ProSight™

REIMAGINING INTERNAL AUDIT THROUGH INNOVATION, INSIGHT, AND ADAPTABILITY

ProSight Internal Audit Conference

Emerging Fraud Risks: Trends, Red Flags, and Internal Audit's Expanding Role

Keith Brashaber

Adrienne Steverson

With You Today

Fraud schemes are becoming increasingly more complex and digitally enabled. This session explores new fraud typologies, red flag detection, and how internal audit can strengthen fraud risk management in partnership with compliance and business units.

Learning Objectives:
- Identify emerging fraud schemes and technology-driven fraud threats in financial institutions.
- Apply data analytics and risk indicators to enhance fraud detection.
- Evaluate internal audit's role in integrated fraud risk management, including prevention techniques.

Keith Brashaber

Director, KPMG LLP

Adrienne Steverson

Director, KPMG LLP

Session Agenda

Fraud schemes are becoming increasingly more complex and digitally enabled. This session explores new fraud typologies, red flag detection, and how internal audit can strengthen fraud risk management in partnership with compliance and business units.

In this session, we will cover the following topics:

- The Evolving Landscape of Fraud
- Emerging Fraud Schemes and Technology-Driven Threats
- Fraud Regulatory Areas of Focus and Internal Audit’s Role in Prevention

Understanding the Evolving Landscape of Fraud

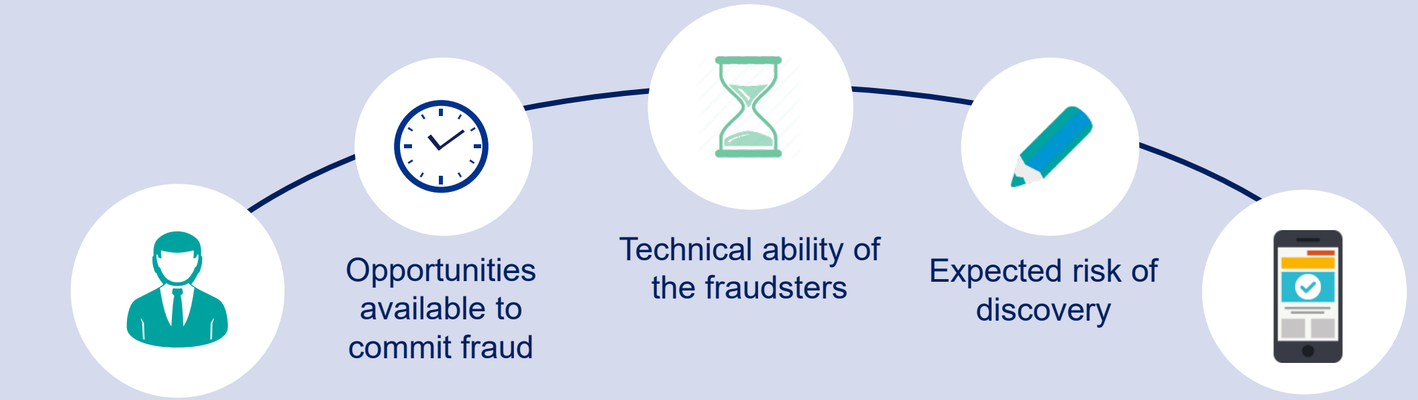
What is Fraud?

Fraud is the process of purposefully deceiving others using a scheme, misrepresentations, concealment of important information, or deceptive conduct to gain something illegally.

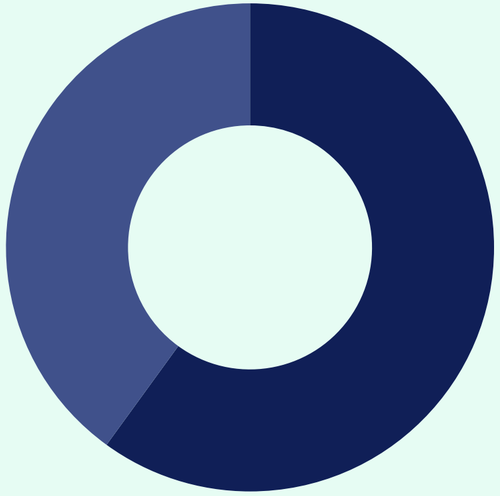
In other words, if you lie in order to deprive a person or organization of their money or property, you are committing fraud.

Fraud often relates to Misconduct. A broad concept, misconduct generally refers to violations of laws, regulations, internal policies, and market expectations of ethical business conduct.

It is helpful to take into account the following factors:



Fraud Continues to Rise at a Steady Rate

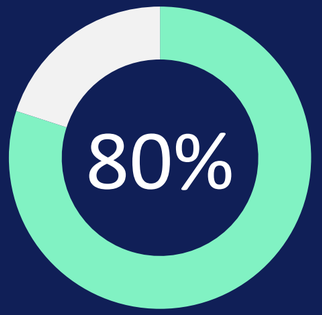


60%

Of financial institutions and fintech's said fraud grew across consumer and business accounts in the last year.

