NC Banking Institute Panel

Fraud in Financial Services: New Technology and Mitigating Liability

February 19, 2025

Moderator

Barbara Meeks
Chapman and Cutler LLP

Panelists

Jason Chorlins
Kaufman, Rossin & Co.

Caterina Petrucco-Littleton
Federal Reserve Board of Governors

Melissa Cohen
Protiviti

Michael Shaw
JPMorgan Chase

Fraud in Banking – Current Landscape

Overview

Fraudsters will use Gen AI, synthetic identities and new tactics to increase and perpetrate fraud in 2025. Macroeconomic conditions significantly influence the trajectory of fraud trends. In times of economic instability or decline, there is a heightened risk of fraudulent activities as criminals exploit individuals under financial strain.

Current issues such as rising interest rates, inflation, and imminent student loan repayments continue to evoke concern among people. The increased vulnerability can lead to higher susceptibility to fraud as individuals navigate their challenging financial circumstances.

- Fraudulent activities are the number one criminal activity around financial crime in many countries.
- In 2023, consumers reported losing more money to **bank transfers and cryptocurrency** than all other methods combined.
- A report by **Nasdaq and Oliver Wyman** found that Fraud cost almost **half a trillion dollars** in 2023, including close to **$450 Bn from payments, check & credit card fraud** and more than **$40 Bn in scams** targeting individuals and companies.
- According to **Alloy's 2024 State of Fraud Benchmark Report,** nearly 60% of banks, fintech's, and credit unions lost over **$500K** in direct fraud losses in 2023.
- Credit Card Fraud has a projected global loss of $43 billion by 2026.
- Banks and other financial service institutions are taking steps to combat fraud by implementing advanced technologies such as **AI, machine learning and biometrics**. However, fraudsters are also constantly finding new ways to bypass these measures.

Reasons for the increase in banking fraud

- There are a few reasons for the increase in banking fraud risk, including the **shift toward digital banking**. It provides more opportunities for fraudsters to access sensitive information and accounts such as banking details.
- Additionally, **online banking is less secure**. Banks & FIs are constantly adapting and improving their fraud prevention measures & fraud management. However, more scammers are comfortable committing fraud online, facilitated by perceived anonymity.
- Lastly, banks have state-of-the-art fraud detection systems. But many small and medium-sized businesses do not. It makes them more vulnerable to fraud and can potentially harm the larger banking system as a whole.

Note that this presentation is for background reference only, and does not reflect the views of any particular panelist or their organizations. With special thanks to Protiviti consulting for use of some of their research and materials.

Fraud in Banking – Current Landscape (continued)

Types of Fraud

External Fraud

It involves outsiders penetrating bank security, often with insider collusion, to access sensitive information or conduct fraudulent transactions. Examples include exploiting poor password security and manipulating mobile banking authentication by temporarily changing customer phone numbers. This highlights the ease with which employees can alter customer information undetected.

Internal Fraud

It is the most common way for banks to suffer losses, with up to 70% of cases involving employees. Fraud occurs at all organizational levels, with middle/senior managers and junior employees frequently implicated. It often involves collusion to bypass controls, particularly among employees with high-level IT access who can manipulate or erase evidence. Fraudsters typically exploit IT system vulnerabilities over time, starting with small changes to test detection.

Types of Financial Frauds

1. Account Takeover
2. New Account Fraud, Payment Fraud and ACH Fraud
3. Check and Card Fraud
4. P2P Payment Fraud
5. Wire Transfer, Application, Loan Fraud
6. Terrorist Financing, Money Laundering, Bribery, and Corruption.
7. Identity theft, Investment Fraud, Mass Marketing Fraud and Money Mules

Future Predictions – Fraud In Banking

1. Generative AI aids fraud through deepfakes, scam websites, and fake/synthetic identities.
2. Consumers trust biometrics but banks are slow to adopt them, increasing the risk of fraud at branches.
3. Synthetic identity fraud has increased during the pandemic and is a growing concern for businesses.
4. Fraudsters will use cause-related and investment scams to target consumers' personal information.

Top Fraud Risks in Banking Industry in 2025

Significant Fraud Risks Faced by the Financial Services Organizations and Banking Industry

Escalating first-party fraud: Rising incidence, including manipulation by legitimate customers, complicates detection & attribution, challenging banks' fraud prevention efforts.

Reimbursement scams: New reimbursement programs may increase first-party fraud claims, demanding heightened vigilance from banks to mitigate escalating risks effectively.

Small- and mid-sized business (SMB fraud): SMB loan applications exhibit a significant uptick in first-party fraud, necessitating enhanced scrutiny amid challenges in distinguishing genuine businesses from synthetic entities.

Image fraud: Detection challenges abound as fraudsters exploit image files, prompting banks to refine screening tools to thwart undetectable manipulations effectively.

Fraud as a service: Increasingly, fraudsters engage in collaborative schemes and offer fraud-as-a-service, complicating fraud detection with diverse document templates and resources.

Deepfake identity fraud surge: Deepfake technology poses significant threat to financial sector, enabling convincing fabrication of IDs & impersonation through hyper-realistic videos. With a 30% rise in deepfake-related crimes in 2023, banks face heightened challenges in fraud detection.

FedNow and instant payment fraud: FedNow's real-time payments risk exploitation by fraudsters, potentially amplifying sophisticated account takeovers and first-party fraud incidents.

Voice clones, deep fakes and AI-enabled fraud: AI advancements fuel voice & document fraud, challenging banks to combat rising instances of imposter fraud and manipulation using GenAI technology.

Digital onboarding vulnerabilities: Digital onboarding's convenience exposes institutions to new vulnerabilities, identity verification & due diligence processes. Fraudsters exploit these weaknesses, leading to synthetic identity fraud & digital document manipulation, posing heightened risks.

Check fraud: This fraud persists due to the thriving market for stolen checks, urging banks to implement robust security measures, like text message confirmations.

Global cross-border fraud complexity: Increasing global transactions bring forth intricate cross-border frauds, exploiting regulatory variations across jurisdictions. This complexity amplifies detection & recovery hurdles for FIs combating fraudulent activities.

KYC data security threats: Sophisticated attacks targeting KYC data integrity are on rise in 2024. Breaches not only affect customer security but also tarnish the reputation of institutions, emphasizing critical need for robust measures.

