SEON FINTRAIL

GUIDE

Collaborative Strategies for Mitigating Fraud Risks in Digital Banking Expansion

Leading Global Fraud Prevention

SEON.IO

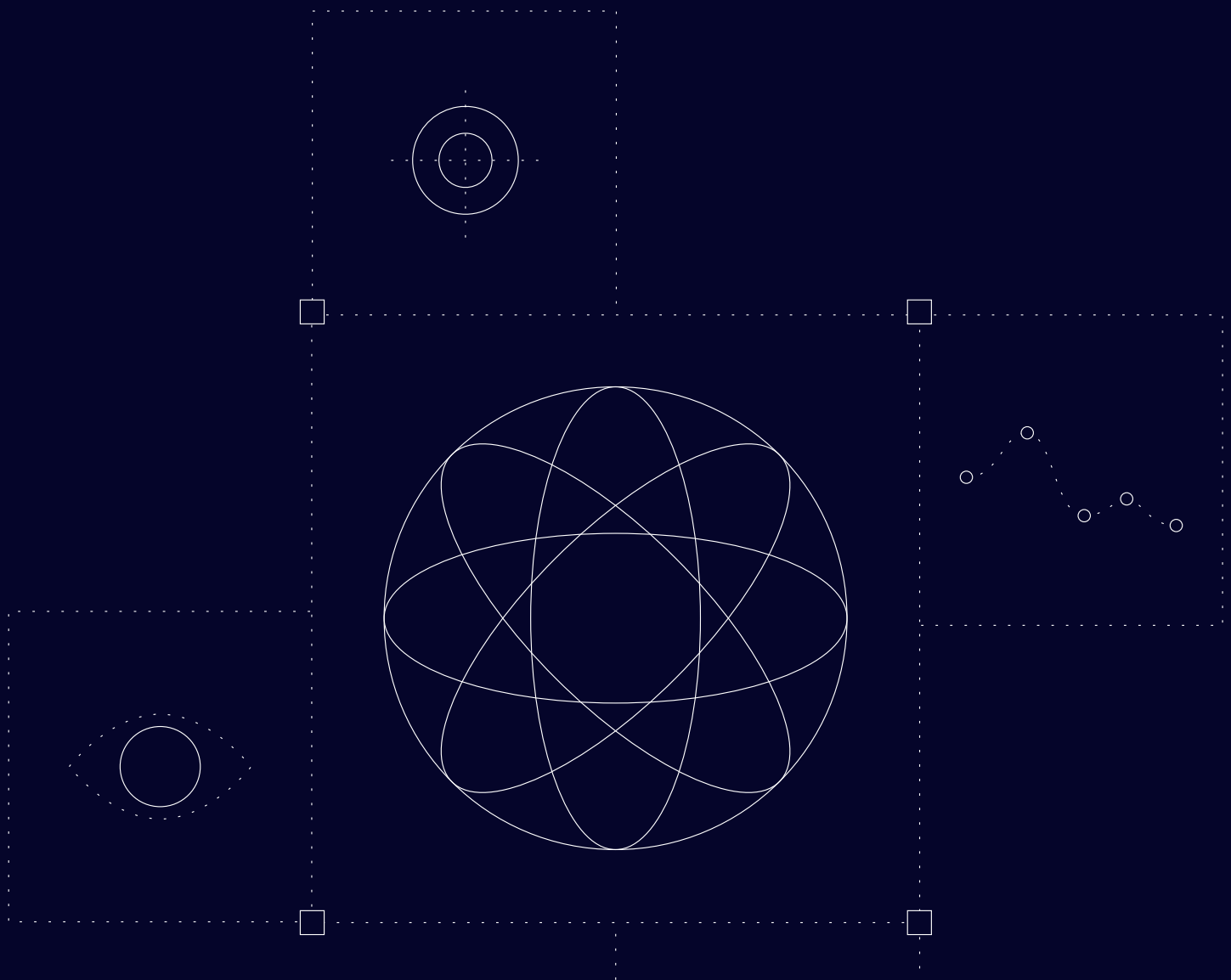


Table of Contents

Introduction

Digital banking is experiencing rapid growth, particularly in emerging markets where the need for financial inclusion is driving innovation. Regions like Africa, Asia-Pacific (excluding China), Latin America and the Middle East are at the forefront of this expansion, with revenues expected to rise from 15% of global fintech revenues in 2023 to 29% by 2028[1].