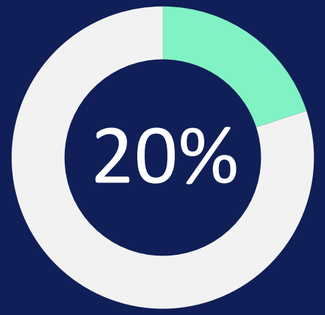
The leading fraud types were:

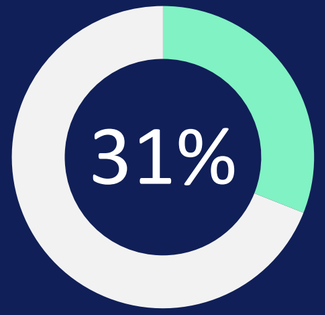
1. Credit card fraud
2. Account takeover (ATO) fraud
3. Identity theft



Fraud was most common on digital channels, with 80% of fraud events occurring on online or mobile banking channels.

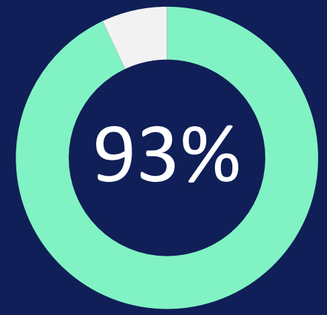
20% of enterprise banks rank check fraud as their most common fraud type.





31% of organizations faced total fraud losses exceeding $1M.

93% of respondents said that their organization is making ongoing investments in fraud prevention in 2025.



Who is Impacted?

Fraud Against Individuals

Fraud is committed against individual people:

Examples:

- Identity Theft and Synthetic Identity Fraud
- Phishing and Impersonation Scams (including Deep Fakes)
- Investment Scams
- Elder Fraud

Internal Organization Fraud

Fraud is committed against an employer by an employee

Examples:

- Embezzlement and Misappropriation of Assets
- Insider Trading and Misuse of Information
- Internal Collusion
- Accounting Fraud

External Organization Fraud

Fraud is committed against a company by an external party

Examples:

- Cybersecurity and Ransomware via:
  - Account Takeover
  - Phishing and Impersonation Scams (including Deep Fakes)
- Payment Related Fraud (Checks / ACH / Wires)

Fraud Categorization

For authorized fraud, organizations often emphasize educating customers and reinforcing security measures to prevent credential abuse. In contrast, for unauthorized fraud, they typically rely on sophisticated detection tools and rapid response mechanisms to intercept and handle suspicious activities effectively.

Fraud Risks

Unauthorized Fraud

Occurs when a transaction is **initiated without the customer's knowledge or consent**. The fraudster gains **unauthorized access** to the customer's account or payment credentials and performs transactions directly.

Authorized Fraud (Scams)

Occurs when a customer **knowingly initiates or approves a transaction but** is **deceived into doing so by a fraudster**. In this type of fraud, the customer's consent is obtained through **manipulation or deception** rather than direct system compromise.

Common Types of Authorized and Unauthorized Fraud

ProSight™

Unauthorized Fraud Types

- **Account Takeover**: Gaining control of legitimate accounts to perform unauthorized transactions.
- **Synthetic Identity Fraud**: Combines real and fabricated information to create false identities for fraudulent activity.
- **Biometric Fraud**: Involves altering biometric traits or impersonating others to defeat security measures.
- **Data Leaks/Phishing Scams**: Obtaining sensitive information through deceit or exploitation of data breaches.
- **Wire/Money Transfer Fraud**: Unauthorized transfers initiated under duress or deceitful circumstances.
- **Check Fraud**: Alteration or forgery of checks to unlawfully access funds.
- **Corporate Banking Fraud**: Targets large corporate accounts for significant financial gains through illicit activities.
- **First Party Fraud**: Individuals engage in deceit using genuine personal information for financial gain.
- **Unauthorized Card Use**: Stolen or counterfeit card information is used for illicit purchases.
- **Chargeback Fraud**: False claims by buyers for refunds after receiving goods or services.
- **Tax Fraud**: Using fraudulent means to file tax returns and gain undeserved refunds or credits.
- **Invoice Fraud**: Issuing fake invoices to businesses to collect payments fraudulently.

Authorized Fraud Types (Scams)

- **Fake Check Scam**: Victims deposit counterfeit checks and send back funds, unknowingly covering the bounced checks.
- **Flipping**: Small payments are sent by victims in anticipation of large returns that do not materialize
- **Imposter Scam**: Fraudsters impersonate officials to elicit immediate payment from victims.
- **Investment/Lottery Scam**: Victims pay advance fees, believing they have won prizes or investment opportunities.
- **Loan Scam**: Upfront fees are collected for nonexistent financial services.
- **Anti-virus Scam**: Malware masquerades as antivirus software to extract funds for non-existent threats.
- **Consumer Fraud Scam**: Payments are made for goods or services, resulting in subpar or no delivery.
- **Advance Fee Fraud**: Victims pay a fee to receive significant promised benefits that never come.
- paying for unnecessary medical alert services.
- **Debt Collection Scam**: Fake debt collection agencies use intimidation to extract payment.
- **Tech Support Scam**: Fake support warnings prompt victims to pay for non-essential tech services.
- **Financial Recovery Scam**: Victims pay for services claiming to recover funds lost in a previous scam.