Top Fraud Risks in Banking Industry in 2025

Fraudulent Payments (Unauthorized)

Unauthorised fraudulent payments are attacks which encompass various fraudulent activities involving an unauthorised transfer of funds from a person or company's account. The following are types of trends which fall under the category of unauthorised fraudulent payments.

Technical support

In technical support fraud, scammers pose as representatives from legitimate tech companies. They might call or email people, claiming that their computer has a virus or issue. The scammer will then ask for remote access to the device to "fix" the problem. During that time, they can steal personal information or financial credentials. They might also charge a fee for this "service."

Mobile SIM swap

Next, mobile SIM swap fraud has risen in recent years. The fraudster can take over the mobile phone number in a SIM swap scam. They'll pose as another person and convince their wireless provider to transfer the number to a new SIM card they control. Once they have access to the person's phone number, they have all the phone call, text messages, and potentially access to any two-factor authentication linked to that number. They can then use this information to commit fraud, such as **accessing bank accounts or credit cards.**

Account takeover

Here, the scammer gains access to another person bank or credit card account by posing as them and providing enough personal information to pass security measures. They'll answer any security questions and change pin codes/login information. As a result, they can potentially drain the account or make unauthorised purchases. They may even take out fake loans.

Bank insider

A bank insider have access to sensitive financial information, such as account numbers and login details. When they think that account holder isn't paying attention, they will skim off small amounts from their account. This scam can go unnoticed for a long time, and the amount stolen may add up over time. Constant vigilance and internal audits can help prevent this type of fraud.

Phishing

Phishing is one of the oldest and most successful forms of fraud. Fraudsters will send emails or texts posing as a legitimate institution, such as the bank. They will request personal information or login details. These communications often contain links to fake websites. Once they have this information, they can commit identity theft or gain access to another person's accounts.

Man-in-the-middle/pharming

Another type of fraud related to phishing is man-in-the-middle or pharming attacks. Here, the scammer will insert themselves between the victim & a legitimate institution. Scammers might intercept communication or redirect users to a different website, and then collect login information or personal information for their own gain. This type of fraud can be especially dangerous because it often goes unnoticed until it's too late.

Top Fraud Risks in Banking Industry in 2025

Fraudulent Payments (Authorized)

In contrast to the previous forms of fraud, authorized fraudulent payments involve the victim actually authorising a payment. However, they may have been tricked into doing so by the scammer. The following banking fraud trends are forms of authorized fraudulent payments.

Business email compromise

In a business email compromise, the scammer will pose as someone in authority within a company, such as a CEO or CFO. They may send an email requesting a transfer of funds to a particular account, that they control. The victim, usually an employee trying to follow orders, may not realize they are being scammed until it's too late.

Invoice fraud

In this type of fraud, the fraudster will pose as a supplier or vendor and send an invoice to a victim requesting payment. The victim may not realize that this is a fake invoice and will end up paying it. For example, if a business usually deals with a particular manufacturer and receives invoices from them regularly, they may not think twice about paying one that seems legitimate.

Investment Scams

Investment fraud involves fraudsters convincing victims to invest in "amazing" opportunities. They may promise high returns with little risk and use false information or pressure tactics to persuade the victim to hand over their money. The cryptocurrency market has proven to be a breeding ground for these types of frauds, as the lack of regulation allows for more room for fraud.

Push payment social engineering

In this type of fraud, the scammer will convince the victim to voluntarily send them money through social engineering tactics. These can range from posing as a government agency requesting payment for fake fines to impersonating a family member needing an urgent funds transfer. Unscrupulous individuals may also wait for a disaster or war and pretend to be charitable organizations requesting donations.

Romance scams

Finally, the shift of dating and socializing online has also opened the door for romance scams. The scammer will create a fake social media profile and start an online relationship with the victim. Ultimately, they will convince them to send money. They may start by catfishing, using a fake identity and photos, and then gradually gaining the victim's trust over time.

OCC Regulatory Guidance on Fraud Risk Management in Banking

Bank fraud results from inadequate processes and internal controls, simple human error, blatant employee misconduct, and other adverse incidents. Examiners and industry experts have identified five characteristics of financial institutions that manage fraud risk well, captured in the OCC's Operational Risk: Fraud Risk Management Principles. The below guidelines offer general best practices for risk officers and banking leaders.

Governance

Institutions require their board and leadership to create a culture of accountability among employees. Does the institution have ongoing employee training programs, strong identity theft controls, an employee code of conduct, and an overarching ethics policy? Some financial institutions (FIs) develop a system of rewarding employees who spot and prevent fraudulent activities.

Fraud Risk Assessment

When community banks & credit unions make fraud risk a part of their enterprise risk management (ERM) strategy, they reduce potential losses and protect consumers.

- Agencies push FIs to treat risk holistically, with vendor management, cyber security, business continuity planning & fraud risk all falling within an FI's ERM framework.
- Fraud risk assessments pinpoint vulnerabilities that bad actors exploit. The assessment should include different scenarios, the probability of occurrence, and potential consequences.
- Data from BSA/AML compliance assessments and Suspicious Activity Reports (SAR) often prove useful in identifying fraud and strengthening an institution's internal controls.

Fraud Risk Controls

The OCC offers a comprehensive list of common fraud risk controls. These controls could be divided into prevention and detection.

Prevention

- Training employees in fraud risk management.
- Systems and controls designed to decrease the likelihood of fraudulent activities by employees, outside consultants, and third-party contractors.
- Separation of roles & dual control over accounting/ consumer transactions.

Detection

- Monitoring & reports of possible fraud across institution's business lines.
- Data analytics and trend monitoring focused on practices such as fee waivers or charge-offs, along with the number of fraudulent activities measured against transaction volume.
- Strong complaint resolution policies and procedures.

Fraud Risk Monitoring

FIs should review historical losses from fraud and benchmark performance by industry standards. When the board or banking leaders have up-to-date reports on fraudulent activity from current and past years, they can decide to implement more robust controls if necessary. Financial institutions should monitor:

- Fraud by type (check, account opening, loan, credit card) & amount (recoveries & net fraud losses)
- SAR filings
- ACH return rates
- Unusual activity in consumer accounts and complaints

Investigating Fraudulent Activities

After building a solid foundation for assessing, monitoring & controlling fraud, institutions can introduce a process of investigation & remediation. FIs need to designate specific employees to oversee suspicious transactions. They must keep close tabs on consumer complaints & respond quickly to incidents.

