterns, or even typing rhythm – to verify a user's identity. In banking, biometric authentication adds a robust layer of security by making it harder for fraudsters to impersonate legitimate customers. With the continued preference for mobile and online banking, biometric authentication can help verify customers' identities during onboarding or before they gain access to accounts; this helps prevent false new account openings, synthetic identity fraud, account takeovers, and other forms of fraud.

Types of Biometrics

Fingerprint Scans:
Fingerprint scans are now standard features in many tech devices, including computers and even in entry-level smartphones.

Facial Recognition:
Phones and apps now allow corporate clients to approve transactions using facial recognition software, which cross-references a pre-recorded image for verification.

Voice Recognition:
Companies like Barclays use voice recognition as a form of two-factor authentication. This technique uses a recording of a customer's voice pattern and matches it with a customer's voice, allowing for the verification of transactions over the phone.

Behavioral Biometrics:
This involves studying patterns in behavior, such as keyboard strokes or mouse movements, to detect fraudulent activity, and it is gaining ground as a nuanced form of security.

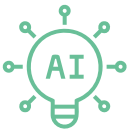
While biometric authentication provides a highly secure form of authentication compared to more traditional security protocols such as passwords and PINs, they are not without their own risks. For one, storing biometric data poses a significant security risk; if breached, this data cannot be changed like a password, creating long-term vulnerability for affected individuals. Moreover, with advancements in generative AI and deepfake technology, fraudsters can create convincing deepfake images, video recordings, or videos that may increasingly be able to trick biometric systems.

Generative AI

AI is driving major transformations across the banking sector, enabling commercial banks to streamline workflows, enhance customer experiences, and improve operational efficiency. Moreover, AI enhances fraud prevention for banks by enabling real-time analysis of transaction patterns, swiftly identifying anomalies, and detecting potential fraud with greater accuracy, thereby reducing financial losses and improving customer trust. We'll discuss this in more detail later on.

However, the rise of AI has also empowered criminals, creating a dual-edged sword for the banking industry. According to Deloitte, cybercriminals are increasingly using AI to exploit vulnerabilities in financial systems, leveraging AI tools to identify gaps and patterns in banking systems to exploit. In addition, criminals are deploying AI-driven social listening and advanced data analytics tools to gather valuable information online. They scan public and private data sources, including social media, open forums, and the dark web, to gain insights into potential security gaps and targets. This intelligence allows them to craft highly targeted social engineering attacks and acquire the data needed to bypass security protocols.

Generative AI is another key emerging fraud enabler, as criminals can use tools such as ChatGPT to create convincing phishing schemes or fake content, including fake documentation. The convergence of deepfake and generative AI tools is also allowing criminals to create highly realistic fake identities or impersonate real individuals. Last month, FinCEN issued an alert noting an uptick in suspicious activity reporting by financial institutions that describe the use of deepfake media and AI generated documents in fraud schemes targeting their institutions and customers. The schemes in question include the altering or creation of fraudulent identity documents to circumvent authentication and verification mechanisms, as well as false video content for secondary visual identification that are indistinguishable from documents or interactions with actual verifiable humans. This report will discuss these risks in detail.



FinCEN Warns of Fraud Schemes Arising from Deepfake Media & Generative AI

FinCEN reported that some financial institutions have seen criminals use AI generated or altered images used for identification purposes, including driver' licenses and passports. FinCEN said it was aware of successful fraud attempts where criminals opened bank accounts using these fraudulent identities, including check fraud, credit card fraud, and authorized push payment fraud, among other fraud types. In their alert, FinCEN advises the re-reviews of account opening documents, including performing a reverse image search of identity photos to see if they match any online galleries of faces created with Generative AI. To the extent capable, they also recommend financial institutions to examine the image metadata or use software engineered to find deepfakes to be assistive. FinCEN also cautions financial institutions to watch for identity discrepancies between account documents.

Blockchain & Cryptocurrency

With the crypto market seeing a recovery year in 2023 and Bitcoin hitting an all-time high in November, it is clear that cryptocurrency offerings are here to stay across the financial sector. Crypto offers various benefits to consumers and financial institutions alike, including faster cross-border payments, reduced transaction costs, and greater financial inclusion. The crypto landscape is likely to get even more complex, with the SEC in the US opening the door in January for bitcoin exchange-traded funds to hit the mainstream, many traditional financial institutions across Wall Street and beyond finally can buy into crypto. Institutions such as Bank of New York Mellon have announced that they are offering cryptocurrency custody services for clients, bringing digital assets into the fold alongside traditional assets.

While crypto offers great opportunities across banking, it also introduces regulatory challenges and fraud risks, with the crypto sector often targeted by criminals looking to carry out illicit activities. The FBI's Internet Crime Complaint Center saw over $5.6 billion in losses tied to cryptocurrency fraud in 2023, a dramatic increase from 2022. More generally, crypto analysis firm Chainalysis found that $24.2 billion was received by illicit addresses in 2023, accounting for 0.34% of the total on-chain transaction volume it analyzed. Key crimes identified by the firm included malware, scams, stolen funds, ransomware, and darknet-related crimes.

Ethereum Manipulation Scheme

This year marked the first of its kind in a crypto fraud case in the US, with two individuals charged with a novel scheme exploiting Ethereum blockchain to fraudulently obtain approximately $25 million worth of cryptocurrency within 12 seconds. The technologically sophisticated scheme manipulated the protocols relied upon by the Ethereum blockchain, gaining access to pending transactions, altering the movement of the electronic currency, and ultimately stealing $25 million in cryptocurrency from victims. This scheme is a worrying development for the integration of crypto services into banking services, as it signals the ability for criminals to manipulate and tamper with the process and protocols by which transactions are validated and added to the Ethereum blockchain, which allows unauthorized access to pending private transactions and use of that access to obtain cryptocurrencies.

Blockchain technology also offers an appealing tool for banks seeking secure record-keeping and fraud prevention. It can serve as the basis for applications ranging from digital identity verification to the secure sharing of documents such as invoices (for example, HSBC has implemented a blockchain-based trade finance platform to streamline operations). The banking sector is also seeing a rise in enhanced cybersecurity technologies, including biometrics, behavioral analytics, and advanced encryption. While these tools offer considerable transparency, efficiency, and traceability benefits, they also create new vulnerabilities that can be exploited for fraud-related purposes. Such tools can have coding vulnerabilities or design flaws that fraudsters can target, and without proper due diligence criminals could create fake identities or conduct transactions under manipulated credentials. Due to the cross-border nature of trade finance, blockchain platforms can also be used to exploit regulatory loopholes or shift transactions to jurisdictions with lax oversight, creating opportunities for fraud and money laundering.

Industry Trends Shaping Today's Fraud Landscape

When Internal and External Fraud Collide

Commercial banks are grappling with heightened risks as external and insider fraud threats intertwine, escalating the complexity of managing financial crime. This convergence facilitates fraud schemes that leverage internal access and external manipulation, exposing banks to vulnerabilities across multiple attack vectors. As a result, traditional defenses are often insufficient, forcing banks to adopt more sophisticated detection and prevention tools to navigate an increasingly volatile risk landscape. This evolution in fraud tactics underscores the urgent need for integrated approaches that address both internal security and external threat intelligence.

Our survey respondents identified various insider fraud threats that are of key concern to their organizations:

52% of respondents identified misuse of privileged access as a top three insider threat to their bank in 2025 (shown in Figure 7).

49% of respondents see unauthorized transactions as a top three insider threat as well (shown in Figure 7).

46% of respondents identified collusion with external actors as a top insider threat (shown in Figure 7).

Impact of Emerging Technologies on Bank Fraud Risk

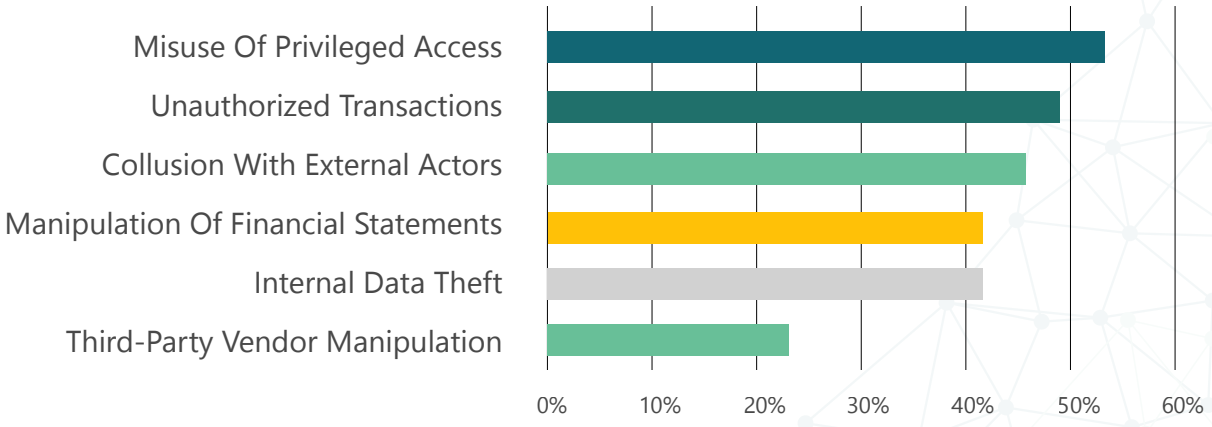


Figure 7*

* Survey respondents were able to select up to three top insider fraud risks.