Fraud Focus Trends

Focus on biometrics - Continued challenges with synthetic IDs

- A focus on biometrics allows for increased security through unique identifiers and a difficulty for fraudsters to forge.

Faster payments

- Growing adoption of real-time payment systems, fraudsters are capitalizing on the speed of transactions to commit more scams quickly.

Increased usage of Artificial Intelligence and Machine Learning

- As fraudsters become faster and smarter, institutions are heavily relying on AI and Machine Learning in the fight against fraud.

Bank liability

- Nearly 1 in 3 financial organizations experienced direct fraud losses surpassing $1M. The true impact is even more when you consider expenses.

Greater collaboration within institutions

- FIs look for ways to bring symmetry with fraud and other areas of financial

Increased focus on fraud risk management practices

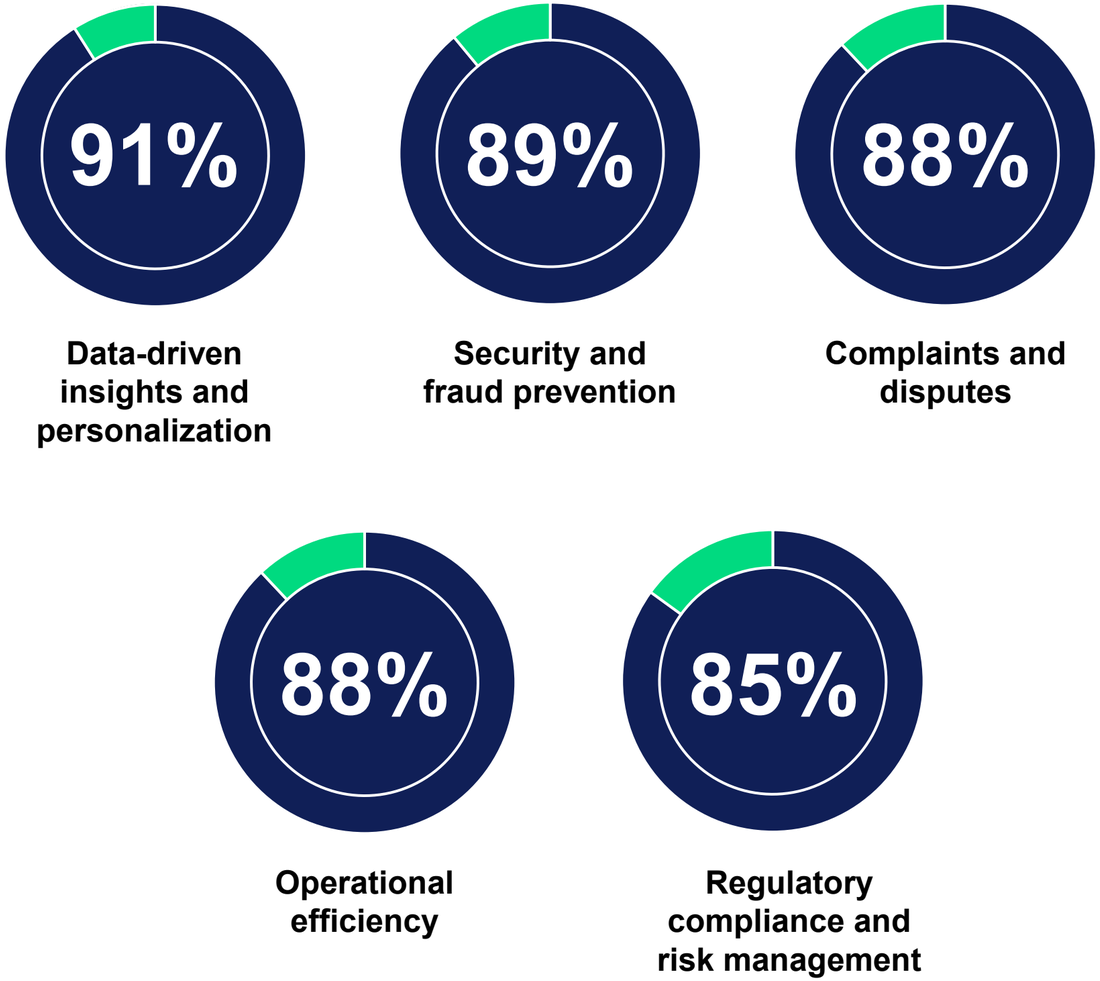
- Fraud risk assessments are integral in identifying key areas of risk within the fraud prevention program, as well as identifying gaps in controls.