Additionally, the FIs is required by federal law to report suspicious activities – whether they were successful or averted. For further information about SARs filing requirements, firms should consult FinCEN laws from the U.S. Department of the Treasury.

Financial Fraud Laws, Regulations, and Contractual Issues

- **Bank Fraud 18 U.S.C. 1344**
  - It is a crime to knowingly executed a scheme in order to defraud a financial institution, or to obtain money or property from a financial institution, using fraudulent pretenses, representations or promises (penalties include fines up to $1 million, up to 30 years imprisonment, or both)
- **Identity Theft**
  - **Fair and Accurate Credit Transactions Act** (15 USC § § 1681-1681x, amends the Fair Credit and Reporting Act: the law requires creditors and reporting agencies to protect consumers' identifying information and take steps to guard against identity theft)
  - **Federal Trade Commission Red Flags Rule**, known as the “Identity Theft Rule” (16 CFR Part 681) requires a written program to identify and prevent identity theft for covered accounts, including keeping up with threats and five general red flag categories:
    - alerts, notifications, or warnings from a consumer reporting agency
    - suspicious documents;
    - suspicious identifying information such as a false address;
    - unusual use of or suspicious activity related to a covered account; and
    - notices from customers, victims of identity theft, law enforcement authorities or other businesses about possible identify theft in connection with covered accounts
- **CFPB UDAAP**
  - The Consumer Financial Protection Bureau enforces Unfair, Deceptive, or Abusive Acts or Practices (UDAAP, 12 USC § 5531), consumer protection laws and rules, including fraud
- **FTC UDAAP**
  - Section 5 of the Federal Trade Commissions Act prohibits unfair or deceptive acts or practices in or affecting commerce, which includes consumer, commercial, and state banking fraudulent activities
- **Bank Secrecy Act/Anti-money laundering laws and regulations**
  - FinCEN compliance programs, currency transaction reporting, suspicious activity reports, beneficial ownership requirements, records retention: Bank Secrecy Act and Suspicious Activity Reporting Requirements under 31 CFR Chapter X

Financial Fraud Laws, Regulations, and Contractual Issues (continued)

- **Federal and state regulatory guidance**
  - Examples include OCC guidance, SEC and FINRA anti-fraud compliance requirements, for example:
    - OCC guidance on fraud risk management in banking (Bulletin 2019-37, see page 11)
    - SEC guide to identify and prevent securities fraud, and FINRA AML Rule 3310
- **Bank management and liability for internal fraud**
  - Ethics and human resources policies and procedures
  - Investigative processes to review and escalate potential internal involvement
  - Sophisticated fraudsters often have knowledge of banking operations and solicit/pay for assistance from internal banking employees at various levels and roles
- **Bank liability and contractual allocation for external fraud**
  - Check clearing, payments (UCC 4A, electronic funds transfer act), cards and loans
  - Applicable security procedures and compliance
  - Clear contractual allocation of liability for fraud losses and various causes (following customer or third party financial institution instructions, security procedures, etc.)
  - Third party risk management and protocols to address vendor or third party subcontractor fraud issues
- **Information and cybersecurity breach protocols related to significant fraud events**
  - Escalate fraud activities involving significant data and security breaches
  - Address regulatory notification or reporting requirements, including for example under the more recent OCC Computer Security Incident Notification Rule

Consumer vs Commercial Accounts: Liability and Regulatory Regimes

Liabilities and regulatory regimes for consumer and commercial accounts differ significantly under U.S. law, primarily in terms of how they are regulated and the protections afforded.

Consumer Account

- **Regulatory Focus:** Consumer accounts are primarily regulated to protect individuals from unfair, deceptive, or abusive practices. The focus is on ensuring fair treatment, transparency, and protection of personal information.
- **Key Regulators:** The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) are the primary regulators for consumer accounts.
- **Regulations and Protections:**
  - **CFPB:** Oversees consumer financial products and services, including mortgages, credit cards, and student loans. The CFPB enforces laws such as the Truth in Lending Act (TILA) and the Consumer Financial Protection Act (CFPA), focusing on disclosures, fair lending, and protecting consumers from abusive practices.
  - **FTC:** Regulates deceptive advertising practices, including false claims and misleading advertisements. The FTC enforces the Federal Trade Commission Act (FTC Act), which prohibits unfair or deceptive acts or practices.
- **Liabilities:**
  - **Liability for Errors and Fraud:** Consumers generally have stronger protections against errors and fraud. For example, under the Electronic Fund Transfer Act (EFTA), consumers have limited liability for unauthorized transactions if reported promptly.
  - **Resolution of Disputes:** There are specific provisions for resolving disputes, including the right to fair treatment in cases of billing errors or unauthorized transactions.

Commercial Account

- **Regulatory Focus:** Commercial accounts involve businesses rather than individuals, and the regulations typically focus on maintaining fair business practices and competition rather than personal consumer protection.
- **Key Regulators:** While the CFPB and FTC also regulate commercial accounts, other agencies like the Office of the Comptroller of the Currency (OCC) and the Federal Reserve may be involved, depending on the nature of the business account.
- **Regulations and Protections:**
  - **CFPB:** The CFPB's jurisdiction over commercial accounts is limited, focusing more on consumer protection rather than business-to-business transactions.
  - **FTC:** The FTC's regulations apply to commercial practices, including advertising and marketing practices aimed at businesses. However, its primary focus remains on protecting consumers.
  - **Other Regulations:** Commercial accounts are also subject to various industry-specific regulations and standards, such as the Uniform Commercial Code (UCC) for negotiable instruments and commercial transactions.
- **Liabilities:**
  - **Liability for Errors and Fraud:** Businesses may have fewer protections compared to consumers. Liability for unauthorized transactions or errors can be higher, and businesses are often expected to have more robust internal controls.
  - **Resolution of Disputes:** Dispute resolution mechanisms can be more complex, and commercial accounts often involve contractual agreements that define the terms and conditions for handling disputes.

Bridging the Gap Between Fraud and Financial Crime Compliance

Integrating fraud and financial crime compliance systems enables banks to break down silos, establish common goals, and achieve significant cost savings. This holistic approach improves transparency, real-time threat response, and operational efficiency. Adopting integrated models is crucial as digital banking channels increase fraud risks. Unified efforts help banks better protect against sophisticated financial crimes, enhancing both security and customer satisfaction.

