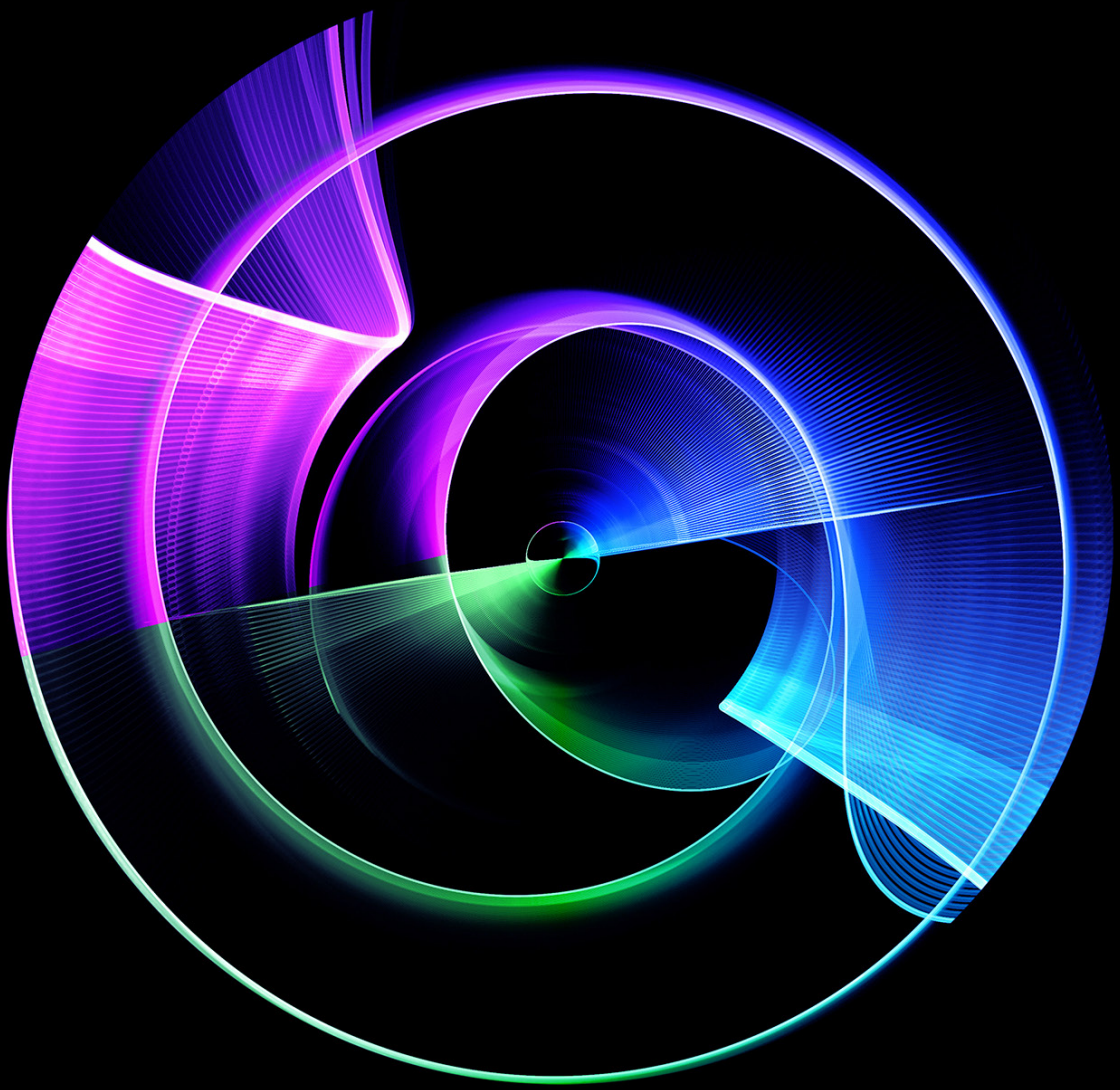
Deloitte.



Digital fraud: The case for change

Executive summary

Digital fraud is a growing threat to financial institutions worldwide. The Carbanak attack in 2015 highlighted the scale and sophistication of modern cybercrimes. Today, the rapid expansion of artificial intelligence (AI) and digital technologies has further exacerbated the risks, leading to significant financial losses. This paper explores the current state of fraud, the challenges faced by financial institutions, and the evolving strategies to combat these threats. It also outlines how Deloitte's Digital Fraud Services can help organizations build a robust fraud risk management ecosystem. To effectively combat digital fraud, financial institutions should not only invest in advanced technologies but also in their human capital.[1] Training and development programs driving behavioral change are crucial to equip employees with the skills needed to detect and prevent sophisticated fraud schemes.