However, this rapid growth comes with significant challenges. Fraudsters are exploiting vulnerabilities created by new markets and innovative products, often outpacing the defenses of financial institutions.

Most criminal groups and fraud rings operate with remarkable organization, access to advanced technologies and robust funding. Unencumbered by bureaucracy or regulatory constraints, they can adapt and scale their operations with agility, posing a massive threat to businesses and institutions alike – and they have one objective: to profit at any cost.

Expected digital banking revenue growth in emerging markets

1 McKinsey & Company

The speed at which organized groups can adapt technology and exploit weaknesses far exceeds the responsiveness of financial service firms. One report[2] noted that some banks are 23 months "behind the bad guys" when detecting financial crimes. In 2023, NASDAQ estimated that fraud schemes totaled $485.6 billion in projected global losses[3]. To protect themselves and their customers, digital banks today must clearly understand their vulnerabilities and have a strategic plan leveraging technology to strengthen their defenses.

To secure growth while maintaining customer trust, digital banks must focus on two critical areas to mitigate fraud risks during expansion: first, thoroughly understanding their fraud risks and product challenges to implement tailored controls, and second, prioritizing data integrity and leveraging high-quality, context-rich signals. While consortium-based collaboration plays a role, it is just one layer of a comprehensive strategy. By embracing a defense-in-depth approach – where layered solutions combine to protect against threats from all angles – digital banks can stay ahead of fraudsters and ensure secure, sustainable growth.

Understanding Fraud Risks in Market Expansion

Fraud risks in digital banking are diverse and constantly evolving, fueled by the sector's expansion. Entering new markets exposes digital banks to localized fraud schemes that may be unfamiliar, while launching innovative products, such as cryptocurrency wallets or instant loans, introduces new fraud vectors. A 2022 report by IBM[4] highlighted significant regional disparities in fraud losses, with Germany experiencing three times the losses of Singapore, demonstrating the importance of understanding localized nuances.

Analysis by the European Banking Authority and the European Central Bank[5] affords a detailed picture of the evolving landscape of payment fraud and how it can manifest differently based on numerous factors:

- 79-82% of credit transfers and card payments during the review period were domestic, with the majority of fraud cross-border.
- 92% of fraud by value in card payments, cash withdrawals and e-money transactions stemmed from fraudulent payment orders issued directly by perpetrators.

2 The Banker

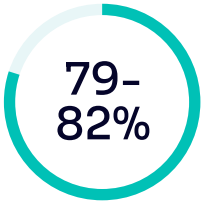
3 Nasdaq Global Financial Crime Report

4 IBM Global Financial Fraud Impact Report

5 EBA and ECB 2024 Report on Payment Fraud

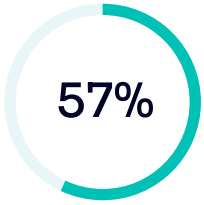
- 57% of fraud resulted from manipulating unsuspecting payers into initiating transactions showcase, often using social engineering.

Digital banks' vulnerabilities often depend on the type of product or service offered. Digital wallets, for example, are frequently targeted for account compromise, while peer-to-peer lending (P2P) platforms may struggle with borrower impersonation. Onboarding processes are another concern, as they are particularly susceptible to synthetic identity fraud, which combines real and fabricated information to create false identities. Addressing these challenges requires a proactive approach to identifying potential weaknesses and adapting to local fraud dynamics. Fraud risks differ from country to country depending on consumer preferences, online behaviors and fraudsters' market penetration. Understanding these variations enables digital banks to implement tailored strategies and controls, ensuring they are well-prepared to mitigate threats and protect their business and customers.



of domestic payments, majority of fraud cross-border

of fraud involved direct payment orders from perpetrators



of fraud used social engineering to manipulate payers

Case Study: US Social Security Numbers

In 2022, a US individual was sentenced for his role in a fraud ring that used stolen social security numbers (SSNs), including those of children, to create synthetic identities. These fabricated identities were used to open credit lines and steal nearly $2 million from financial institutions.[1] Firms expanding to the US and using SSNs for the first time should know how they can be misused. SSNs are highly valuable for committing fraud because they serve as a key identifier across multiple systems, allowing fraudsters to impersonate other people in numerous scenarios.