Challenges in Fraud Detection and Prevention

Departmental Separation: Fraud detection and prevention are handled separately by different departments (e.g., customer service, risk management, investigations, compliance). This results in fragmented views and a lack of comprehensive insight.

Digital Transformation: The rise of digital banking channels increases opportunities for fraud, posing a critical threat to the banking and finance industry.

Need for Integration

Current State: A KPMG survey found that 43% of respondents had no integration between fraud and financial crime compliance.

Enterprise Platform: Aligning risk response strategies under an enterprise platform can improve transparency and communication.

Survey Findings: A Chartis survey indicated that 71% of senior financial executives see a compelling business case for integrating anti-fraud and AML systems into a single technology environment.

Benefits of Integrated Systems

Breaking Down Silos: Integration eliminates departmental silos, enabling real-time responses to threats across all banking sources and improving the detection of sophisticated criminal activities.

Establishing Common Goals: Unified systems align fraud, compliance, AML, and risk management departments, ensuring consistent data use and collaborative efforts towards combating financial crimes.

Cost Savings: Centralized data platforms and streamlined processes reduce system ownership costs and workforce redundancies, leading to estimated savings of 20-30% while enhancing overall operational efficiency.

Bank Fraud – Detection, Investigation & Mitigation Protocols

"Every Dollar Lost to a Fraudster, Costs North America's Financial Institutions $4.41"

Bank fraud **investigation, detection, and prevention** encompass policies, **protocols**, and technologies used by banks and financial institutions to protect against fraud through threat monitoring, account monitoring, behavioral profiling, and proactive risk identification. **Prevention** measures include internal controls, employee training, and multi-layered security.

Importance of Fraud Investigation, Detection and Prevention in Banking

Fraud detection and prevention helps protect customers' financial assets and personal information, maintain consumer trust and reduce financial losses due to fraudulent activities.

- **Financial Loss Prevention:** By implementing effective fraud detection and investigation measures, banks can better identify and stop suspicious transactions, thus minimizing potential losses.
- **Customer Trust:** Enhance customer loyalty by showcasing the bank's commitment to their protection through robust fraud investigation practices.
- **Regulatory Compliance:** Implementing strong investigation mechanisms helps banks stay compliant with various AML/CFT regulations.
- **Reputation Management:** Preventing fraud through diligent investigation helps maintain a positive image and better ensures customers view the institution as a safe place to conduct financial transactions.

Banking Fraud Survey Findings - KPMG 2018

Internal Fraud

Volume and value of internal fraud are increasing, with **41%** of respondents reporting an increase in volume and **24%** reporting an increase in value.

External Fraud

Volume and value of external fraud are also increasing, with **61%** of respondents reporting an increase in volume, **31%** reporting an increase in value, and **59%** reporting an increase in average value.

Key Components of Fraud Mitigation Protocols

01 **Use of fraud detection and prevention software**
Integrate modern software for real-time fraud detection and prevention using multiple data sources and machine learning analytics.

02 **Designing of internal policies**
Develop internal policies defining fraud, detection processes, and access controls for customer data.

03 **Deployment of risk management systems**
Deploy a centralized risk engine for automated evaluation and customizable risk assessment to comply with regulations.

04 **Training of employees**
Provide ongoing training on fraud policies, risk management trends, and regular testing for employee awareness.

05 **Education of customers**
Inform customers about online fraud risks and secure practices for compliance.

06 **Regular evaluation of the fraud program**
Regularly review and test fraud prevention tools, processes, and customer account monitoring to identify and address gaps.

Latest Technologies in Fraud and Prevention

**Fraudsters are becoming more sophisticated, and their methods are evolving,
so it is important for the banks and financial institutions to evolve and being scalable to the latest technologies.**

- **Automation**
  - The adoption of a fully automated fraud management platform is crucial. They can cut down on human resources devoted to fraud detection process and introduce less friction as these solutions find more useful data that is impossible for a human counterpart to discover. BNPL providers that want to optimize customer experience for minimal friction should certainly automate their risk assessment. This way, inspecting identity attributes that aren't readily apparent can be detected, and those determinations can then inform the overall risk score.
- **Artificial Intelligence**
  - AI-based fraud monitoring systems can ingest and parse massive quantities of data - a must, given the high volume of transactions banks process each day - and detect fraudulent activity in real-time. Compared to rules-based engines, AI is highly adaptable, enabling banks to easily pivot their fraud management strategy based on new and emerging threats. And finally, AI offers far greater accuracy than manual or rules-based fraud detection, significantly reducing the rate of false positives and providing banking customers with a better overall experience.
- **Machine Learning**
  - Machine learning is a powerful tool for fraud prevention in the banking industry. ML enables fraud monitoring & detection systems to "learn" from behavioral data, consortium data and other internal & external data sources and adapt accordingly. The result is that banks are better able to navigate increasingly complex fraud landscape and deliver more proactive protection to customers and their assets.
- **Biometric Authentication**
  - Biometric authentication is an identification technique that relies on a customer's unique physical characteristics, such as their voice, facial features, or fingerprints, to verify their identity. Biometric authentication has quickly become a popular security measure with FIs because customers' biometric data cannot be stolen, forgotten, or lost. Although fraudsters can spoof a customer's biometric data, it is far more challenging to do so than it is to steal their identity or credentials. To get the greatest value out of biometric authentication, banks should pair it with other technologies & controls to create a truly multi-layered security strategy.