Introduction

In an increasingly digital world, financial institutions are under constant threat from sophisticated cybercriminals. The Carbanak attack in 2015 was a wake-up call, demonstrating the potential scale of digital fraud. As technology evolves, so do the tactics of fraudsters, making it imperative for organizations to stay ahead of the curve.[2] This requires not only technological advancements but also a robust investment in human capital and effective change management strategies so that employees are aware of and well-equipped to handle emerging threats. This paper delves into the current landscape of digital fraud, the challenges faced by financial institutions, and the strategies needed to build a resilient fraud risk management framework.

A new era of cyber fraud

In 2015, Kaspersky Lab, working with INTERPOL and Europol, uncovered one of the largest cybercrimes observed to date. Orchestrated by the Carbanak gang, the attack stole over US$1 billion from customer accounts across more than 100 global financial institutions in the United States, China, Germany, United Kingdom, and Eastern Europe.

The bad actors employed spear phishing to infect bank employees' computers with malware, gaining access to the banks' networks. From there, they employed a multipronged approach to steal funds. This included manipulating account systems to inflate account balances, transferring money directly from the customers' accounts to their own (often routing the funds through banks in China or America), and programming ATMs to dispense cash at predetermined times.

What was remarkable about the Carbanak attack was not only its size and scale, but the length of time before detection. In response to the attack, Sanjay Virmani, Director of the INTERPOL Digital Crime Centre indicated, "These attacks again underline the fact that criminals will exploit any vulnerability in any system. It also highlights the fact that no sector can consider itself immune to attack and must constantly address their security procedures."[3] The bad actors were able to disguise their fraudulent activities behind seemingly legitimate activity and were not detected for nearly two years.

The state of fraud and fraud prevention today

The financial services industry is facing growing complexity and challenges as fraud is continuing to rapidly evolve, resulting in a significant rise in fraud-related risk and losses. In a world where customers interact primarily through digital channels, cyber-enabled attacks are becoming more ambitious in scope and omnipresent, eroding the value of personal information and security protections. In 2023 alone, there was an estimated loss of more than US$1.8 billion through malware-based bank transfers or payments and a 3,100% annual increase in Generative AI (GenAI)—including deepfake voice and video—fraud attempts.[4] This brings to light the deepening connections between cyber breaches and most types of fraud and financial crime.

The rapid expansion of AI and GenAI tools provides the resources for bad actors to scale their attacks, both on the financial institutions and directly to their customers. Deloitte's Center for Regulatory Strategy estimates that the proliferation of GenAI tools could enable fraud losses to reach US$40 billion in the United States[5] by 2027, up from US$12.3 billion in 2023, a compound annual growth rate of 32%.

Many organizations today are struggling to identify and mitigate sophisticated attacks and are faced with the challenges of lack of an end-to-end fraud strategy, siloed fraud detection and prevention efforts, ineffective tooling, and vulnerabilities within their ever-evolving fraud attack surface. Whereas organizations acquired several tools over the past few years in response to individual control gaps, sometimes leading to increased costs and redundancies, there is a broad recognition that this "whack-a-mole" type of approach to these interconnected risks is becoming increasingly untenable, and at leading organizations, the push is on to bring together efforts on cyber, fraud, and financial crime.

How financial institutions are evolving

Movement toward centralization for fraud risk management

Modern experiences demand faster risk decisions, and organizations must strike the right balance between friction and fraud. Recognizing that fraud risk is expected to grow, financial institutions are evolving their operating models, tools, and people to better respond to the growing threat of digital fraud. Central to this evolution is the investment in human capital, including regular training programs, cross-functional collaboration, and leadership development to build a fraud-resilient workforce.[6]

Similar to the journey that cybersecurity underwent over a decade ago, fraud risk management is moving away from a federated model, in which each product or business line team develops their own fraud risk strategy, to a more integrated, hub-and-spoke fraud mitigation team. Whether this centralized team sits within Information Security, Risk, Compliance, or another organization, they often have similar responsibilities, including:

- Identification of fraud risks, including maintaining a centralized fraud risk taxonomy and collaboration with peer institutions on new or evolving fraud schemes.
- Managing a centralized tools and technology strategy. This often includes a centralized fraud data asset.
- Defining standards and leading practices for fraud detection within different lines of business teams. These may include benchmarks for fraud prevention and detection efforts, as well as minimum controls required.
- Managing centralized reporting, including the prevalence of fraud attempts, gross fraud losses, and net fraud losses, as well as key operational metrics within the fraud program.
- Owning responsibility for regulatory requirements related to fraud risk mitigation, including those involved in settlements.
- Identification of training needs across boards of directors, senior management, and operational product teams, and spreading awareness throughout the enterprise on leading fraud schemes.