Organizations often over-rely on SSNs as a secure identifier despite their vulnerability to theft. Unlike passwords or PINs, SSNs are not easily changed once compromised. They can also be cross-referenced with public and private databases to gather additional information, enabling more sophisticated fraud schemes.

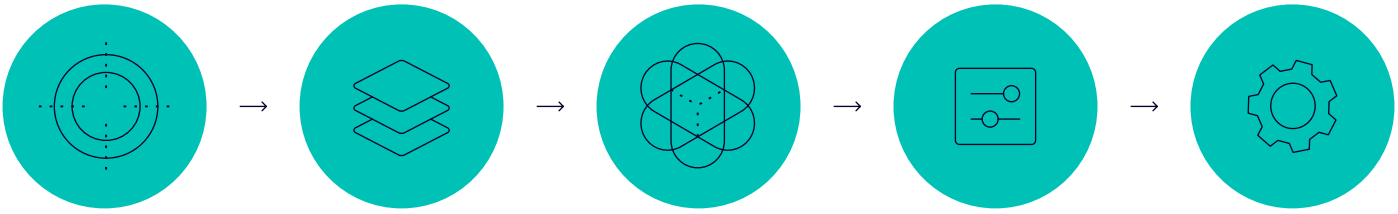
1 US Department of Justice

Mapping Out Product Vulnerabilities

Every product or market in a digital bank's portfolio has inherent risks that fraudsters can exploit. For example, a phishing ring in Spain stole over €5 million using fraudulent links and follow-up calls to gather personal data. The stolen credentials were then used to withdraw funds, transfer money overseas or convert it into cryptocurrency[6]. Such incidents highlight the importance of mapping vulnerabilities to mitigate risks effectively.

A structured fraud risk assessment is essential when entering new markets or launching new products.

This process begins by evaluating how fraud exposure may shift due to business changes, such as entering a new region or offering a novel product. Insights into relevant fraud typologies can be gathered from local law enforcement, national financial intelligence units and risk assessments. Existing controls should then be mapped against identified risks to uncover gaps and weaknesses. Clearly defining the organization's fraud risk tolerance ensures that efforts are prioritized effectively. Once vulnerabilities are mapped, the next step is to translate these insights into effective controls that address specific fraud typologies and adapt to evolving threats.



Identify Risks

Evaluate market-specific fraud typologies

Map Controls

Overlay existing controls to assess

Gap Analysis

Identify weaknesses in current defenses

Define Risk Tolerance

Set acceptable risk thresholds

Implement Tailored Controls

Adjust controls to address gaps

6 Eurojust

Informing Downstream Controls

Fraudsters often operate on an industrial scale, using automation and continuous experimentation to bypass controls. These sophisticated attacks are frequently impossible for analysts to detect manually. While human oversight remains crucial, fraud prevention measures must be complemented by advanced technology capable of identifying unusual patterns and interconnected fraudulent activities.

Potential frameworks and controls across a customer lifecycle could include elements of the following:

- **Identity verification and likeness checks:** Preventing fraudsters from exploiting lax KYC procedures with stolen or synthetic identities.
- **Risk-based authentication:** Dynamic systems that evaluate login attempts and trigger additional checks for high-risk activities.
- **Behavioral monitoring:** Using AI to detect anomalies in user behavior, such as unusually frequent logins or sudden changes in transaction patterns.
- **Dynamic risk scoring:** Continuously evaluating customers' risk levels based on new patterns and market-specific intelligence.
- **Continuous monitoring:** Leveraging machine learning models that evolve with emerging fraud patterns.

By proactively mapping vulnerabilities and implementing these controls, digital banks can quickly minimize vulnerabilities and respond to threats.

Case Study: Regional Expansion

A digital bank launching in a new geographic region overlooked the prevalence of SMS-based phishing attacks in that market. Fraudsters exploited this gap, leading to significant losses and reputational damage.

Proactively mapping vulnerabilities and adapting controls to local threats, such as using real-time monitoring systems to detect suspicious transactions initiated after customer activity, like password changes or new device logins, could have mitigated this risk.