As banks increasingly rely on digital infrastructure, the risk of insider collusion grows, making strong internal security and monitoring essential. Bolstering internal controls and deploying advanced technologies to detect both insider and external fraud exposures is critical. It is also vital to recognize that insider threats may come from contractors, vendors, and third-party partners, emphasizing the importance of rigorous due diligence and training across all these roles. It is also important to consider the potential impact of security laps by third parties, such as Amazon last month announcing employee data was impacted due to a third-party vendor security breach.

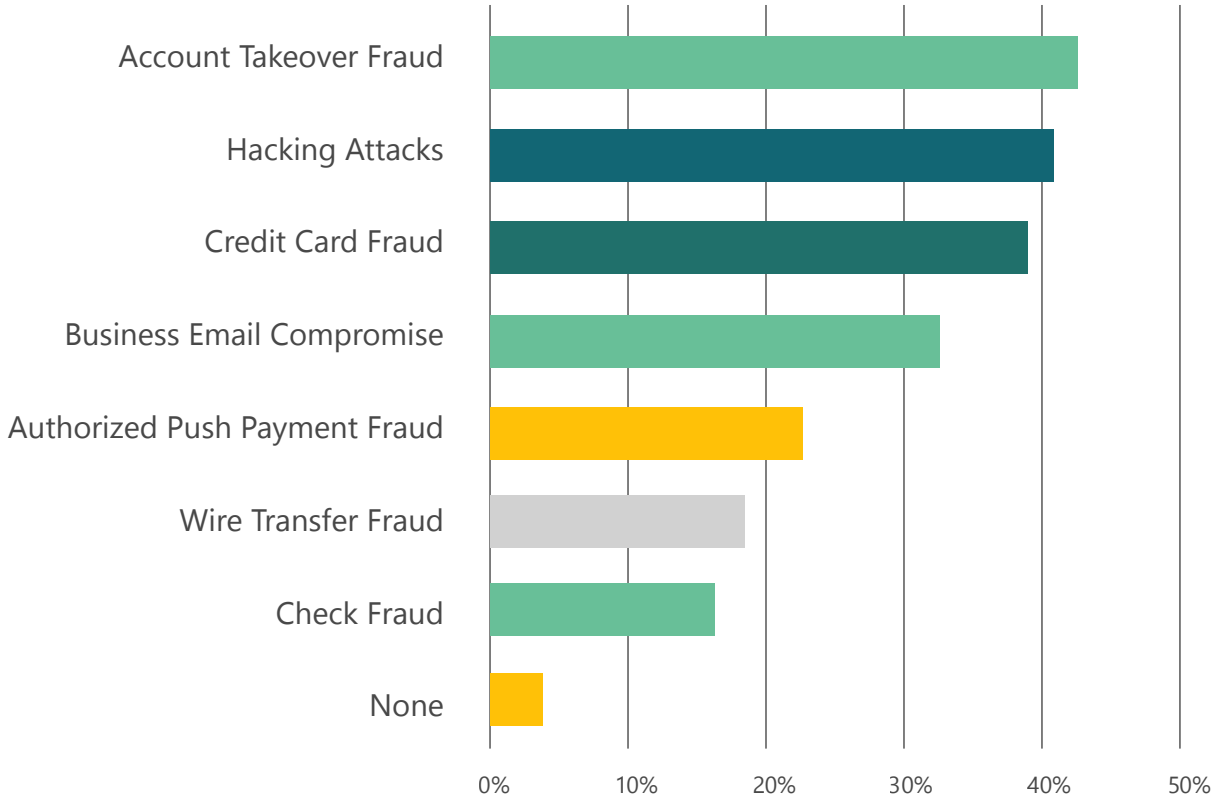
Growth in Cross-Border Fraud

The incidence of cross-border fraud has also risen significantly as a result of globalization and the growing complexity of cross-border payments. Thirty years ago, less than 1% of fraud reported to the FTC was cross-border, whereas today well over 10% is cross-border. Expectations for cross-border transactions have increased with technological developments such as payment rails, according to a J.P. Morgan report, with customers expecting faster and more efficient transactions. While such technology helps to improve cross-border payment processes, it also creates new risks around fraud and cybersecurity. Having multiple systems, jurisdictions, and regulations can also make identifying and preventing fraud more complex. Another area to consider is the use of new forms of cross-border payment systems, such as AI and blockchain networks, that could help reduce fraud risks. For instance, in October 2024, Swift announced an AI-enabled enhancement to its Payment Controls Service (PCS) as part of efforts to address fraud. The enhancement builds on Swift's existing fraud detection capabilities, utilizing advanced machine learning to analyze pseudonymized data from billions of transactions across the Swift network, allowing for more effective detecting and flagging of suspicious activity.

Chapter 3: Key Fraud Trends For 2025

As 2025 kicks off, it's crucial to spotlight the coming year's most pressing fraud trends, including new tactics, vulnerabilities, and challenges poised to shape the banking industry and anti-fraud efforts. We put this question to our survey respondents, and their insights reveal a snapshot of today's evolving fraud landscape.

Threat Level of External Fraud Risks



* Survey respondents were able to select up to three top external fraud risks.

Figure 8*

The Interplay of Account Takeover, Emerging Technology & Insider Fraud Risks

44% of our survey respondents identified account takeover (ATO) fraud as one of the greatest threats to their bank and client base in 2025 **(shown in Figure 8).** As one of the most prevalent and costliest fraud types for banks, projected losses from ATO fraud were estimated at $13 billion in 2023 in the US alone. Moreover, ATO fraud has increased in recent years. ATO fraud occurs when a fraudster gains unauthorized access to someone else's account, such as a bank, email, or e-commerce account, to steal funds, make purchases, or engage in other illicit activities. This type of fraud often begins with the theft of personal credentials—typically through phishing, social engineering, data breaches, or malware attacks—that allows the fraudster to bypass security measures and impersonate the legitimate account holder.

Therefore, ATO fraud is often linked to data breaches and identity theft, with criminals stealing customer data directly from bank systems or buying credentials on dark web marketplaces. This heightens associated insider fraud risks, as employees may be tempted to sell sensitive information to criminals or third parties, thus lowering barriers to entry for fraud and increasing opportunities for exploitation. There is also the risk of unintentional breaches or other employee actions that can leave banks vulnerable to ATO fraud. For instance, employees with privileged access can either intentionally or unintentionally enable ATO fraud by providing criminals with valuable information, such as account details or security practices.

Rise in Data Breaches

There have been high-profile cases of employees and former employees leaking sensitive data of companies, such as Tesla reporting a data breach affecting over 75,000 company employees that was due to two former employees leaking the information online. One recent study by cybersecurity company Code42 found that there has been a 28% average increase in monthly insider-driven data exposure, loss, leak, and theft events since 2021.

Generative AI also amplifies ATO risks by enabling criminals to craft highly convincing phishing messages and to automate credential testing across multiple banks. These advances allow attackers to target accounts more broadly and effectively, complicating detection and response efforts for banks. The intersection between data theft and generative AI is also an important one to note. The same study by Code42 found that 85% of respondents believed that their company's sensitive data was increasingly vulnerable to new AI technologies, including the inadvertent exposure of sensitive data by inputting into tools such as ChatGPT. This raises a potential future concern around fraudsters getting their hands on sensitive data via AI chatbots that can then be used to carry out fraud schemes. Additionally, more sophisticated phishing schemes can target employees, increasing the likelihood of an employee falling victim to a scheme and inadvertently granting access to critical systems or data, fueling additional fraudulent activity.

Additionally, fraudsters are now using automated tools to carry out credential stuffing – testing large volumes of stolen usernames and passwords, often from data leaks, to gain access to accounts more effectively. With more people also relying on mobile devices for banking and authentication, fraudsters are targeting these devices to attempt to intercept passwords and personal information.

