Impact Study

In association with:

Brighterion, a Mastercard company

# 8 Steps to Efficient Transaction Fraud Monitoring

# Contents

# 01 | The current state of card transaction fraud

In the wake of the widespread shift to digital banking and ecommerce, fraud teams have seen a sharp increase in card transaction fraud. This has been an upward trend for some time. Since 2014, card transaction fraud has increased by an average of 8.9% per year and exceeded $32 billion in losses in 2021 alone. By 2028, this number is predicted to reach $91 billion.

In an increasingly complex threat environment, card transaction fraud has devastating consequences for banks and merchants alike. For these reasons, organisations must do all they can to protect themselves against fraud. Different stakeholders, including issuers, banks, payment processors, and merchants, are turning towards new and emerging technology to enhance their fraud mitigation tools and strategies.

Technologies like the cloud, artificial intelligence (AI) and machine learning (ML) pave the way for innovative fraud solutions. Yet, in order to effectively deploy these tools, banks need to address their underlying risk strategies, technical infrastructure and the quality of their available data.

This impact study explores the eight steps for banks to reach transaction fraud monitoring excellence.

# 02 | 8 steps to efficient transaction fraud monitoring

## Step 1: Identify fraud solution use case and implementation method

Today, fraud poses an increasingly complex and prevalent threat to financial institutions and merchants alike. In order to mitigate risk, banks need to determine which fraud solution to implement for which type of fraud. Yet the challenge lies in the diverse fraud environment they are facing. Building a holistic customer risk score based on multiple types of fraud allows acquirers to assess and manage risk across all aspects of a customer's relationship with the bank.

### The most common fraud types:

| | |
|---|---|
| PHISHING | In many cases, card transaction fraud begins with a phishing attack. Using social engineering techniques, fraudsters trick victims into revealing sensitive information. Popular phishing techniques include emails impersonating legitimate sources, such as banks or corporations, with urgent calls to action that trick victims into clicking on malicious links. |
| CREDIT CARD SKIMMING | Credit card skimming is another way fraudsters gain access to card information. Fraudsters attach small devices known as 'skimmers' to PoS machines and steal card information when the machine is used for a transaction or to withdraw cash. |
| CREDIT CARD APPLICATION FRAUD | Credit card application fraud is based on identity theft. Fraudsters use stolen information to apply for credit cards, which can often go undetected until the victim checks their credit score or applies for another credit card. |

**CARD-NOT-PRESENT FRAUD**

Card-not-present fraud occurs when a fraudster uses a person's card information, instead of the physical credit card, to make an unauthorised transaction online or via the phone.

**LOST OR STOLEN CARDS**

One of the most common types of credit card fraud occurs when cards are lost or stolen. Fraudsters then make unauthorised purchases until the card is frozen by the victim.

**ACCOUNT TAKEOVER**

During an account takeover, fraudsters use stolen information in order to contact the credit card company and change sensitive information such as PINs or passwords. The victim will no longer be able to use their card.

**FRIENDLY FRAUD**

Friendly fraud occurs when a cardholder disputes a legitimate purchase. This can happen:

- due to confusion, when a customer doesn't recognise a transaction on their statement;
- when a customer wants to bypass a merchant's refund policy and files a reimbursement claim directly with their card provider;
- or out of malintent, when a customer uses a reimbursement claim in order to receive both the product and reimbursed funds.

Acquirers need to find a fraud prevention solution that allows them to consolidate numerous fraud risk signals into a single, holistic assessment. Every fraud case is unique, which means that there are many factors to consider when determining a bank's ideal method.

### Rule-based fraud prevention systems

Rule-based fraud detection identifies fraudulent activity based on sets of pre-determined attributes, such as location, time stamps and frequency, as well as account numbers. Any activity deemed to be unusual will then be flagged as potentially fraudulent. Examples include purchases outside of the common area for the customer, an increase in unusual transactions for the customer profile, as well as transactions to/from unfamiliar accounts that have been newly created.

The advantages of rule-based fraud prevention systems lie in their transparency; however, they are reactive rather than proactive and can be prone to blind spots. Rule-based system also rely on thousands of rules to increase accuracy, which makes them comparatively slow and harder to manage than other fraud prevention methods.

### Cloud technologies

Cloud providers are subject to thorough scrutiny and adhere to high security standards. The cloud gives banks access to immense computing power, which is fast and precise in detecting fraud, offers dynamic scaling and provides additional layers of security and cost efficiencies. Additionally, many cloud providers include fraud detection tools in their services, so the combined effort of provider and bank can help detect and mitigate risks.