Emerging Fraud Schemes and Technology

2025 Banking Investment Priorities

- Artificial Intelligence (AI) is front and center in the Financial Service industry. Banks are walking a tightrope of rapidly advancing their AI agendas while working to better define the value of their investments. Among 2025's top investment priorities, generative AI (GenAI) is proving a promising tool in aiding fraud detection and prevention and cybersecurity efforts, yet there is still reticence in the industry to release customer-facing GenAI solutions into production.

- In KPMG's 2025 Banking Technology survey results, we see companies investing predominately in the five areas shown.



Evolving Fraud Technologies and Capabilities

ProSight™

Lifecycle Phase	Account Acquisition	Authentication / Login	Account Management	Money Movement	Customer Screening
Key Fraud Risks	• ID Theft • Synthetic IDs • Bot Attacks	• Account Takeover • Credential Stuffing • Phishing • Phone SIM Swap	• Account Takeover • Remote Access • Phone SIM Swap	• Account Takeover • OTP Vishing • Remote Access • Scams • Money Laundering	• Social Engineering
Key Capabilities / Controls	• Email Risk Intelligence • Identity Verification • Funding Account Verification • Web Application Firewall • Phone Risk Intelligence • Device & Behavior Risk Intelligence • ID Scanning	• Web & Wallet Behavior Risk Intelligence • Multi-factor Authentication • SMS OTP Authentication • Web Application Firewall • Strong Authentication via a Trusted Biometric Device • Phone Risk Intelligence • Web Application Firewall	• Device Risk Intelligence • Multi-factor Authentication • SMS OTP Authentication • Web Application Firewall	• Device Risk Intelligence • Account Identity Verification • SMS OTP Authentication • Fraud Detection Risk Decisioning • Web Application Firewall	• Click to Call • SMS OTP Authentication • Web Application Firewall • Trusted Device Verification

Impact of AI on Fraud

Current trends indicate that AI-based fraud vectors are predominately being leveraged to circumvent authentication controls and victim manipulation highlighting significant vulnerabilities.

01

Deep Fakes of Documents

- Ping's identity's 2024 survey on AI and identity fraud protection revealed that 97% of organizations struggle with identity verification
- Generative AI creates realistic fake IDs, complicating identity verification processes. FinCEN and FINRA have highlighted increased use of deepfake media for fraudulent credentials, urging closer scrutiny of document authenticity to address this threat
- Generative AI improves the realism of scams by enhancing the language in emails and websites. Large language models (LLMs) can create convincing chatbots, increasing the believability of fraudulent schemes

02

Deep Fakes of Videos

- AI can manipulate video footage, alter faces and create fake video records. These can be used as false evidence or to legitimize scams, a tactic already exploited by groups like the "Yahoo Boys" in Africa.
- According to Moonlock, AI scams have surged by 148% in 2025.
- Cybercriminals use deepfake video technology to impersonate company executives in virtual meetings. In 2024, attackers posed as Arup's CFO, deceiving employees into approving $25 million in fraudulent transfers

03

Voice Cloning Scams

- A Hiya survey found that 31% of US respondents experienced deepfake calls in the past year.
- Scammers are leveraging AI to clone the voices of bank officials, agents, and politicians to extract personal information or access devices.
- The email provider Paubox found that AI- generated phishing attempts, including voice and video clones, are advancing rapidly, with nearly 48% bypassing current email and call security systems.

Integrating AI for a Comprehensive Fraud Prevention Strategy

Fraud, AML/KYC, and cybersecurity must integrate to address common criminal networks, using a unified platform for a holistic entity risk view—alerts should include device reputation and fraud history

Key Opportunity Areas

Analytics the Brains

- **Predictive and Behavioral Analytics with Machine Learning** replace static, rules- based systems, creating dynamic client profiles based on device usage, location, and activity.
- **Network Analytics** (Graph Databases) reveal complex relationships, identifying money laundering, synthetic identity schemes, and connections to known fraudsters.
- **Generative AI** aids fraud analysts by summarizing adverse media and drafting SARs quickly from structured data, reducing filing time by 50-70%