SIM Swapping

One emerging risk is SIM swapping, which allows criminals to intercept one-time passwords and other verification codes sent via SMS, enabling them to bypass two-step authentication or other security protocols. SIM swapping, also known as a port-out scam or SIM jacking, is a type of identity theft that involves taking over a person's phone number. Often, a hacker will use information they have gathered to convince the victim's mobile carrier to reassign their phone number to a new SIM card. The hacker now has access to the victim's phone number and can intercept any calls, texts, or other communications. They can use this to gain access to the victim's online accounts, such as email and banking, by intercepting security codes.

The FBI has issued alerts that SIM swapping schemes are on the rise in the US. There have been reported cases of SIM swapping resulting in banking fraud. In one case earlier this year, a victim found out that $21,000 had been withdrawn from his account after criminals got hold of his personal information and were able to convince the victim's cellphone company to transfer his cellphone number to a new phone. The criminals were then able to bypass two-factor authentication and access his bank account on their mobile device.

Rising Sophistication of Business Email Compromise & APP Fraud

33% of our survey respondents identified business email compromise (BEC) fraud as one of the greatest threats to their bank and client base in 2025 **(shown in Figure 8).** BEC is also among the costliest forms of fraud, responsible for an estimated $6.7 billion in losses globally in 2023, or 15% of total consumer fraud losses. The FBI reports $2.9 billion in BEC losses for the US alone in 2023, with the average claim rising sharply from $84,000 in 2022 to $183,000. In BEC, criminals use social engineering and cyber-attack tactics to gain access to email accounts, using them to trick people into sending money or sharing sensitive information. Common tactics include impersonating vendors or suppliers to alter payment details, which poses a heightened risk for banks handling multiple vendor accounts. BEC attacks can also lead to unauthorized access to bank systems, exposing sensitive customer data, which increases the risk of reputational damage, regulatory fines, and client attrition.

BEC fraud is often used to target businesses to trick employees into transferring money or making payments into criminal bank accounts. In one case this year, a commodities firm in Singapore realized that it had been tricked into transferring funds into a fraudulent bank account, with criminals pretending to one of their legitimate suppliers. The firm transferred over $40 million into an account after the criminals contacted them using a slightly different email address from the supplier's official one. Such fraud cases leave commercial banks highly vulnerable as customers may fall prey to criminals impersonating vendors or third-party partners. Fraudsters are also increasingly targeting third-party vendors themselves; once inside a vendor's email system, they can launch secondary BEC scams that appear legitimate as they are coming from the actual supplier or partner account.

Emerging BEC threats are escalating as criminals adopt advanced tools like generative AI, enabling more realistic, targeted phishing and impersonation schemes that mimic the language and tone of executives, suppliers, and clients. AI also amplifies attack speed and reach, raising the probability of successful breaches across banking networks. One study by VIPRE Security Group found that 40% of all BEC email fraud targeting their customers was entirely created via generative AI. The company also found a rise in BEC schemes lacking the typical red flags that would have been used to identify BEC fraud previously, such as spelling errors and grammatical mistakes. There is also the risk of criminals using voice deepfakes to impersonate executives in phone calls, convincing employees to authorize payments and other transactions.

Specific teams within companies may be more prone to being targeted. For instance, fraudsters are now targeting payroll departments with compromised or stolen employee credentials, looking to reroute direct deposits and other payments related to employee salaries. With more employees working remotely, criminals can exploit lack of communication or familiarity. Moreover, criminals can exploit weaker home network security and the use of personal devices to compromise email accounts, initiating BEC attacks from these compromised devices.

Infiltration of Company Communication Platforms

Fraudsters are increasingly targeting internal communication platforms such as Slack, Microsoft Teams, and project management tools such as Trello. If criminals successfully access such platforms and tools, they can initiate BEC schemes that are directly from trusted, internal sources. It was revealed in October that the ransomware group Black Basta had begun targeting internal platforms including Microsoft Teams. By impersonating IT support on these trusted platforms, Black Basta was able to bypass traditional external security measures and gain access to company networks. This marks a worrying trend at the intersection of fraud and cybersecurity, where attacks driven by external actors can actually come from within as much as from outside an organization. Employees are more likely to have their guard down when engaging with people within their internal systems, thus helping increase a fraudster's rate of success. Once an employee is successfully targeted, the fraudster uses remote-access tools to take control of that employee's device, at which point they can carry out fraud and data theft attacks.

More sophisticated BEC schemes targeting companies also increase the risk profile for commercial banks criminals often facilitate payments that use banks' networks. Additionally, as BEC often exploits vendor and partner relationships, banks may face risks if any linked organizations in their supply chain experience a BEC incident. BEC vulnerabilities can spread through networks, potentially exposing sensitive banking information.

A key goal of BEC fraud is often authorized push payment (APP) fraud. APP fraud is a more general term that encompasses other forms of authorized payment fraud, such as investment or romance scams, that use building a direct relationship with the victim through social engineering tactics. APP fraud has garnered a lot of attention across the financial industry in recent years, with banks and regulators alike looking to address this pervasive fraud type. In fact, the UK's new APP Reimbursement Rule went into effect in October, but more on this later.

APP fraud losses in the US and UK are projected to reach $5.25 billion by 2026. Like other forms of BEC fraud, APP fraud has grown more complex in recent years, with criminals exploiting communication platforms and social engineering tactics to convince victims to authorize payments willingly. Today, 77% of APP fraud originates from online targeting of victims. Fraudsters also often use personal information obtained from data breaches, similar to ATO fraud, to carry out attacks. Attackers often also do research on victims, posing as trusted individuals within a victim's network.

Fraudsters also often look to impersonate authority figures. A common tactic on the rise in recent years is criminals posing as bank employees, warning victims of fraudulent activities to trick them into transferring money to secure accounts, which are in reality controlled by the criminals. Like other forms of social engineering tactics, generative AI can be used to make these impersonations more believable.

Despite all this, only 24% of our respondents identified APP fraud as one of the greatest threats to their bank and clients in 2025 **(shown in Figure 8).** This is very interesting and could be reflective of just how prominent and all-consuming the other threat types are for banks at the moment. It could also be because banks may feel more attention has been paid to APP fraud in recent years and, therefore, they understand the threat better and are potentially more prepared for shifting dynamics across APP fraud.

Mobile Banking's Boom and the Surge in Mobile Malware

Mobile banking has surged in popularity in recent years, particularly among younger users, as more consumers opt for the convenience of mobile apps over physical bank branches. In 2023, 81% of consumers accessed mobile banking at least once a month in the US. The mass adoption of mobile-first banking, however, means more fraudsters will likely target mobile banking vulnerabilities. In fact, the volume of mobile banking fraud cases was up 62% according to UK Finance members, and for the first time ever, was higher than the volume of web-based banking cases.

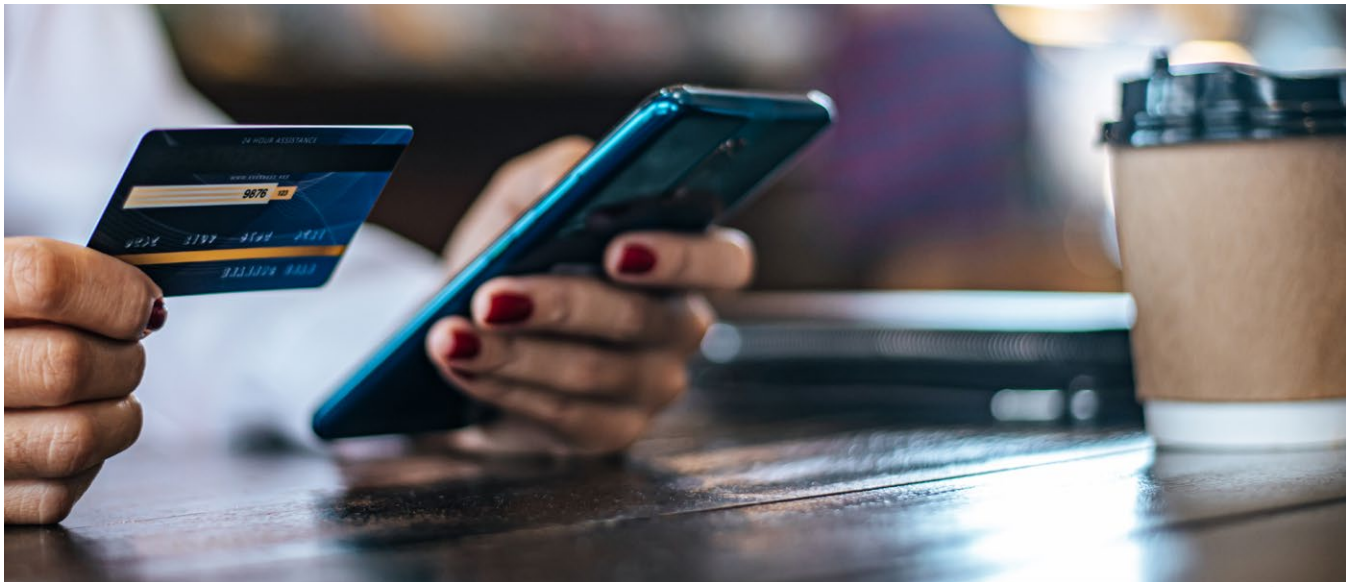
Cybercriminals are increasingly exploiting mobile vulnerabilities to carry out fraud, including through phishing and malware schemes. The FTC highlights, for instance, that as fraudsters adopt more sophisticated digital tactics, they are getting increasingly good at defrauding mobile banking users. The targeting of mobile banking opens the door to a range of fraud risks, as more mobile banking apps are offering higher-risk services such as cryptocurrency and digital asset access, and cross-border and instant payments.