At the center of this organization is a leader tasked with building an organizational strategy for fraud mitigation. These individuals are technology-savvy, data-driven, and well-connected with peer institutions.

Getting started

Financial institutions are faced with the challenge of reshaping the structure and function of teams and the technology that supports fraud management to account for newly emerging threats. Below are five considerations for organizations to consider in their journey to build a more resilient fraud risk management ecosystem.[7]

1. **Assess end-to-end risks**
   At the heart of a centralized fraud strategy is an assessment of fraud risks throughout the customer journey. This includes account onboarding, login (including transaction authentication), transaction monitoring, and claims and disputes. By identifying the opportunities for fraud, organizations can map vulnerabilities against capabilities for fraud risk management and determine a technology strategy accordingly.

2. **Set the foundation with a fraud management governance model**
   Effective fraud risk management occurs through a clear governance structure, including roles and responsibilities between product teams and departments (e.g., information security) playing a role in preventing, detecting, and responding to fraud. In addition to the interaction model, a set of fraud policies and standards should be in place, backed by fraud reporting mechanisms, metrics, and dashboards to collect and distribute critical information between the governance parties.[8]

3. **Revisit data and technology investments**
   The effectiveness of a fraud detection system is significantly influenced by both the quality and the variety of the data it can access. Technology that captures customer identity, behavioral, and transactional data across each stage of the customer life cycle enables enhanced detection strategies. Siloed detection systems that do not provide interoperability and the easy transfer of data can create system gaps that fraudsters aim to exploit.

4. **Build customer fraud prevention awareness programs**
   Regardless of how robust the control framework is, the human element remains the most crucial defense against fraud. Most institutions have built programs to educate their investigations teams on the latest schemes and conduct cross-team training between teams supporting both fraud and financial crime, but leading institutions are considering customer education as well, including periodic communications over email and through in-app alerts, about how customers can further safeguard their accounts.

5. **Establish a tech-savvy team**
   Building a resilient fraud risk management ecosystem requires assembling a tech-savvy team with a mix of technical and fraud detection and prevention subject matter domain knowledge. Financial institutions can focus on becoming a destination for top technical talent by addressing tech talent's motivators, including creating meaningful work opportunities designed around a fraud technology strategy, attracting tech talent with competitive compensation, and emphasizing strong company reputation and culture.[9]

How we can help

Our Digital Fraud Services brings together cybersecurity, forensic, risk, regulatory, artificial intelligence, data, and human capital capabilities and industry experience to transform how financial institutions prevent, detect, and respond to fraud events. Here's how Deloitte[10] can assist your organization in combating digital fraud:

1. Greenhouse Lab and fraud risk assessment

- **Greenhouse Fraud Insight Lab:** We often start working with organizations through a Greenhouse Lab, a collaborative environment designed to foster innovation and problem-solving. In this lab, we bring together key stakeholders to brainstorm and develop innovative solutions for fraud detection and prevention. This includes understanding pain points, fraud risks, and existing fraud mitigation capabilities.[11]
- **Fraud risk assessment:** Conducting a comprehensive fraud risk assessment helps in identifying vulnerabilities and gaps in an organization's current fraud management framework. This assessment can include the development of a business case for investments in people or technology, or a set of objectives for a new fraud leader.

2. Development and implementation of fraud tools

- **Tool configuration and implementation:** As financial institutions look to develop a new fraud toolset or rationalize the tools they already have, we assist with the configuration and implementation of these tools. This includes integrating advanced technologies such as machine learning models to enhance fraud detection and prevention capabilities.[12]
- **Analytics and machine learning models:** We help in the analysis of data to identify patterns and anomalies that could indicate fraudulent activities. We have built accelerators, including a library of machine learning use cases, a list of more than 80 foundational detection scenarios, and critical data points for organizing to hit the ground running with enablement of fraud analytics and AI.