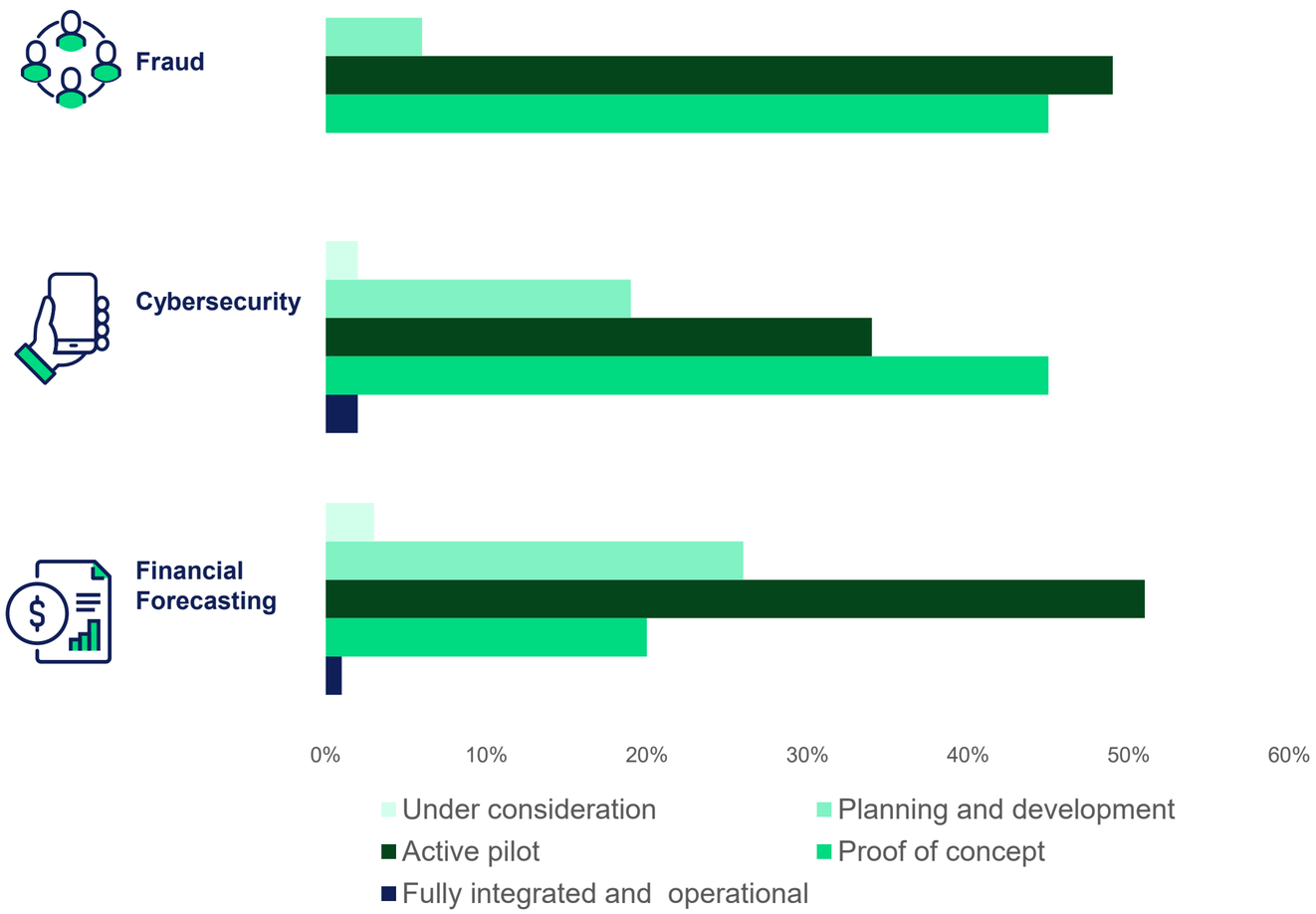
Strategy & Operations: The Engine

- Smart risk-based friction safeguards institutions and enhances customer experience, applying thorough verification for high-risk clients and minimal friction for low-risk ones.
- **Automate low-risk** alerts with predictive models and direct true suspicious alerts to human experts with AI-enhanced insights.
- **Dispute Resolution as an Intel Source:** Treat chargebacks not as a cost but as vital intelligence. Near real-time dispute analytics can identify breached merchants and new fraud typologies.

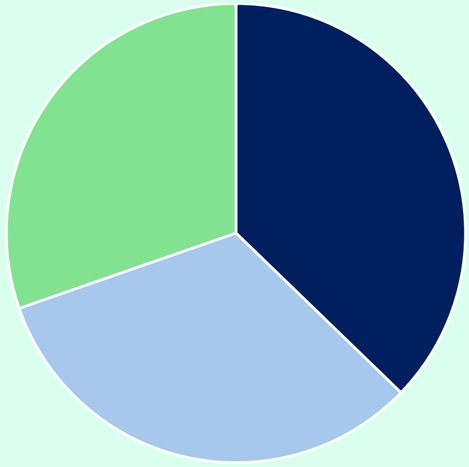
Outsourcing & Supply Chains

- **The Ecosystem Shift** from outsourcing processes to orchestrating capabilities**.** Leverage a global supply chain of specialized Reg Techs via APIs for identity verification, sanctions screening, and crypto analytics rather than BPOs**.**
- **Co-source commodity functions** like Level 1 alert reviews but never outsource core responsibilities. Financial institutions should always own the risks, policy decisions, and the ultimate responsibility of filing SARs

GenAI Investments



What bank executives are saying about the opportunities and threats of GenAI:



Your bank is increasing cybersecurity efforts due to emerging technology such as GenAI

Despite ongoing economic uncertainty, GenAI is a top investment priority for your bank this year

GenAI is an integral part of your long-term vision for driving innovation and ensuring your business remains relevant five years from now

Internal Audit Best Practices | AI Fraud

When considering how internal auditors can prepare for and counteract fraudsters using AI, it's important to focus on understanding the technology that fraudsters might leverage, as well as implementing counter- strategies that effectively address these tactics.