While banks implement biometric authentication and other security measures to protect mobile banking offerings from fraud, criminals are getting more savvy at targeting these measures. The rise of more sophisticated mobile malware is a particular concern as bad actors can bypass traditional security measures to gain access to bank apps or a user's device itself. Criminals often gain access through texts or emails that contain a malicious link. Criminals are also now turning more towards fake banking apps and spoofed interfaces, delivering malware via essentially trojan malicious apps that are disguised as legitimate ones. Fake malicious banking apps have been found on app stores such as Google Play.

Adware is another major risk, with victims redirected to unwanted websites and promoted to install malicious apps. Another risk is hackers using QR codes or mobile payment requests, notably on Venmo or other apps, to direct victims to malicious links. Unsuspecting victims then may log in to these fake websites, where fraudsters can then steal their information. As discussed earlier, SIM swapping is another potential technique used by fraudsters to target mobile devices. These tactics can be used to access banks accounts and carry out unauthorized transactions. As banks continue to consolidate various services into one single app, known as "super apps," the potential scope of fraud carried out on these apps will expand.

Enduring Risks: The Persistent Threat to Traditional Payment Types

While digital threats such as malware and phishing schemes are, in large part, dominating banking fraud today, fraud targeting more traditional payment types and banking services such as credit cards or checks remains a persistent and evolving risk. It is important for banks to continue investing attention and resources into protecting these more traditional payment forms from fraud schemes. Moreover, criminals now leverage new technologies to enhance their effectiveness at targeting checks and credit cards, combining familiar methods with new enhanced tools and tactics. This means the threat landscape for these traditional payment methods can be as dynamic as the threats stemming from newer financial services and payment forms.



A key traditional fraud type to pay close attention to is check fraud, which has increased over the last few years in the US, despite checks being on the decline. Some estimates place check fraud losses at $21 billion in the US in 2023. Suspicious activity reporting for check fraud more than tripled in the US from 2018 to 2022 as well and continued to grow in 2023. Check fraud SARs increased more for personal or business checks than for any other financial instrument during this time. Various factors have led to a resurgence in check fraud. The US Treasury Department, for instance, points to financial institutions' limited capacity to verify the legitimacy of checks in a timely manner, the lack of self-verification systems built into checks, and the prevalence of remote capture technology as key drivers. The rise in this type of fraud can present a particular concern for commercial banks catering to small businesses, which may be more likely to use checks to pay vendors or other business expenses. Indeed, the US Treasury has stated that criminals actively target checks from businesses due to the perception that these accounts are less likely to bounce.

A key emerging threat is the use of messaging platforms such as Telegram and other online spaces to purchase stolen checks, creating an environment where it is harder to trace back the original source of the stolen check and fraud networks. The combination of this traditional paper form of payment with today's online fraud ecosystem is an interesting one, as it highlights how technology and social media can impact even the most traditional forms of fraud. Moreover, as more advanced ways to remove the original ink on a check or photoshop a check are developed, the risks become even more pronounced.

The Increasing Sophistication of Counterfeit Check Fraud

Another threat is the use of counterfeit or forged checks, which are produced using advanced printing techniques and software to replicate the look and feel of real checks. As technology improves, the ability to create highly realistic counterfeit checks increases. Generative AI could potentially be used to create images of realistic looking checks. This can be combined with fake identities created from generative AI as well to create "drop accounts" to deposit the checks into. Fake ID tools using generative AI have already popped up online, such as OnlyFake which let anyone quickly and easily generate convincing ID documents. Last year, US authorities uncovered an organized crime scheme using forged checks and stolen identities to defraud banks. The criminals would present fake identities to evade detection by law enforcement and to create debts under other names besides their own.

Credit card fraud also remains a major risk globally, with some estimates pitching card fraud losses at $165.1 billion over the next 10 years in the US alone. In 2023, 60% of credit card holders experienced attempted fraud, according to Experian. Our own survey found that credit card fraud is still a concern to respondents, with 38% viewing it as one of the greatest external fraud risks to their bank and clients in 2025.

Some credit card fraud involves lost and stolen credit cards; however, the majority increasingly involves digital methods, where the card is not actually present. This often happens when someone has been able to steal personal and card information through phishing or account takeover schemes, for instance. Skimming is a key tactic for carrying out credit card fraud, which involves criminals illegally placing devices on ATMs or point-of-sale terminals to steal card information. Moreover, experts point to data breaches as a major driver in credit card fraud; for instance, the National Public Data breach which reportedly exposed millions of personal data records, including credit card information.

Unlocking Future Threats: The Growth of Open Banking

The rise of open banking is transforming the financial landscape by fostering more transparency, efficiency, and innovation, as banks and third-party providers collaborate to offer consumers more personalized and seamless financial services. However, open banking does bring with it new fraud challenges. As already discussed, 59% of our survey respondents see the rise of open banking as a banking service trend that has particularly high potential to increase their bank's fraud exposure. **(shown in Figure 5)**

What are these risks? For one, open banking relies heavily on APIs (Application Programming Interfaces) to facilitate data sharing between banks and third-party providers. Poorly secured or misconfigured APIs can be exploited by fraudsters to gain unauthorized access to sensitive financial data or initiate fraudulent transactions. The sharing of sensitive financial information increases the risk of, and the potential damage caused by, data breaches, where unauthorized parties could gain access to personal and account data. Account takeover attempts may increase, with fraudsters attempting to exploit weaknesses in authentication processes. Moreover, if third-party applications and APIs are not secure, they may become targets for hackers who then use personal data to carry out fraud schemes.

Fraudsters can also exploit the increased number of parties involved in open banking to launch phishing and social engineering attacks aimed at non-banks, as some of these companies may be less aware of fraud risks and techniques. Criminals may also impersonate legitimate third-party providers or banks to attempt to trick customers into revealing their login credentials. With multiple parties having access to an individual's financial data, there is also a heightened risk of ATO fraud, where criminals could compromise a third-party provider or API endpoint. Another potential future threat could be the use of fake third-party applications that appear legitimate to users.

Open banking also enables more efficient cross-border transactions and data sharing, which increases exposure to international fraud risks and heightens the risks related to cross-border payments. Fraudsters can potentially exploit varying regulations and security measures, for instance, to target users in different regions, complicating fraud prevention efforts.
All these trends demonstrate the overlapping nature of fraud trends, as open banking may potentially create new risk exposure for banks relating to ATO fraud, data breaches, cross-border fraud, and other trends already discussed thus far in the report. As open banking evolves and becomes more common, banks must understand the direct impact of this technology on fraud risks.