Adopting Proactive Measures

Digital banks must invest in systems that can adapt in real time. AI and data analytics enable fraud detection by identifying patterns, predicting risks and responding to suspicious activities as they occur. Proactive measures not only minimize fraud losses but also reinforce customer trust.

Tactics for strengthening fraud prevention include:

- Using onboarding data to establish a baseline of normal behavior for ongoing monitoring.
- Pairing strong customer education with technical measures like two-factor authentication (2FA) and behavioral monitoring.
- Deploying real-time transaction monitoring systems to detect suspicious activities and refining models to improve post-transaction detection.

Prioritizing Data Integrity and Contextual Signals

Fraud is a collective challenge, but effective prevention demands more than collaboration alone – it requires high-quality data, contextual understanding and strategic layering of defenses. Consortium-based collaboration, while valuable, is just one layer in a robust fraud prevention strategy. A defense-in-depth (DiD) approach is essential to secure growth and maintain customer trust, combining diverse solutions to address threats from all angles.

Consortiums, such as Cifas in the UK or Mastercard's MATCH system, provide valuable shared intelligence that accelerates fraud detection. However, more than consortium data is required. The insights depend on the quality of shared signals, and competing interests can lead to delays or incomplete data.

Digital banks should focus on signal quality and data integrity to mitigate these limitations. Banks can develop a more accurate and contextualized risk profile by leveraging diverse, enriched signals – including behavioral patterns, device intelligence, and real-time transactional data. Advanced technologies such as machine learning further enhance this layered approach, allowing for proactive anomaly detection and better adaptability to evolving fraud schemes.

For example, combining consortium data with dynamic risk modeling and real-time monitoring allows banks to detect coordinated phishing scams targeting multiple institutions while minimizing false positives. Integrating consortium insights with proprietary data ensures fraud prevention efforts remain actionable and contextually relevant, enhancing operational efficiencies.

Ultimately, the success of a DiD strategy depends on moving beyond reliance on past data and static flags. Instead, digital banks must adopt a proactive, layered model that blends shared intelligence with cutting-edge technology and contextual analysis. By doing so, they can stay ahead of fraudsters, protect customer relationships and achieve sustainable growth in even the most challenging markets.

Closing the Gap: A Unified Approach to Fraud Prevention

By understanding fraud typologies and product vulnerabilities, digital banks can implement tailored prevention strategies that address specific risks during expansion and growth. The future of fraud prevention lies in unity – combining technological advancements with collaborative ecosystems to safeguard customers and maintain trust. By embracing this approach, digital banks can secure growth while fostering innovation and confidence in the rapidly evolving digital financial landscape.

Case Study: Cross-Jurisdictional Collaboration

In 2020, a cyber-fraud ring that exploited stolen payment card details to make unauthorized purchases was dismantled by an international investigation led by US and European agencies. Coordinated efforts across multiple jurisdictions ensured the arrest of key suspects and the recovery of financial losses.[1]

1 Europol

About SEON

SEON is the leading fraud and money laundering prevention solution transforming how top-tier risk teams fight fraud. By combining real-time digital footprint analysis, device intelligence and a customizable AI-driven rules engine, SEON empowers businesses across industries to detect and prevent potential threats before they happen. Trusted by over 5,000 global companies across igaming, fintechs, financial services, payments and retail companies, SEON has stopped $200 billion in fraud costs to date, earning trust and recognition with 300 reviews across G2, Capterra and the AWS Marketplace as the leader in fraud detection software. The company is the recipient of Deloitte's Technology Fast 50 and G2's Fastest Growing Software award and operates globally from its Austin, London and Budapest offices. Learn more at seon.io.

Speak with an expert

About FINTRAIL

FINTRAIL is a global financial crime consultancy. We've worked with over 100 leading global banks, FinTechs and other regulated financial institutions to implement industry-leading approaches to combatting money laundering, fraud, and other financial crimes. With significant hands-on experience, we can help you navigate the complexities of managing your fraud risks, delivering bespoke fraud risk assessments, independent fraud reviews, and targeted training to fortify your defenses and meet evolving regulatory requirements. Visit fintrail.com to learn more.


SEON