### Multi-factor authentication and biometrics

Passwordless authentication methods are being increasingly adopted among banks and financial institutions in order to mitigate fraud. Biometric authentication relies on biological characteristics to verify users, making identity theft nearly impossible. Voice biometric authentication is another method that is starting to be used by customer call centres to combat fraud.

### Machine learning (ML)

Traditional rule-based fraud prevention systems can be enhanced with ML capabilities to mitigate fraud more quickly and effectively. While traditional methodologies would not be capable of identifying new patterns, ML-based fraud prevention systems can analyse patterns in data to predict and respond to new conditions for which they were not initially programmed or trained for. Since the algorithm is designed to detect patterns in huge transaction volumes, machine learning additionally helps decrease false positives. ML detection methods arguably provide the strongest defence against fraud, as they are capable to learn from each fraud cycle and continuously improve over time.

## Step 2: Integrate fraud solution with data flows and decisioning platforms

In order to effectively detect and mitigate fraud, banks need rich data flows that inform their decisions. But to do that, banks will need to unify siloed data pools across their organisation. Fragmented data across different geographic locations, departments or systems can create barriers between cybersecurity, fraud mitigation and anti-money laundering teams that weaken the company-wide effectiveness at fighting financial crime. Integrating these various data points into a single fraud information exchange will inform the chosen fraud solution in the most effective way.

Secondly, effective decision making can only take place with contextual data. Even after data pools are unified, the question remains whether banks can leverage their data in the right way. Banks need to have the right infrastructure in place to ensure the right data is fed through to the decisioning platforms.

McKinsey research found that 75% of banks have only just started their advanced analytics efforts and are still experimenting with the setup of their solutions. And this isn't just relevant to combat financial crime. For example, leveraging data and advanced analytics to build a unified and intuitive platform withing the CRM system will help banks gain a better understanding of customer behaviour, which in turn will help inform their fraud detection efforts. Data, combined with the right technology, enables both issuers and acquirers to develop models that allow for reduced fraud and increased transaction approvals.

The availability of pre-trained, market-ready models allows acquirers and PSPs to more easily integrate a fraud solution into their decisioning platforms. This removes the need to share historical data batches, though datasets can be added for further optimisation. Pre-trained models additionally decrease the time needed for a solution to be ready for deployment.

## Step 3: Enhance AI scoring with rules to address business needs

In today's complex fraud environment, automation and AI are critical components of a bank's fraud mitigation strategy. In order to build better risk profiles and reduce card transaction fraud, automation helps PSPs and acquirers to detect risky merchant behaviour, and AI provides automated risk scoring engines that are based on self-learning algorithms. AI-enhanced fraud solutions are able to connect multiple data points to detect these emerging patterns that can easily be overlooked by human analysts.

For further enrichment of their fraud detection solution, PSPs and acquirers can complement their AI scores with additional rules, which is often used to achieve specific business goals or meet regulatory requirements. Enhancing AI scores with custom rules allows banks to combine the speed and efficiency of AI-based frameworks with the increased control, flexibility and adaptability of rule-based methods.

## Step 4: Choose decisioning score threshold based on risk appetite

Risk management is an integral part of a bank's governance and corporate management mechanisms. It provides a framework for identifying and managing uncertainty, taking managed risks and preparing successful responses. An effective risk management strategy helps banks balance risks and opportunities and supports informed decision making.

When it comes to card transaction fraud, financial institutions need to carefully determine their risk appetite. Both qualitative and quantitative data can help to weigh up the risks and define key risk indicators (KRIs). A bank's KRI is a metric that combines the probability of an event with its expected consequences in order to provide an early warning to adverse potential events.

There are three steps to determine a bank's risk appetite.

1. Defining risk drivers
2. Setting up KRI thresholds
3. Determining outcomes of KRI breaches

Firstly, banks need to establish an understanding of both the nature and methods that are driving fraud and financial crime in an increasingly complex threat landscape. This will allow them to define their most pressing risk factors, which will in turn inform their KRI thresholds. For example, the number of customer calls to report identity theft can serve as a KRI to account takeover fraud. Anomalies in the average, meaning an increasing number of calls, can indicate an increase in operational errors or intentional mistakes that are driving complaints. Other factors, such as the outsourcing of key activities or expansion into new markets also impact fraud KRIs.

Additionally, acquirers and PSPs need to determine where they want to land on the trade-off scale of fraud detection and customer experience. If they set more granular decisioning scores to catch more fraud, they also face a higher risk of flagging false positives, which damages the customer experience. On the other hand, focusing on minimising false positives can lead to a higher number of fraud cases that slip through detection. This sliding scale is another factor that businesses need to consider when defining their risk appetite.