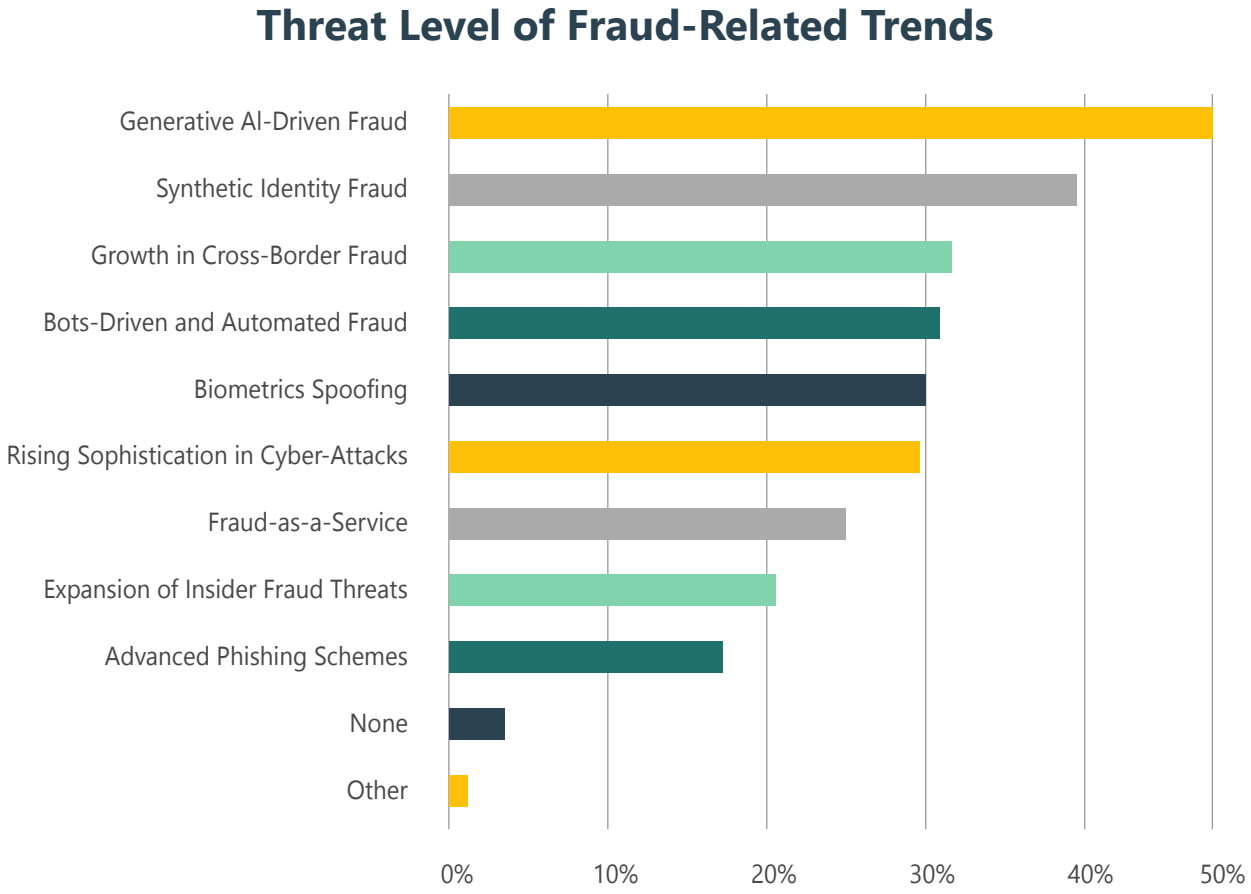


Figure 9

* Survey respondents were able to select up to three top trends.

Synthetic Identity Fraud as a Growing Tactic of Choice

The rise of open banking also overlaps with another key fraud threat – synthetic identity fraud. Synthetic identity fraud is the fastest-growing financial crime in the US, with some estimates placing the cost to banks globally at over $20 billion. Nearly 40% of our survey respondents believe synthetic identity fraud will pose one of the greatest threats to their bank in 2025 **(shown in Figure 9).** This threat is primarily due to the complexities it presents for detection. In fact, one study estimates that 95% of synthetic identities are not detected during the onboarding process at financial institutions.

Unlike traditional identity theft, which involves stealing a 'real' person's data and identity, synthetic identity fraud combines real and fake information to create new, fictitious identities. Criminals often use these synthetic profiles to open accounts, establish a fake business or credit history, and carry out financial transactions. A recent Wakefield Research report commissioned by Deduce indicates that synthetic identity fraud is accelerating, driven by an environment where gaps in both digital and traditional identity verification provide fertile ground for exploitation.

Synthetic identity fraud is likely to escalate in 2025 and beyond, as criminals become more adept at navigating financial institutions' patchwork of digital and paper-based verification systems. Large-scale data breaches provide useful information for criminals to utilize when creating synthetic identities. Furthermore, generative AI can be used to produce highly realistic synthetic data that can pass through standard identity verification processes, including realistic names, addresses, and even potentially synthetic biometric information such as videos or voices.

As cybercriminals continue to exploit these gaps, many commercial banks may find that their current identity processes, largely dependent on government-issued identifiers and other legacy verification systems, are insufficiently agile. Moreover, with the expanding digital economy and growing reliance on remote services, the creation of synthetic identities is poised to become even easier. This is because online onboarding and account opening, highlighted earlier in this report as an important trend across the banking fraud landscape, create an opening for the use of synthetic identities.

Synthetic Identity Bank Fraud Scheme

The US has brought various cases against criminals using synthetic identity techniques to carry out fraud against commercial banks. In one case, authorities uncovered an organized scheme using stolen and synthetic identities to defraud numerous banks. In this scheme, an individual was offering a "credit repair service" where clients paid him a fee for supposed services to help improve their credit history. In reality, however, the individual built a network of co-conspirators and took advantage of clients, creating fictitious credit profiles and fraudulently altering client credit data using fictitious police reports. Moreover, the defendant opened credit accounts in the name of fraudulent identities, then cashing out the accounts and thus defrauding the bank at hand. These fake identities were created using a stolen social security number along with made-up personal information. All in all, the scheme resulted in over $3.4 million in losses.

Rise of Generative AI, Deepfake & Biometric Hacking Fraud

50% of our survey respondents identified generative AI-driven fraud as one of the trends posing the greatest threat to their bank in 2025 **(shown in Figure 9).** This reflects the increasing sophistication and accessible nature of deepfake technology today. Initially recognized for its use in creating hyper-realistic videos, deepfake technology has now expanded to include fake audio, images, and even text. The risks associated with these advancements are substantial.

2023 saw a reported 700% increase in deepfake incidents alone. There have been various high-profile cases, such as that of UK engineering group Arup, which lost $25 million after fraudsters deployed a digitally cloned version of the CFO during a video call to trick an employee into transferring money. In another case, scammers unsuccessfully impersonated the CEO of the public relations firm WPP using a fake WhatsApp account, a voice clone, and YouTube footage in a virtual meeting. Luckily in the latter case, the targeted employees were able to identify it as a scam, perhaps signaling the growing awareness across industries of the risk of deepfake impersonation scams.

Notable Advancements in Deepfake and Generative AI Tools

A recent advancement was highlighted earlier this year when OpenAI introduced an audio feature capable of recreating a human voice from just a 15-second clip, even in foreign languages (it has withheld the release of this technology due to concerns regarding potential misuse). The company also unveiled a system named Sora, which generates high-quality, realistic videos from simple text descriptions, further illustrating the growing capabilities of technology and associated vulnerabilities to misuse for deepfake creation. One of the critical challenges posed by modern AI-enabled deepfakes is their self-learning capability, where they are continuously improving.

OpenAI has itself highlighted deepfake audio's potential misuse to impersonate an individual and facilitate transactions such as payments or unauthorized access to sensitive data and systems. As deepfake technology grows more accessible and sophisticated, voice and image-based biometric authentication security measures could become more obsolete. Generative AI, for instance, can create highly convincing fake IDs, which can, in all likelihood, successfully bypass banks' ID verification processes to gain access to accounts. Criminals have also started using AI-generated face-swap videos to attempt to evade more in-depth biometric security protocols, which will be discussed in more detail below.

There is also an increasing concern over the use of deepfake and generative AI for biometric hacking and spoofing – a type of attack where a criminal can access unauthorized biometric data, or create fake or altered data, to bypass identification security protocols. This type of fraud is becoming more prominent as fraudsters find new ways to bypass security protocols. The still newer nature of this trend but increasing relevance of it is highlighted by our survey respondents, with 30% believing it will pose one of the top threats to their banks in 2025 **(shown in Figure 9).** Going forward, attackers may use stolen or intercepted biometric data to evade authentication systems, which can be rendered vulnerable by flaws in hardware, software, or implementation.

A study by the cybersecurity firm Sensity found, for instance, that "liveness tests" used by banks to help verify users' identity can be fooled by deepfakes, highlighting the vulnerabilities of these systems. The firm tested various liveness test systems using deepfake videos and found that nine out of the 10 were extremely vulnerable to deception. Different biometrics have varying ranges of susceptibility to spoofing and impersonation; for instance, more active methods, such as fingerprint identification, tend to be harder to spoof, whereas passive methods, like images, leave more room for fraud.

Types of Biometric Spoofing

Print: The simplest form of spoofing, criminals use a printed photograph of the target's face to trick facial recognition systems. This can be effective against less sophisticated systems but not more advanced systems.