Latest Technologies in Fraud and Prevention (continued)

- **Two-factor and/or Multi-factor Authentication**
  - Two-factor (2FA) & multi-factor authentication (MFA) are identification techniques that require banking customers to provide two or more pieces of evidence to verify their identity. 2FA and MFA are fairly standard security measures that, like biometric authentication, should be layered with the other technologies shown here to create a comprehensive anti-fraud strategy.
- **Advanced Analytics**
  - Financial institutions process hundreds - even thousands - of transactions each day, each of which generates data. When analyzed using advanced data science techniques, customer and transaction data can be incredibly potent, enabling banks to gain a 360-degree view across the business, enhance operational efficiency, and engage in predictive fraud detection.
- **Device Fingerprinting**
  - While behavioral analytics tracks user behavior, device fingerprinting solutions track the devices and applications authorized users typically use to carry out this behavior. For example, when it comes to online banking, most people will typically access these services using their mobile phone or tablet, and possibly a work and/or personal computer. They may also tend to use certain browsers or applications on these devices. Device fingerprinting techniques can identify deviations in typical device access patterns and trigger alerts or 2FA challenges in response. The best fraud detection software combines both behavioral analytics and device fingerprinting capability. As more customers turn to mobile apps for their financial services, businesses should be increasingly leaning on device fingerprinting to remove as much anonymity from the mobile space as possible. This will mitigate the damage done by synthetic ID fraudsters, business email compromises, and APP fraud.
- **IP Reputation Analysis**
  - IP reputation analysis can help detect potential fraud by analyzing IP addresses associated with transactions and identifying any unauthorized activity. IP analysis can also help identify phishing scams, sophisticated frauds like wire fraud and money laundering, and even suspicious activity that could lead to identity theft.
- **Data Mining**
  - Data Mining can be used to identify patterns of bank fraud by looking for suspicious transactions. It can also be used to reduce the risk of investment fraud, such as large purchases of stocks that are not well-known or that are not expected to perform well. Common data mining techniques for fraud detection include - decision trees, neural networks, association rule mining, support vector machines, logistic regression.

Overview – Bank Fraud Detection and Prevention

- **Most common traditional bank fraud detection & prevention approaches**
  - **Rule-based systems** - Use predefined rules to detect fraud, for example, showing alert when a transaction is exceeding above a certain unusual amount.
  - **Human review** (e.g., internal audit or external audit) - Manual examination of transactions and organization data to find out potential suspicious transactions and take prevention actions.
  - **Statistic models** - Use historical data to identify patterns and anomalies that may indicate fraud.

Problems in traditional bank fraud detection/ prevention

- **Not able to keep up to new type of frauds on time** - Fraudsters are looking for new ways to tackle traditional models, once they found a gap from the models or systems, they exploit them to maximize financial gain. Banks normally will only find out when unusual huge loss being incurred while this resulting in bad press that might negatively impact customers' trust.
- **High percentage of false positives** - Lack of relevant data to generate accurate insights to detect frauds and/ or human errors that waste time and effort on exanimating the false positives cases. Research found over 95% of system-generated alerts are closed as "false positive" since 5 years ago and this issue still remain unsolved for many banks globally.
- **Causing bad customer experience** - Difficulty in balancing fraud detection & prevention with customer experience, as some fraud detection measures can lead to increased friction/ inconvenience for customers.
- **Regulatory Compliance issues** - Cautious of taking new digitalization move or searching trustworthy advanced technology providers that are able to stay complaint with regulations such as data privacy laws, while collecting and using data for fraud detection purposes and deal with data security and privacy concerns.
- **Geolocation no longer the primary way to detect fraud** - Previously, unexpected changes in geolocation were often primary means to detect fraud. However, it has become common for both fraudsters & F/CaaS software to use configurable VPN or proxy to disguise connections as originating from an expected geolocation. Therefore, checking geolocation alone is no longer an adequate strategy. It must be combined with device & behavioral data to build a unique "fingerprint" for bank's authorized users.

Best Practices/Strategies – Fraud Detection and Prevention in Banking

With global fraud rising beyond control, it's vital that organizations implement effective fraud prevention policies and procedures that provide security while ensuring a quality customer experience. With the best practices for fraud prevention, businesses can onboard customers quickly and seamlessly.

1. **Implementing robust internal controls**

   Internal controls play a crucial role in fraud detection in banking. They encompass a set of rules, policies, and procedures to detect and prevent fraudulent activities. This could include dual controls for critical operations, regular audits, segregation of duties to ensure that no single individual controls all parts of a financial transaction, and rigorous vetting procedures for new staff. Strict adherence to internal controls can help identify suspicious activities.

2. **Behavioral data & behavioral targeting technology**

   Use of Behavioral Data & Behavioral Targeting Technology can reduce fraud by analyzing & identifying unique online behavior patterns of customers. In this fast-changing environment, it's important to understand the customers by comparing customer's current behavior to their typical behavior. A better understanding about the customers behaviors could increase opportunities to optimize customer experience while also to discover suspicious patterns for fraudulent activities. Steps involved in fraud risk mitigation using behavioral targeting technology include - **behavioral data collection, behavioral profiling and real-time monitoring & fraud detection.**

3. **Develop multi-layered security systems**

   A successful bank fraud prevention and detection strategy should be multi-faceted and include administrative, physical, and technical controls:

   - At administrative level, institutions should develop policies, procedures & guidelines that reduce their risk exposure, such as security education/awareness programs & password management policies.
   - At the physical level, institutions should instate tangible security measures, such as restricting access to specific computer programs and data files and cross-checking asset or liability values against those documented in control records.
   - At technical level, institutions should implement technology that will reduce their risk exposure, such as firewalls, anti-virus & anti-malware software, and AI-powered fraud monitoring systems.

4. **Multi-layered fraud detection methodologies**

   Rule-based systems is still necessary in detecting fraud but it's not enough. It can be taken as the "first line of defense" especially for the known frauds pattern and more machine learning algorithms or diagnosis can be included in the system such as model-based model, cased-based model, and more.

5. **Advanced scoring model or ranking system**

   An Advanced Scoring Model or Ranking System that enable the banks to priorities on the fraud prevention tasks. A well-trained and developed fraud detection and prevention model is useful for the organization, but it's also important that the system interpret the model into scores and/ or ranks. The end users use gain better understanding on which customer or transactions are more likely to be fraudulent so that they are able priorities on the high score or rank customer transaction and take immediate prevention actions.

Best Practices/Strategies – Fraud Detection and Prevention in Banking (continued)

6. **The use of network analysis**

   The Use of Network Analysis in bank fraud detection that could analyze the anomaly behavior correlated across channels & detect organized crime and collusion based on the analysis of relationship. Network analysis could directly provide a 360-view about the case and the anomaly behavior in just a few clicks to save investigation time and also improve operational efficiency for the financial institutions (FIs) to make quick decisions to tackle the frauds.