Leveraging AI to help the Audit Team – Suspicious Activity Reporting (SAR)

- Regulators are focused on timely and complete SAR filings – leveraging AI can help shift from manual sample- based testing to full-population continuous analysis
- Continuous workflow monitoring to ensure timely SAR filing
- Natural Language Process (NLP) can analyze and extract key information from unstructured data sources and review SAR narratives for clarity and completeness

Focus on Data Integrity and Security

- Focus on strong data governance and security measures to protect against data manipulation by AI-driven scams
- Review access controls to critical systems as well as encryption and continuous monitoring
- Collaborate with cyber security teams to analyze threats and potential weaknesses withing the Banks products and offerings

Conduct scenario planning and stress testing

- Simulate potential AI-fraud schemes to help identify weaknesses within the Bank
- Deepfakes and synthetic IDs are sophisticated ways for fraudsters to bypass fraud detection - simulate such attacks to test the Bank's defenses such as multi-factor authentication
- Validate internal AI models are working as intended – look out for biases that may lead to inaccurate or discriminatory information

Fraud Regulatory Areas of Focus and Internal Audit's Role in Prevention

Governance Best Practices

Organizations face significant challenges related to external fraud such as first party fraud and victim fraud. Below, are leading practices financial organizations should follow to adequately mitigate fraud risk.

Governance

- **Defining an adequate governance structure** for the organization's risk profile
- **Designating fraud risk management roles and responsibilities** that are in alignment with the organization's strategy and objectives

Fraud Risk Management

- **Creating a risk management system** inclusive of appropriate policies, processes, and control systems consistent with the organization's size, complexity, and risk profile.
- **Implementing internal controls** that appropriately prevent and detect fraud

Fraud Risk Measuring and Monitoring

- **Implementing effective measuring and monitoring practices** to aid management in understanding and identifying fraud losses
- **Employing tools** to properly assess and quantify risk, loss experience, and exposure

Fraud Response and Reporting

- **Implementing adequate processes for timely investigations** of suspected and confirmed fraud
- **Participating in voluntary sharing of information** internally and externally with other private and public organizations

Reviews and Audits

- **Including fraud risk in control reviews and audits** and conducting these in alignment with organization's size, complexity, and risk profile

Fraud Regulatory Focus Areas

Regulatory focus continues to be high in organization's ability to identify fraud, investigations and mitigations, and oversight. Areas receiving increased regulatory scrutiny involve how organization's handle the following elements which Internal Audit Departments must focus this audit programs to cover.

Identification & Tips	Complaints Management	Enhanced Oversight
Identification and escalation of potential cases of fraud, through active monitoring of: • Fraud reports received from employee and vendor hotlines. • Alerts generated by surveillance systems and models/thresholds. • Investigations reports related to non-compliance with guidance and regulations (e.g., market manipulation, red flag indicators, securities registration, telemarketing sales • Trend/fact patterns	Evaluation of the organization's timeliness, substance, and completeness of responses / remediation to customer complains, claims, and disputes as a measure of "fair treatment." They will also consider the clarity of consumer communications, including what is reimbursable as well as the consistency of responses and/or remediation between consumer groups.	Effectiveness of risk and compliance oversight and coordination across the AML / CFT, cybersecurity, and fraud functions. Regulatory attention will also focus on demonstratable, effective Board oversight and implementation of threat detection/monitoring processes that included: • Maturity of endpoint detection and monitoring solutions • Coverage of threat intelligence (both on premises and cloud environments).

Fraud Internal Audit

Enhancements to the fraud risk management framework are vital for an effective program. Therefore, the scope of a Fraud Internal Audit program should include the following:

Fraud Internal Audit

Fraud Risk Coverage

Consistent assessment of fraud risk through **combination of business and functional audits**.

Talent Strategy

Defined **talent strategy** to mobilize resources to keep pace with transformative changes in organization.

Reporting

Synchronized internal audit reporting from individual audit report to senior management and boarding reporting.

Methodology Integration

Fraud internal audit approach unified with existing internal audit methodology and technology.