Video: Criminals record a video of the target person's face and play it back in front of a camera. This approach is often more successful than a print attack since it incorporates motion, which many facial recognition systems require.

Deepfake: Criminals use deepfake technology to create a video of a target's face, which can create convincing facial movements and expressions, making it difficult for some facial recognition systems to differentiate between real and fake.

The Rise of Fraud-As-A-Service, Automated Fraud & AI-Enabled Hacking

Bot-driven and automated fraud techniques are rapidly increasing, significantly escalating both the scale and speed of attacks. These sophisticated methods allow fraudsters to launch high-volume attacks with minimal human intervention, bypassing traditional security measures and quickly exploiting vulnerabilities. This threat is recognized by our survey respondents, with almost 35% of them believing that bot-driven and automated fraud will pose one of the greatest threats to their bank in 2025.

Another associated risk that is also emerging comes from the rise of "fraud-as-a-service" (FaaS), which enables fraudsters to subscribe to tools, resources, and services that are designed for executing fraud. This criminal service model makes fraud methods more accessible, allowing even inexperienced criminals to orchestrate complex attacks with minimal effort (for instance, FaaS can provide tools for creating synthetic identities or carrying out phishing attacks, or provide access to dark-web stolen data marketplaces). Reflecting the growing threat, 25% of our survey respondents believe that fraud-as-a-service will pose one of the greatest threats to their bank in 2025 **(shown in Figure 9).**

Automated bots are increasingly used in credential stuffing attacks, as already discussed, where stolen login credentials from data breaches are tested across multiple sites. FaaS providers offer credential-stuffing services to clients, making it easy for criminals to conduct mass login attempts on banking apps or websites. There has also been a notable increase in bot-driven password reset attacks, which fraudsters often use to attempt to log into banking and other financial accounts.

Another interlinking trend is between FaaS and ATO fraud, as FaaS providers can offer automated tools specifically designed to perform account takeovers. These tools help fraudsters compromise bank and payment accounts, enabling unauthorized transactions. Specialized bots are used to automate "carding" attacks, where fraudsters use stolen payment card information to make small test purchases. Moreover, FaaS providers may also offer bots that can conduct phishing attacks to carry out BEC and APP fraud, among other phishing attacks.

As the tools driving automated and FaaS fraud continue to grow more sophisticated, these threats could outpace current bank defenses. AI and machine learning in particular can potentially be used to refine fraud tactics and prolong the effectiveness of FaaS tools. Moreover, as bots are more effectively integrated into other fraud schemes, the risks presented by these fraud types will likely unfortunately increase. Banks much therefore stay vigilant and safeguard against these automated fraud types.

The rapid advancements of these tools, coupled with criminals abusing AI to write malware and other malicious codes, means we will likely see the deployment of more sophisticated hacking attacks by criminals with more rudimentary backgrounds. This risk is reflected in our survey responses, with 40% of respondents forecasting that hacking attacks will be a top threat to their bank and clients next year. Threat actors may also increasingly be able to use advanced AI-based tools that are typically used for cyber defense by developers and testers to discover vulnerabilities and identify weaknesses in a bank's system, network, and security measures. This creates a real vulnerability for banks, as they will need to AI-proof their security systems.

Chapter 4: Navigating An Evolving Regulatory Landscape

Today's fraud landscape is marked by increasing regulatory scrutiny and stronger enforcement. Understanding these compliance expectations is vital, as global regulators are intensifying their focus on internal controls and leadership in fraud prevention. Overall, banks largely welcome these changes; **60%** of our survey respondents believe that recent fraud-related regulations have improved their fraud detection and prevention efforts, with only **5%** feeling the changes hindered their efforts; **35%** saw no impact **(shown in Figure 10).**

Proactively staying on top of compliance trends is crucial to navigating this complex landscape, mitigating risks, and adapting to evolving requirements. Moreover, as banks increasingly integrate AI into their compliance and fraud prevention frameworks, attention must also be paid to emerging regulations around AI development and governance. Regulators are focusing on ensuring AI is used ethically, transparently, and in a manner that is explicable. Key regulatory changes in the fraud space to consider as 2025 kicks off are highlighted below.

Impact of Fraud-Related Regulations on Banks' Approaches to Fraud Detection and Prevention

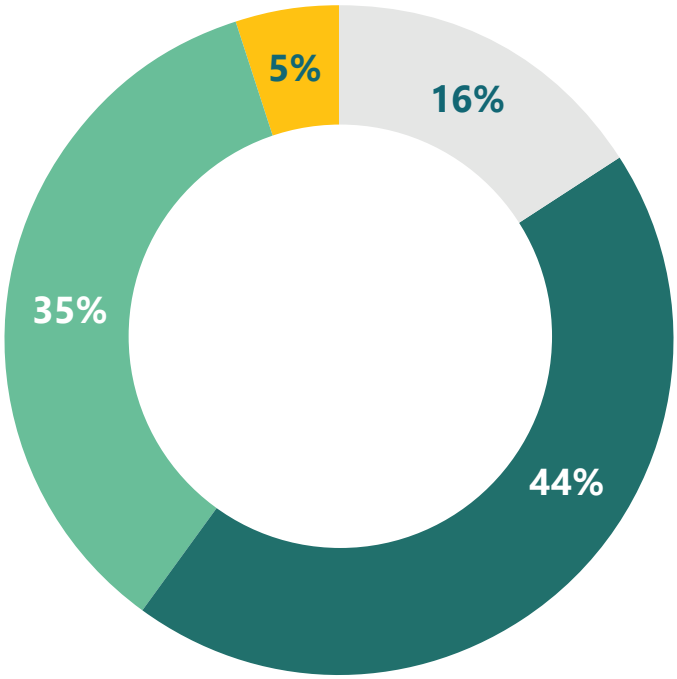


Figure 10

A Snapshot of US Regulatory Updates

The Federal Trade Commission (FTC) finalized in April its Government and Business Impersonation Rule, which aims to protect consumers and businesses from scams where fraudsters impersonate government agencies, businesses, or other organizations to gain sensitive information for fraud purposes. The rule holds significant implications for commercial banks, as it imposes stricter liability on entities that fail to protect consumers from impersonation scams. Banks may face heightened scrutiny for their policies and security measures, including their authentication protocols.

The Consumer Financial Protection Bureau also issued its long-awaited open banking rule in October, as part of today's broader push towards open finance. The new rule will be a major shift in the way banks share data and engage with third-party service providers, as it requires commercial banks to facilitate data-sharing with authorized third-party providers at the request of customers. It outlines data safety and protection requirements for open banking, including compliance checks and audits to ensure customer data remains secure, even when accessed by third parties. With open banking unlocking a new world of potential data security issues, this rule is crucial in ensuring the banking sector has alignment in its security practices. Some commentators on the rules expressed concern that an obligation to make data available to third parties could open the door to fraud and security breaches.

A Snapshot of UK Regulatory Updates

The UK's new and highly anticipated reimbursement rules for APP fraud came into effect in October 2024 and mark a landmark development, requiring UK payment service providers to reimburse customers who fall victim to APP fraud. The rule outlines mandatory reimbursements for consumers, microenterprises, and charities of up to £85,000. Both sending and receiving payment providers will share responsibility for reimbursements. While the new reimbursement scheme primarily focuses on individual consumer protection currently, there are discussions about possibly extending similar protections to businesses in the future.

As the new rule shifts the burden of APP fraud losses from customers to banks, the financial liability and impact of APP fraud will be more greatly felt. Banks in the UK must now consider not only the operational costs of fraud prevention and detection, but reimbursement as well. This makes it all the more necessary for banks to have the most effective anti-fraud measures in place. Banks may also look to better educate their customers to try and reduce the number of successful APP fraud attempts. Stricter verification and authentication protocols will also be incredibly important.

The new regulation has also sparked a debate between many banks and technology companies over liability and fraud prevention. Banks have previously pointed to the fact that despite fraudsters often time targeting victims of APP fraud via social media platforms, only banks are currently liable for reimbursement. This begs the question of the point at which fault or liability should be assigned in a fraud scheme. More banks are calling for social media and other tech companies to do their part in financially compensating victims who fall for schemes that involve their social media and messaging platforms.