7. **Host regular fraud awareness training**

   Bank employees are a popular target for cybercriminals — particularly for phishing attacks and other forms of social engineering — so it's essential to educate staff about recognizing potential fraud and what to do if they suspect that they've been compromised**.**

8. **Create a database of known threats**

   It's crucial that banks be aware of and on the lookout for active & emerging threats. By collecting fraud data from internal and external sources, banks can gain a comprehensive view of fraud landscape and make more informed risk decisions. FIs can also use such a database to support fraud awareness training and enable employees to recognize a broader range of potential threats.

9. **Educate banking customers**

   Customer fraud awareness is every bit as important as employee fraud awareness and can help a bank's customers protect themselves against would-be threat actors. Adding educational resources to an existing knowledge base, similar to what Wells Fargo has done with its Fraud Education Library, can be an effective means of keeping customers in the know. And customer education shouldn't end at fraud: Banks should also make customers aware of advanced security measures, such as 2FA or MFA and biometrics authentication, to increase their likelihood of opting in.

10. **Monitor transactions in real time**

    Transaction monitoring is not only essential to comply with KYC standards and AML laws, it's also an effective way to detect fraudulent activity. Banks must develop behavioral profiles that establish a baseline for each customer's normal activity. Once an institution has created a behavioral profile for a customer, it can monitor transactions against the baseline & proactively flag any anomalous activity.

11. **AML Compliance**

    Institutions should integrate an AML solution into their fraud prevention. Sanctions laws dictate that facilitating or participating in financial transactions with sanctioned entities will result in fines or, even worse, penalties. Complete AML compliance should consider things like politically exposed person list checks, adverse media screening & processes to determine ultimate beneficiaries of transactions.

12. **Create touchpoints at different stages across the customer experience**

    Complete digital footprint analysis at onboarding can easily blocks fraudsters. However, this analysis is not enough, as these kinds of scams will be exploiting accounts that have gone past the onboarding stage. Allowing fraud prevention software to create touchpoints at different stages across the customer experience will allow fraud teams a better win rate when it comes to preventing costly phishing scams from turning into huge reputational and regulatory damage.

Best Practices/Strategies – Fraud Detection and Prevention in Banking (continued)

13. **Consortium data**

    Increasing the breadth of data utilized in the development of fraud detection systems enhances their efficacy. Integrating diverse data sources introduces additional layers of complexity for potential intruders seeking unauthorized access to the network. Collaborative efforts among banks to exchange fraud data and identify online threats provide automated systems with a more comprehensive understanding of the challenges they face. Consortium data harnesses the collective intelligence of the industry, enabling collaborative data-driven strategies to combat fraudulent activities effectively.

14. **High tech standardization**

    Gaining a comprehensive understanding of financial systems is important for understanding the intricacies of monetary transactions. Centralizing all company data within a unified system represents the optimal approach for achieving this understanding. Many of the “legacy systems” contain vulnerabilities that fraud perpetrators know how to exploit, with some systems even continuing to use physical ledgers and paper records to bridge gaps. Consolidate the internal systems into one solution enables the organization to easily identify suspicious behavior**.**

15. **Governance, Risk, and Compliance (GRC)**

    Using GRC systems not only protects data, it also provides a set of processes that help businesses achieve objectives, address risk, and act with integrity. It’s these principles working together that allow complete coverage and protection for the data landscape. Each principle supports the other two principles, and all three consider the same information, people, and technologies.

16. **Access risk Management (ARM)**

    As the discipline of managing access risks, ARM contains methods that identify, assess, and prioritize risks from an access provisioning and compliance perspective. With risk taking on many shapes and sizes, the ARM approach helps to vigilantly monitor data while using preventative measures to manage access across all users and accounts. ARM gives organization a clear understanding of how, when, and where to deal with a specific breach.

17. **Regular risk assessments**

    Conducting regular and thorough risk assessments is fundamental. This involves evaluating emerging trends in fraud, assessing vulnerabilities in existing systems, and adapting strategies accordingly. Risk assessments provide the basis for refining and enhancing fraud detection protocols.

18. **Adaptive strategies**

    Flexibility is paramount in the realm of fraud detection. Implementing adaptive strategies that evolve alongside emerging threats ensures that banks remain one step ahead. This may involve the integration of machine learning algorithms that learn from new patterns and continuously improve detection capabilities.

19. **Collaborating with banks for better fraud protection**

    By collaborating with banks, FinTechs can take a better approach to financial fraud prevention. Banks can bring their expertise in complying with ever-changing KYC, KYB, and AML regulations. Whereas, FinTechs can play their part and bring in the much-needed technological expertise. Financial technologies such as online document verification software and online bank account verification software and proof of address verification software tend to enhance the overall fraud detection and prevention programs.

Best Practices/Strategies – Fraud Detection and Prevention in Banking (continued)

The Latest Technologies for Banks to Detect and Prevent Credit Card Fraud

Banks, neobanks, and other financial institutions (FIs) can leverage emerging technologies like machine learning and artificial intelligence to detect and prevent fraud.

- **Voice biometrics** is a new technology being used by FIs and banks to passively authenticate callers based on their voiceprint. By comparing a caller's voice characteristics against a verified, previously enrolled voice sample, this technology can help identify fraudsters and flag calls made under duress.
- **Enhanced knowledge-based authentication (KBA)** validates cardholder identities against outside sources, such as personal information. By checking whether the information provided by a caller appears in association with the same individual in other records, KBA can create extremely hard-to-guess challenge questions.
- **Adaptive authentication** is an AI fraud risk scoring capability that will pull together analytics from multiple channels to provide clear guidance to agents during a call. By combining anomalies such as unusual device attributes, excessive numbers of transactions, or failed voiceprints into a single risk score, agents can take the appropriate actions to prevent fraud before it happens.
- **Address verification service or AVS** is one of the most widely used fraud prevention tools in card-not-present (CNP) transactions. AVS compares the billing address used in transaction with the issuing bank's address information for the cardholder to ensure that the purchase goes to customer's address.
- **Geolocation** matches a cardholder's mobile phone location with the location of a transaction, offering one more data point when accepting or declining a transaction.
- **Account takeover tools** detect account takeover attempts through biometric authentication, activity analytics that compare current online behavior with past established patterns, and general card verification. Card verification methods, such as card verification value (CVV) or card verification code (CVC), are required in CNP transactions where a PIN cannot be used.