People

Processes

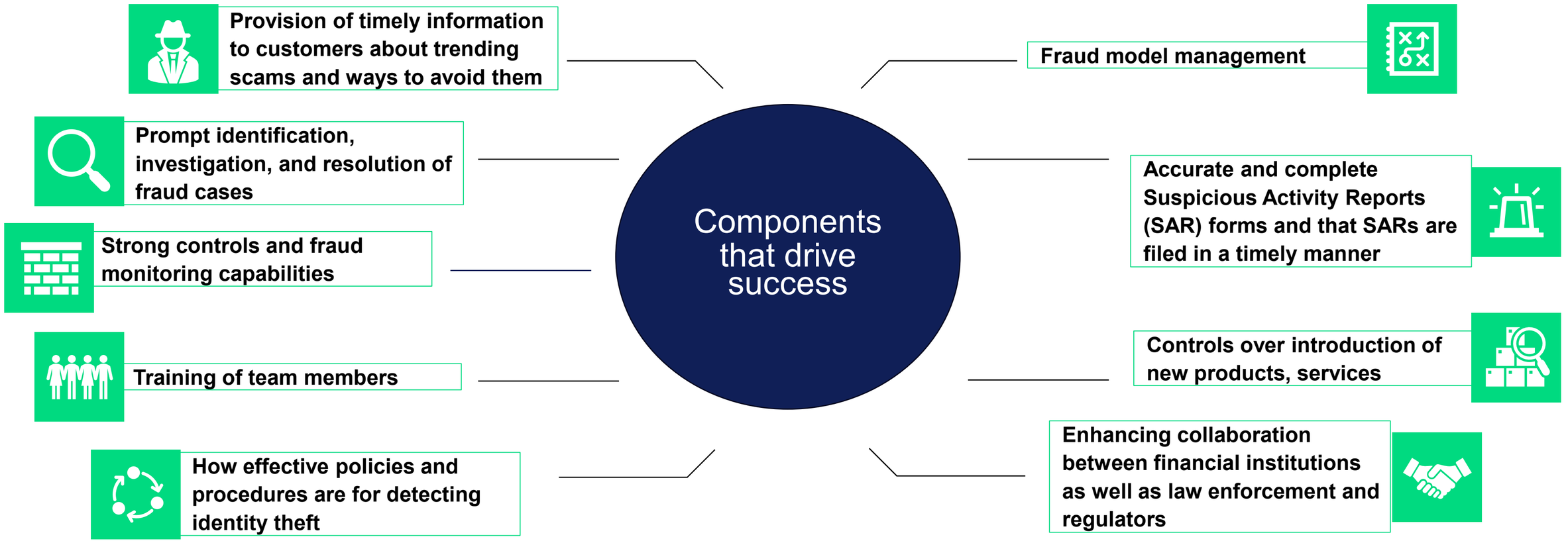
Technology

Fraud Risk Areas in Scope

Product & Service Offerings	New Product/ Service Assessments	Electronic Transactions
Delivery Channels	Monitoring Activities	Fraud Controls
Governance	Checks	Identity Theft

Fraud Audit Program Components

As fraud continues to rise, there is an increased focus on Internal Audit Departments being able to focus on FinCEN priorities[2]. KPMG recommends continuously reviewing your audit program to determine if it includes the key focus areas including those noted below.



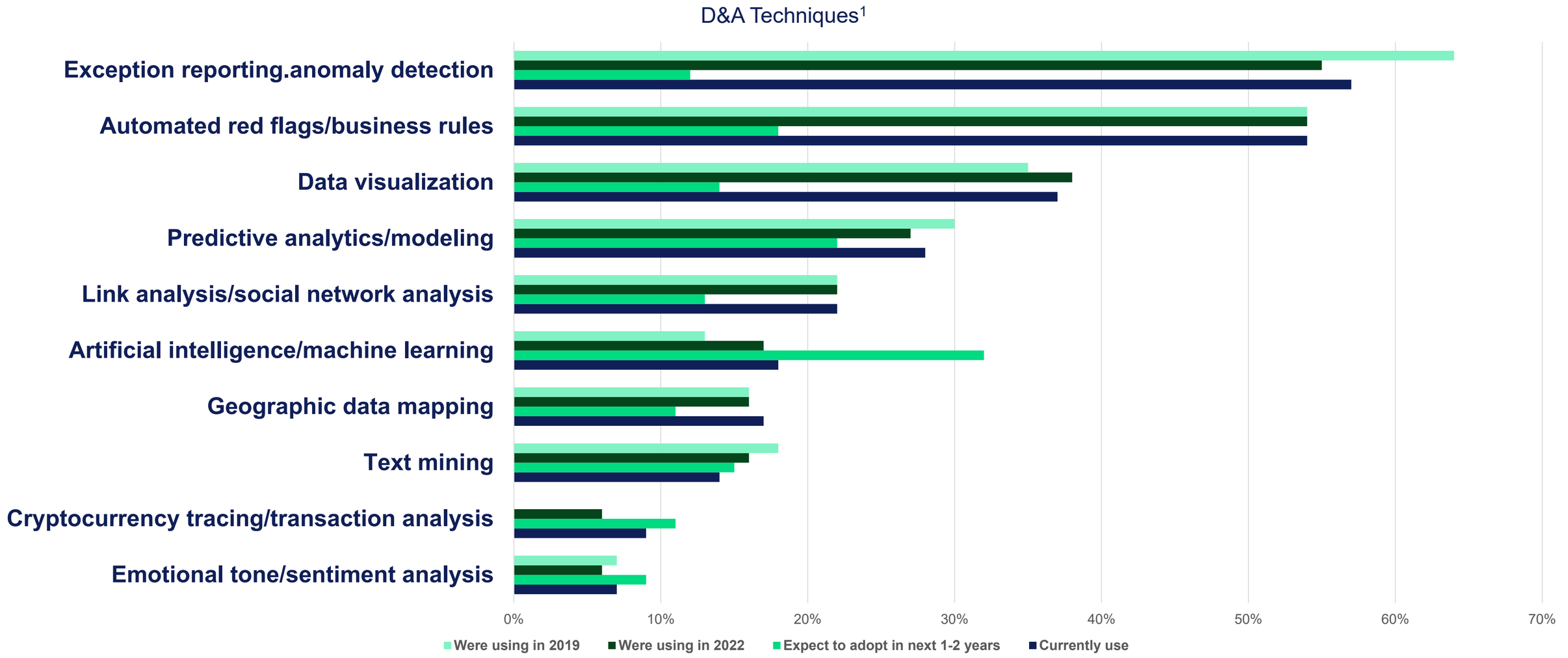
[2] https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