In a move championed for helping facilitate coordination between the banking and technology sectors on fraud prevention, the UK's Online Fraud Charter outlines a voluntary agreement between the government and the technology sector to reduce fraud on their platform and services. Signatories of the Charter agree to taking proactive steps to prevent fraud on their respective platforms, including working with the UK government and enforcement bodies directly. Key technology companies including Google, Meta, Snap Inc., Microsoft, and X have signed on. The UK Online Fraud Charter is highly relevant to commercial banks, as it mandates a coordinated effort between financial institutions, telecom providers, tech companies, and government entities to tackle online fraud. For commercial banks, the charter outlines key responsibilities and encourages proactive measures to protect consumers and reduce financial losses, including understanding emerging fraud trends and anti-fraud strategies. Intelligence and data sharing are encouraged, to help coordinate responses across sectors.

Last month, the UK released long-awaited guidance on its new "failure to prevent fraud" offense under the Economic Crime and Corporate Transparency Act 2023. Going into effect in September 2025, the law can hold large organizations criminally liable if an associated person commits fraud to benefit the organization or, in some cases, its clients. The offense is effectively one of strict liability, with organizations liable even if they were not aware of the fraudulent activity. Organizations can, however, defend themselves by demonstrating that "reasonable procedures" to prevent fraud were in place at the time of the fraud, but guidance leaves these procedures undefined, placing the burden of proof on organizations.

The law applies to large organizations across all sectors of the UK economy, including the financial sector. 'Large' is defined as meeting at least two of the following criteria: more than 250 employees, more than £36 million turnover, and/or more than £18 million in total assets. Associated persons can include employees, agents, subsidiaries, or service providers. Fraud that takes place outside of a work capacity does not give rise to corporate liability.

The guidance does outline six principles for designing and maintaining a fraud prevention framework. These include top-level commitment to fraud prevention through proportionate anti-fraud measures, effective training, a supportive reporting culture, and robust whistleblowing protections. Overall, the law encourages more organizations to implement or improve prevention procedures, with the aim of driving a major shift in corporate culture to help prevent fraud.

Failure to Prevent Fraud Guidance – Illustration of Associated Person

The following is an example given in the guidance on who is an associated person. Bank C uses Bank D to provide clearing services. In the course of these clearing services, Bank D (corporately, with the knowledge and involvement of its senior management) commits a fraud that benefits Bank C's clients. For the purpose of this offence, Bank D is an associated person of bank C. Bank C is the relevant body that could be liable for the offence under clause 199(1)(b) unless a court decides that it had reasonable procedures in place to prevent the fraud.

A Snapshot of International Updates

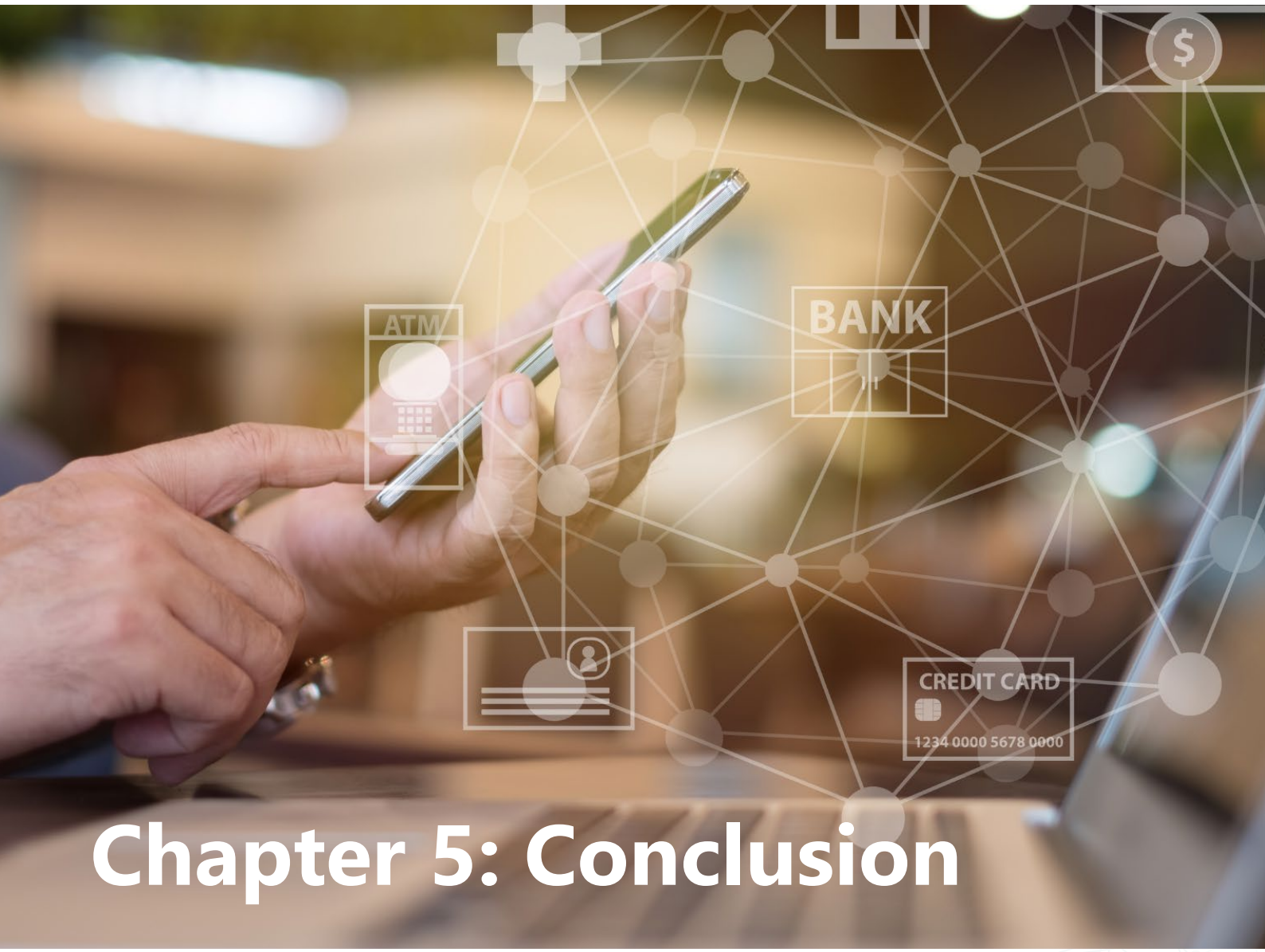
The EU adopted its latest package of new AML rules earlier this year. These rules included regulation harmonizing AML rules for the first time throughout the EU, closing loopholes including for fraud. For example, the new rules require financial institutions to implement more robust fraud prevention protocols for high-risk transactions, such as large transfers or transactions involving new accounts. The new reforms also intend to enhance cross-border cooperation and intelligence sharing, to help better combat fraud and other financial crime risks.

The EU's Third Payments Services Directive (PSD3) will likely come into effect in 2026, with the directive's initial draft currently in review. Building on the EU's current Second Payments Services Directive (PSD2), the latest version focuses on improving customer protection requirements, improving open banking accessibility and adoption, and increasing transparency in cross-border payments. A new Payment Services Regulation (PSR) will come alongside PSD3, with the aim of creating a two-pronged approach to strengthening protections and transparency across the banking sector. While the directive is not yet final, banks can take steps to prepare for likely changes, such as likely mandatory payee verification and increased reporting requirements for cross-border payments.

Canada has also had key regulatory updates in the fraud space over the last year. It has continued to enhance anti-fraud measures in its financial sector, focusing on strengthening cybersecurity defenses to prevent financial fraud. The Bank of Canada and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) have been updating their guidance on detecting, reporting, and preventing fraud, particularly in relation to money laundering and terrorist financing. The Financial Consumer Agency of Canada (FCAC) has also issued new guidelines to financial institutions, emphasizing the need to detect and respond to fraudulent activities like phishing, account takeovers, and unauthorized transactions. This also includes increased monitoring of digital and online transactions, which have seen a rise in fraudulent activities.

What Does All This Mean?

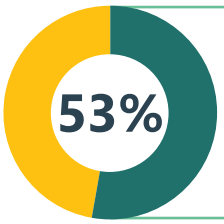
As regulatory frameworks and requirements related to fraud continue to evolve, banks face mounting pressure to allocate increasing resources to fortify their fraud defenses. Stricter legal and compliance frameworks, and enhanced legal and even financial liability, demand more sophisticated systems, processes, and personnel to meet heightened expectations. Failure to comply not only risks substantial penalties but also jeopardizes reputational integrity, making it imperative for banks to stay ahead of evolving regulations. These requirements will continue to shape the financial sector, making investment in technology and expertise to mitigate risks even more important to safeguard against fraud.