Top Strategies for Mobile Banking Fraud Prevention

Implementing robust fraud prevention measures in mobile banking is crucial to safeguarding against different fraud scenarios. Below strategies can help fortify security in mobile banking:

- **Trustworthy identity verification:** Implementing enhanced identity verification measures is essential for ensuring the legitimacy of users accessing mobile banking services.
- **Multi-factor authentication (MFA):** Adopting methods Two-Factor Authentication (2FA) enhances mobile banking safety significantly.
- **Consumer email & text alerts:** Real-time notifications of unusual account activities empower consumers to promptly confirm legitimate transactions, bolstering fraud detection.
- **Online activity logging & behavioral analysis:** Monitoring user account access enables the identification of irregularities, such as logins from unfamiliar locations. Leveraging AI-driven fraud detection software enhances the effectiveness of spotting fraudulent behavior.
- **Multi-channel fraud & suspicious activity monitoring:** Fraud monitoring solutions integrate data from various channels, providing holistic view to detect suspicious activities.
- **Regular malware monitoring and removal:** Implementing up-to-date security software is vital to detect and eradicate malicious software that can compromise user information.
- **Secure access through HTTPS:** Employing HTTPS protocol ensures secure connections and encrypts data transmission, mitigating the risk of data interception. This protects consumers against potential data theft during online transactions.
- **Continuous vigilance:** Employing comprehensive fraud management solutions enables proactive identification and mitigation of potential threats.
- **Transaction monitoring:** By implementing robust & real-time monitoring mechanisms, institutions can identify suspicious transactions and take immediate action to mitigate risks.
- **Continuous innovation and adaptation:** By proactively adapting to changing fraud trends and schemes, and leveraging cutting-edge solutions, banks can effectively safeguard customer assets and maintain trust in mobile banking services.

Fraud Governance Role in Risk Management

In an environment where trust and financial security are paramount, understanding the dynamics of reporting, governance and compliance is the key to effectively combatting fraud and preserving the financial stability of institutions.

Role of Governance in Fraud Management

- **Enhancing Anti-Fraud Efforts:** The compliance program plays a crucial role in a company's anti-fraud efforts, offering a strategic advantage in mitigating risks associated with fraudulent activities. Compliance with relevant regulations and standards is essential for **effective fraud risk management** in the banking industry.
- **Strategic Value Beyond Regulatory Compliance:** A robust ethics and compliance program goes beyond regulatory requirements, offering strategic value by effectively managing fraud risks, enhancing the control environment, and fostering a culture of integrity and ethics throughout the organization.
- **Fraud and Corruption Prevention:** Compliance practices include measures to prevent internal fraud and corruption. They help maintain the integrity of banking operations and protect institutions' reputations.
- Data from BSA/AML compliance assessments and Suspicious Activity Reports (SAR) often prove useful in identifying fraud and **strengthening an institution's internal controls**.
- **Supporting Auditors' Assessments:** Compliance officers can anticipate a shift in their working relationship with audit firms, as auditors are urged to be more aggressive in assessing fraud risk. A robust compliance program provides **auditors with vital evidence and insights into the effectiveness of a company's controls**.
- **Assessment of Entity-Level Controls:** Compliance officers oversee crucial components such as the code of conduct, whistleblower hotlines, anti-corruption training, and efforts to promote an ethical culture, all of which contribute to the overall control environment.
- Compliance officers can proactively audit the effectiveness of their compliance program, including conducting employee surveys on corporate culture and evaluating the functionality of whistleblower hotlines. This proactive approach helps demonstrate the efficacy of the control environment which is indispensable to anti-fraud efforts.
- **Refinement of Fraud Risk Assessments:** Compliance teams collaborate closely with internal audit or anti-fraud teams to support fraud risk assessments. By conducting thorough investigations and providing insights into the root causes of fraud incidents, compliance officers **contribute to the refinement and focus of fraud risk assessments** within the organization.
- Regulators are now starting to embrace a more proactive posture to ensure successful anti-fraud measures in the financial services industry. This may require organizations to place a greater primacy on **compliance and fraud prevention**.

Source: Linkedin, Ncontracts, Navex, Pymnts

Fraud Governance Role in Risk Management

Fraud Reporting

At the core of fraud prevention and detection lies the concept of **fraud reporting** – an integral process vital for the maintenance of financial integrity. Fraud reporting entails systematic collection & distribution of critical information about fraudulent activities & incidents. Institutions must establish and maintain robust fraud detection & prevention systems, complemented by efficient reporting mechanisms. These mechanisms not only ensure the collection of accurate data but also facilitate timely transmission of this information to the relevant authorities, thereby enabling swift action and the mitigation of potential harm.

A comprehensive fraud reporting program should include the following components:

- **Clear guidelines & procedures:** A comprehensive fraud reporting program should begin with well-defined guidelines and procedures. These should outline what constitutes fraud, how to report it, who to report it to & the steps to follow when a potential incident is identified. Clarity in these processes ensures that employees & stakeholders understand their role in reporting.
- **Training and awareness:** Regular training and awareness programs are crucial to educate employees and stakeholders about the importance of fraud reporting. This includes recognizing potential red flags, understanding reporting mechanisms, and fostering a sense of responsibility toward fraud prevention.
- **Multi-channel reporting:** A robust program should offer multiple reporting channels, such as online forms, dedicated hotlines, and in-person reporting, to accommodate diverse preferences and ensure that anyone can report fraud conveniently.
- **Data security and protection:** Ensuring the security and confidentiality of the information reported is paramount. The program should have strict measures in place to safeguard sensitive data, assuring individuals that their information is safe.
- **Escalation protocols:** Clearly defined escalation protocols should be established to handle different types of fraud reports. This ensures that the appropriate authorities are informed promptly and that necessary actions are taken promptly.
- **Documentation and record keeping:** Comprehensive documentation of all reported fraud incidents is essential. This documentation not only aids in investigations but also helps in trend analysis, allowing institutions to proactively identify and address vulnerabilities.
- **Regular auditing and monitoring:** Continuous fraud monitoring and periodic audits of the fraud reporting program can help identify any weaknesses or gaps. This proactive approach allows for program improvement and adaptation to evolving fraud threats.
- **Collaboration with authorities:** Establishing strong relationships with law enforcement and regulatory agencies is vital. The program should have mechanisms for seamless collaboration with these entities to facilitate investigations and prosecutions.
- **Feedback and communication:** Those reporting fraud should receive acknowledgement of their reports and be kept informed about the progress and outcomes of investigations whenever possible. Open communication builds trust in the reporting process.
- **Whistleblower protection:** Implementing policies to protect whistleblowers from retaliation is critical. These protections should extend to customers & stakeholders who report fraud in good faith.