Fraud Internal Control Regulatory Expectations

Effective internal controls are crucial to safeguard against fraud, protect consumers, and ensure the integrity of your operations. Regulators expect robust controls in several key areas.

Control Area	Description
Authorization	Implement strong consent management and customer authentication, such as multi-factor authentication, password protection, one-time passwords, biometrics, third-party access, tokens, and peer-to-peer platforms. All represent **preventative** measures organizations can take.
Risk Management Program	Continuously update your fraud risk management program to keep pace with evolving threats and enhance reporting and consumer protection. Emphasis on: - Reporting on more categories of fraud scams - Defining and clarifying when customers can be reimbursed - Implementing risk programs to identify and mitigate fraud and scams directed at vulnerable customer groups (e.g. elderly, military) - Detecting threats and ongoing monitoring and testing of fraud surveillance.
Data and Reporting	Establish processes to effectively track and trace customer and transaction data, ensuring data quality and accuracy in fraud models.
Resolution/Remediation	Bolster risk mitigation through self-identification, self-reporting, and accountability in response to fraud alerts and customer complaints.

Data Analytics techniques used to fight fraud



[1]Association of Certified Fraud Examiners. (20204). *2024 Anti-Fraud Technology Benchmarking Report*

IA Findings and Recommendations Surrounding Fraud Risk Management

- **Lack of analytics and automation** to client and third-party onboarding
- **Inability to aggregate data and** reporting to have a single view of customers to more effectively manage complex fraud activities and strike a balance between fraud controls and customer experience.
- **Antiquated** technology and evaluate / implement emerging regtech capabilities to enhance transaction monitoring
- **Misalignment between fraud models** to consumer protection regulations, monitor for suspicious activities, and provide real-time notifications and alerts
- **Inconsistent or unformalized process** for sharing information real-time across departments (e.g. fraud, cyber, disputes).
- **Maturity of the conduct risk program**.
- **Inadequate or gaps in** controls in regulatory focus areas (e.g. FinCen priorities)
- **Failures in IAM strategies**, including PAM and MFA to secure access to critical customer systems and data. Regularly review access privileges.
- **Lack of integration in BSA / AML** Requirements into KYC processes
- **Insufficient skills assessment** of staffing needs for day-to-day operations of fraud monitoring identification, investigations, and escalations.
- **Lack of clarity within** consumer communications, including what is reimbursable as well as the consistency of responses and/or remediation between consumer groups.

Issues Management in Fraud Internal Audit

Issues management is a crucial aspect of internal audit in addressing and resolving fraud-related concerns and incidents within an organization. Fraud Focus Areas are **highlighted.**

Completeness of issues inventory capture

Firmwide ratio of issues by originating source (i.e., Self ID vs. 2LOD vs. 3LOD vs Regulators)

Inconsistent application or varying severity definition of issues (issue vs finding vs observation)

Inadequate root cause analysis for issue remediation plan resulting in repeat failures

Aging / increasing volumes of issues

Insufficient planning, tollgates, and in-flight scope changes (e.g., adequate BRDs, business and technology alignment)

Poor management / oversight of "like" or interrelated issues and related dependencies

Various issues management methodologies or source systems

Identification, aggregation, management, and/or monitoring of "thematic" issues and look-across / lessons learned

Increased oversight and testing requirements on "Low" and "Moderate" rated issues

Integration of issue related data into risk assessments

Issues tagged / created at varying inconsistent levels of granularity (e.g., Entity, Business Units, Risks, Controls)

1LOD/2LOD/3LOD role in self testing, challenge, and validation across high-risk issues

Speed to remediate and/or multiple target date extensions degrade regulatory confidence

Regulatory matters categorized as inadequate supervision over the control environment, governance over the issues management lifecycle, and/or ineffective issues management program.

Thank you for attending

Keith Brashaber

Director, KPMG LLP

kbrashaber@kpmg.com

Adrienne Steverson

Director, KPMG LLP

asteverson@kpmg.com

ProSight™

Emerging Fraud Risks: Trends, Red Flags, and Internal Audit's Expanding Role

SESSION SURVEY