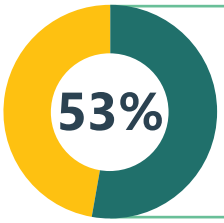
Chapter 5: Conclusion

So, how can we work with this knowledge on the latest fraud trends? It is important to build a holistic risk management strategy that enables proactive threat detection. Keeping banks safe demands a multifaceted approach – one that blends advanced technology, strategic collaboration, and forward-thinking governance to ensure the security and resilience of banks and today's financial system. A key part of this is understanding what challenges banks face in building and implementing effective anti-fraud strategies.

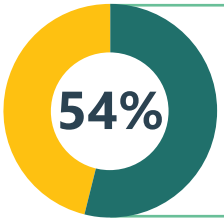
Our survey respondents identified the following as key challenges as we kick off 2025:



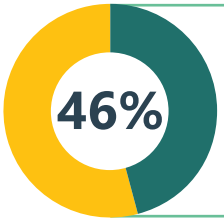
53% identified the cost of integrating new fraud prevention and detection technologies as a key challenge.



53% also identified the difficulty of integrating new fraud prevention and detection technologies due to incompatibility of existing systems or resistance by management as a key challenge.



54% highlighted the cost and time involved in training staff to use new fraud prevention and detection tools



46% underlined the difficulty of ensuring staff keep abreast of new fraud techniques and red flags.

Harnessing the Power of Technology and Data

In the face of today's escalating fraud threats, adopting cutting-edge technologies is no longer a matter of choice but an essential component of fighting fraud in commercial banking. Advanced tools enable banks to more effectively detect, investigate, and prevent both internal and external fraud threats. Despite this, 62% of our survey respondents find their current fraud prevention and detection technologies only 'somewhat' effective at addressing insider and external fraud risks simultaneously, which is a major gap in anti-fraud efforts. A key problem is the siloed nature of many anti-fraud technologies in only addressing either insider or external fraud, instead of addressing the potential interconnectedness of these fraud types.

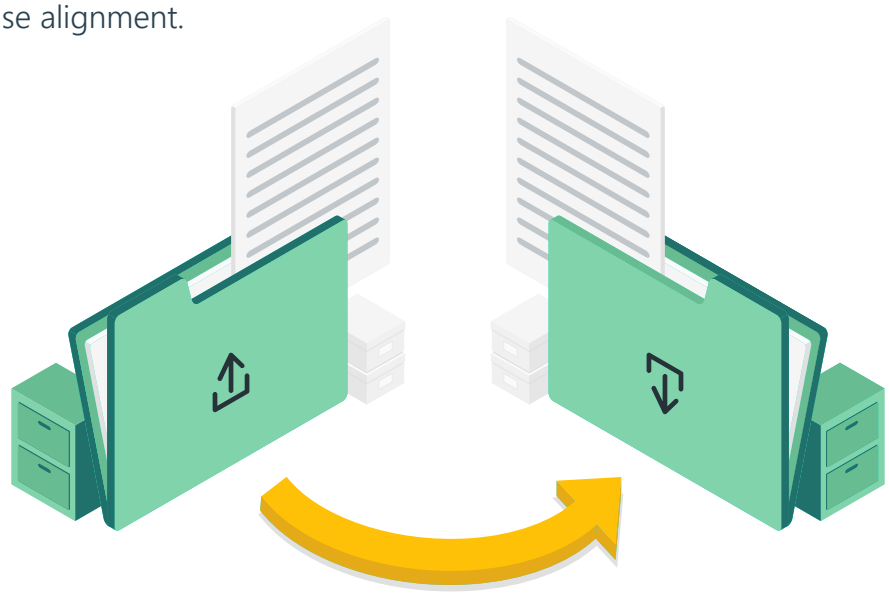
More firms are embracing AI-enabled solutions, including for fraud detection and prevention, as well as screening, transaction monitoring, and automated reporting to regulators, according to a study by Comply Advantage. In fact, a recent survey found that banks were significantly ahead of other industries in terms of AI adoption. This is a very positive development, as the latest cutting-edge technology must be leveraged to improve our fraud defenses.
Just as fraudsters are employing the latest technology for their illicit activities, so should we. From better spotting patterns and anomalies to more streamlined reporting and communication, banks must be at the forefront of AI integration. With advanced analytics and machine learning, solutions can help banks better identify unusual behaviors that could damage business and harm clients. By analyzing large volumes of data in real time, banks can identify patterns that are indicative of potential fraud. Technology can be used to flag suspicious activity and enhance investigations, allowing banks to correlate data across multiple channels and timelines, tracing the origins of complex fraud schemes.

Alongside detection, technology also strengthens protection. For instance, despite the new risks that biometric authentication and other new security protocols can create, they do offer considerable protection. This demonstrates once again just how dual-edged technology is today. But it is important not to get discouraged by this. By investing in the latest technology and integrating it more effectively into fraud defenses, banks can help prevent fraud by using the very technology that criminals are looking to exploit, thus beating criminals at their own game. For example, behavioral analysis can help secure customer accounts against unauthorized access, reducing the risk of identity theft and social engineering attacks. These tools also protect banks from internal threats – such as employee collusion – as much as external threats.

Technology is only as powerful as those who use it, however. There is much progress to be made in how banks leverage and integrate technology. For example, 70% of our survey respondents find that their bank's processes and teams interact and coordinate somewhat effectively to prevent and detect both insider and external fraud. While this is good, only 16% found that their teams interact and coordinate very effectively, with 10% finding their teams were ineffective in this regard. There is much room for improvement here.

Importance of Data Sharing & Awareness Building for Holistic Approach

It is important for banks to adopt a multi-pronged approach to fraud prevention to keep pace with emerging trends and risks, building on technology and in-house systems. Industry-wide working groups and information sharing initiatives are crucial as they can provide new insights into key risks and red flags. Collaboration with law enforcement and regulators is also important. Banks have highlighted both private-to-private and public-to-private collaboration models as key areas that could drive greater effectiveness in crime fighting efforts, according to Nasdaq's 2024 report. Moreover, coordination with other industries is paramount, as fraud is not a 'one industry problem,' nor does it occur in a vacuum. Cross-industry coordination can thus help stop fraud in its tracks before it gets to the point of any loss in money. These various initiatives help decrease siloes and increase alignment.



Moreover, training and awareness-building initiatives are an important element of an effective defense. To best utilize the latest anti-fraud technologies, highly skilled teams with a strong understanding of fraud threats are essential. Indeed, Comply Advantage's State of Financial Crime 2024 report found that many banks are increasing their compliance budgets with a clear focus on investing in personnel, technology, training, and enhancing capabilities. Many of our survey respondents highlighted the importance of training, too. There is also a great opportunity for better coordination around preventative measures between banks and their customers. There can be a lack of awareness among customers of the latest risks and red flags. Customers can also be encouraged to report suspicious behaviors or trends they are seeing themselves. Banks would do well to invest more in proactive, preventative measures that help spread awareness of the latest risks and how technology today impacts the fraud risk landscape.

Final Takeaway

Despite the various fraud trends identified by our survey respondents, there is much to be hopeful of as we kick off 2025. The commercial banking sector is one of the most proactive in terms of recognizing and mitigating fraud threats as they emerge. This report can serve as a helpful guide as banks look to employ the latest technology and approaches to fraud threat management, which can thus result in better detection, prevention, and investigation of both internal and external fraud.

THEMIS

Themis helps clients identify and manage their specific financial crime risks, through a combination of innovation, insight and intelligence. Our cutting edge platform helps organisations understand these strategic threats through an ESG and socio-economic lens and protects their clients, suppliers and 3rd parties from criminal attacks or association. Founded, developed and delivered by financial crime subject matter experts.

Contact us

UK: +44 (0) 20 8064 1724
UAE: +971 267 67453
info@wearethemis.com
www.wearethemis.com

Bottomline

Bottomline makes complex business payments simple, smart and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, and state of the art fraud detection, behavioural analytics and regulatory compliance solutions. Thousands of corporations around the world benefit from Bottomline solutions. Headquartered in Portsmouth, NH, Bottomline delights customers through offices across the U.S., Europe, and Asia-Pacific. For more information, visit www.bottomline.com

Corporate Headquarters
325 Corporate Drive
Portsmouth, NH 03801
United States of America
Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
Fax: +1-603-436-0300
info@bottomline.com

Europe, Middle East, Africa
Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom
Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
Fax: +44-118-982-2253
emea-info@bottomline.com

Asia Pacific Headquarters
Level 3, 69-71 Edward Street
Pyrmont, Sydney NSW 2009
Australia
Tel: +61-2-8047-3700
Fax: +61-3-9824-6866
apac-info@bottomline.com

Connect with us

REV US061422LM

Bottomline