In summary, a comprehensive fraud reporting program goes beyond just reporting incidents; it encompasses a holistic approach that includes prevention, education, protection, and collaboration. By having such a program in place, FIs can better safeguard their integrity and contribute to the overall resilience of the financial sector against fraud.

Source: Fraud.com

Fraud Governance Role in Risk Management (continued)

The synergy between reporting and compliance

In summary, the collaboration between reporting and compliance creates a strong anti-fraud strategy that not only keeps fraud at bay but also ensures that FIs adhere to their regulatory responsibilities. Below tips can help financial institutions to craft effective reporting and compliance strategies:

- Understanding the critical role of reporting & compliance in the fight against fraud, financial institutions can successfully deter fraudulent activities, minimize risks, and stay compliant with regulations. By embracing these approaches, organizations can safeguard their assets and reputation while making it difficult for fraudsters to operate.
- Additionally, the symbiotic relationship between reporting and compliance goes beyond the mere prevention of fraud. It also fosters transparency and trust within the financial industry. When FIs prioritize accurate reporting and stringent compliance measures, they send a strong message to their stakeholders, customers, and the broader market that they are committed to ethical and responsible practices. This commitment not only enhances their reputation but also attracts investors and customers who value integrity and security.
- Furthermore, the collaboration between reporting and compliance is not limited to just mitigating risks; it also enables FIs to proactively identify and address emerging threats. With the ever-evolving landscape of financial fraud, having a robust system that continuously monitors and reports suspicious activities ensures that institutions can adapt quickly to new fraud schemes and regulatory changes.
- This adaptability is a crucial advantage in current dynamic financial environment, where staying one step ahead of fraudsters is essential. In conclusion, the synergy between reporting & compliance not only safeguards against fraud but also fosters a culture of responsibility, trust & adaptability.

Responsibilities of bank fraud governance and compliance teams

- The Banking Governance and Compliance departments are responsible for any potential security concerns, such as flagging and freezing accounts at risk of possible fraud. Such actions serve to help avoid or minimize both financial and administrative losses.
- **Tax Evasion Prevention -** People and corporations can use certain unethical accounting practices to avoid paying taxes. These include concealing assets behind a false or stolen identity, or in a shell corporation that doesn't have any actual business operations. Thus, bank fraud compliance teams are responsible for developing KYC/KYB policies and procedures in order to verify that clients are individuals or entities that legitimately exist and are acting in their own capacity.
- **Anti-Money Laundering** - Financial customers may also use fake/stolen identities, fake companies, and other tricks to make it seem like ill-gotten money is coming from legitimate sources. So as with tax evasion, bank compliance departments need to make sure customers are legitimate and are acting as themselves. They also need to monitor and analyze transactions to look for patterns where valid customers may be making fraudulent money moves on behalf of another entity.
- The monitoring of the compliance of policies and procedures may be performed by the fraud risk management department or the organization's risk management function. Monitoring is performed to ensure compliance with approved policies and procedures. The monitoring department must be allowed and provided with resources to check compliances and identify any non-compliance issues.

Source: Fraud.com, Visualping.io, Unit21.ai, Financialcrimeacademy.org

Fraud Remediation

Fraud Remediation Tips for Bankers

Bank fraud remediation seeks to reverse the damage done by the fraudulent act. This may include recouping cash from liable parties and/or bringing legal charges against the perpetrator. Remediation may also include attempts to make customers whole after losses and public relations campaigns, especially in the aftermath of data breaches. However, bank fraud remediation should also look at the cause of the fraud.

To protect the financial institution from future attacks, banks should assess why the fraud happened and take steps to address that vulnerability. This may include investing in better fraud detection tools, educating the customers about the risks of fraud, tightening up internal controls, or taking other steps. However, banks should focus on prevention of the fraud to minimize the need for remediation.

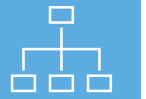
Outline remediation operating procedures

Fraud remediation strategy should outline who's responsible for dealing with cases of fraud. It should detail exactly how & when the team communicates with clients about fraud on their accounts. The plan should also explain how you deal with canceling cards, stopping checks or preventing fraudulent transactions from affecting victims' accounts in other ways. The plan should note procedures and processes for dealing with allegations of internal fraud. In addition to outlining the consequences of committing fraud, this part of the plan should also list the consequences of false allegations made against other employees. Note that in cases of internal fraud, firms may need to revisit their fraud remediation team to ensure there are no conflicts of interest.

Create a template of response actions

Streamline the operating process by creating templates that allow firms to conveniently record the incident and track response. For instance, firms may want to create a template that allows the team to log details about the date, time & details of the fraud. They should also be able to easily record how the fraud was discovered (fraud detection software, employee detection, customer report, etc.) and the actions the organization took to remediate the fraud.

Assign remediation roles



Many different people inside and outside the financial institution will be responsible for the remediation process. Make sure that you know who handles what. Assigned roles should address every aspect of the process including responding to transactions flagged as potentially fraudulent by the fraud software, answering customer calls about fraud, contacting customers about fraud, reporting the fraud to external parties, talking with the media, etc. Firms should also have well-defined protocols about which external individuals and organizations they need to contact about the fraud. Organizations' list of external advisors may include people who help with investigation, evidence collection, communication, and legal issues.

Collect evidence

The evidence needed varies based on the type of fraud. The fraud remediation plan should detail the types of evidence one need to document and collect for various types of fraud. It should also include a confidentiality policy and strategies for avoiding bias during the investigation. The plan should also explain any evidence that the clients should provide if they have been the victim of fraud. For instance, a customer who disputes an online transaction on their card may need to provide details about their legitimate transactions. Or, a customer who falls prey to check fraud may need to prove that they don't bear liability for giving a thief access to their checkbook.

Source: SQNbankingsystems, SQNbankingsystems, Complyadvantage

This document has been prepared by Chapman and Cutler LLP attorneys for informational purposes only. It is general in nature and based on authorities that are subject to change. It is not intended as legal advice. Accordingly, readers should consult with, and seek the advice of, their own counsel with respect to any individual situation that involves the material contained in this document, the application of such material to their specific circumstances, or any questions relating to their own affairs that may be raised by such material.