3. Centralized fraud management strategy

- **Centralized tools and technology strategy:** We assist in managing a centralized tools and technology strategy, often including the development of a centralized fraud data asset with the goal that all fraud detection and prevention efforts are streamlined and effective.
- **Policies, procedures, and leading practices:** We help define policies, procedures, and standardized leading practices for fraud detection and investigation across business teams and geographies. This includes advising on benchmarks for fraud prevention and detection efforts, key performance indicators, and establishing minimum controls.

4. Regulatory compliance and reporting[13]

- **Regulatory requirements:** We provide guidance on meeting regulatory requirements related to fraud risk mitigation. This includes providing advisory services for consumer protection, complaints, chargebacks, and disputes programs, among other regulatory obligations.
- **Centralized reporting:** We help manage centralized reporting, including the prevalence of fraud attempts, gross fraud losses, and net fraud losses. We also assist in developing key operational metrics within the fraud program.

5. Human capital development[14]

- **Training and development programs:** We provide assistance with designing and implementing training programs for employees across the enterprise to stay updated on the latest fraud schemes and prevention techniques. This includes specialized training for boards of directors, senior management, and operational product teams, as well as cybersecurity and financial crime teams that often have a supporting role in fraud prevention and detection.
- **Leadership development:** As you identify leaders who are adept at navigating the complexities of digital fraud, we can collaborate with you to design leadership development programs to nurture their growth.

6. Customer education and awareness

- **Customer fraud prevention programs:** We help institutions build customer education programs, including periodic communications over email and through in-app alerts about how customers can further safeguard their accounts. This proactive approach helps in reducing the risk of fraud by empowering customers with the knowledge to protect themselves.[15]
- **Multichannel communication strategy:** A multichannel communication strategy can be used so that fraud prevention messages reach customers through their preferred channels. This includes emails, social media, mobile apps, and even in-branch communications. Content can include interactive learning models to make customer education more engaging, as well as case studies and real-life examples of fraud incidents to make the education process more relatable and impactful. A consistent and widespread approach increases the likelihood that customers will engage with and absorb the educational content.

Call to action

Digital fraud is an ever-present threat that requires constant vigilance and proactive measures. Financial institutions should assess their current fraud risk management frameworks, invest in advanced technologies, and foster a culture of collaboration and ongoing improvement. By taking these steps, organizations can build a robust and resilient fraud risk management ecosystem that effectively addresses the evolving threats in the digital landscape. Deloitte's Digital Fraud Services is here to support you in this journey, providing the skills, knowledge, and tools needed to help combat digital fraud effectively.

Contact us

Satish Lalchand
Principal | Deloitte Transactions and Business Analytics LLP
slalchand@deloitte.com

Alex Bolante
Managing Director | Deloitte & Touche LLP
abolante@deloitte.com

Tara Mahoutchian
Principal | Deloitte Consulting LLP
tmahoutchian@deloitte.com

Endnotes

1. Deborah Golden et al., "Earning digital trust: Where to invest today and tomorrow," Deloitte Insights, February 16, 2022.
2. Satish Lalchand, Jill Gregorie, and Val Srinivas, "Using biometrics to fight back against rising synthetic identity fraud," Deloitte Insights, July 27, 2023.
3. Kaspersky, "The great bank robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide," press release, February 16, 2015.
4. Onfido, Identity fraud report 2024, November 2023.
5. Satish Lalchand et al., "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking," Deloitte, May 29, 2024.
6. Saad Qureshi and Humaid Hussain, "The need of the hour: Stepping-up counter fraud controls in the banking sector," Deloitte, 2022.
7. Nancy Albinson et al., "How CDOs can manage algorithmic risks," Deloitte Insights, June 7, 2018.
8. Mike Brodsky, Holly Tucker, and Sofia Hussain, "A proactive defense: A survey on the fraud risk assessment experience," Deloitte, 2023.
9. Deloitte, Winning the war for tech talent in FSI organizations, February 2022.
10. As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, Deloitte Transactions and Business Analytics LLP, Deloitte & Touche LLP, and Deloitte Consulting LLP, which are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.
    This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.
    Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.
11. Deloitte, Deloitte Greenhouse® Virtual Breakthrough Labs, accessed September 2024.
12. Lalchand et al., "Using biometrics to fight back against rising synthetic identity fraud."
13. David Kuczma et al., P2P fraud challenge: Mitigating risk in a changing digital and regulatory landscape, March 2023.
14. Deloitte, Human Capital Consulting, accessed September 2024.
15. YEC Expert Panel, "Eight effective methods for educating consumers about cybersecurity," Forbes, March 31, 2023.

Deloitte.

About Deloitte.