Once the KRIs have been set up, banks need to determine thresholds based on the severity of a KRI breach. This involves planning for responses and measures should the KRI be breached. The combination of these responses can help financial institutions implement fraud mitigation and risk acceptance measures within the organisation.

## Step 5: Optimise investigative efficiency with case management automation and workflows

Case management workflows are another important factor that is needed to create a holistic view of a bank's fraud mitigation efficiency and help improve investigative effectiveness. Should a bank not have a unified case management system, investigations are siloed, directly hindering an investigator's ability to perform, and the bank's risk will increase. Inefficient case management is often caused by legacy technology and siloed teams.

Similar to earlier points, access to data is crucial for case management and data silos need to be eliminated. Increased connectivity and sharing data between teams in order to automate procedures and help to build traceability is crucial for the mitigation of financial crime. In order to streamline their case management, banks need to adapt a single, unified case management solution that is resilient, agile, scalable and intelligent enough to provide a holistic view of the institution's risk.

Using the right case management solution will enable acquirers and PSPs to set up more accurate risk scoring as well as automate workflows. This boosts the efficiency of case management teams, allowing the analysts to spend less time chasing empty leads and more time working the cases that have the highest impact.

## Step 6: Monitor performance with reporting and analytics tools

Once banks have put all of these fraud detection and mitigation processes in place, they need to monitor their performance to determine their effectiveness. Based on how effective (or ineffective) their new measures are, they can determine whether or not any part of the strategy, data or solutions needs to be adjusted.

Additionally, by monitoring the fraud data itself, forward-thinking financial institutions can build an intimate understanding of risk profiles and leverage this information to develop new and tailored products. The information collected by organisations on merchants and customers – in order to run their fraud algorithms – is often the most comprehensive available, and can include behavioural, geo-location and online data.

Understanding customer behaviour is critical to open up new revenue streams. In order to do this, contextual data is crucial, but banks also need the right analytics tools to turn raw data into useful insights. AI will play a key role here, as it will enable banks to customise their product offerings in highly individual ways at high speeds and lower costs compared to traditional strategies.

## Step 7: Refine decisioning threshold, investigation processes, and model performance with additional data points

As banks need to consistently monitor their performance, there will come a time when it will be necessary to refine their processes or add additional data to the model. Depending on the underlying technology, this has the potential to be challenging. While cloud-based solutions are easily scalable and adaptable, legacy systems are hard to mould for today's complex threat environment. Banks that have invested in modernisation will find it easier to refine their fraud mitigation strategies and tooling compared to banks that have opted for stop-gap measures without addressing the underlying systems.

Another, overarching, challenge banks will encounter during this digital transformation is ensuring an appropriate balance is struck between innovation and data security. The key is ensuring enough security measures are inserted into the process, without the experience becoming cumbersome for their merchant customers. That's why it's crucial to the success to consistently monitor and review the internal risk appetite framework. Factors such as organisational changes or new regulatory requirements can potentially affect a bank's risk appetite, so the frequent monitoring of risk strategies will allow them to align their frameworks accordingly and find the sweet spot between innovation and security.

## Step 8: Expand fraud solution to additional transaction volumes, use cases, and payment flows

Once banks have set up the most efficient fraud detection solution for their individual requirements, they can look at the bigger picture. How can they scale their fraud solution to other use cases? The more contextual data is available to their solution, the better will be the systems' effectiveness at detecting fraud and enhancing customer experience. Real-time fraud detection, process improvements, further automation, AI enhancements and the provision of data on additional payment flows, such as account to account transactions or AML monitoring, are all factors that will enable banks to streamline not just their fraud mitigation, but their overall operational efficiency.

# 03 | Embracing modernisation to achieve efficient transaction fraud monitoring excellence

Card transaction fraud is growing in numbers and complexity. To minimise fraud losses, banks need to leverage the power of modern and emerging technologies. Legacy systems are no longer fit for purpose–banks need to invest in infrastructure modernisation in order to unify siloed data that informs their fraud prevention solution.

Automation, cloud, AI and ML are all crucial parts of effective fraud mitigation strategies and enable banks to increase their speed and accuracy and easily adapt to emerging threats. Yet no fraud mitigation strategy is complete without having risk appetite and case management frameworks in place.

Achieving transaction fraud monitoring excellence is a multi-faceted process that needs to be continually monitored and adjusted. If successful in these efforts, banks can turn the recent spike in financial fraud into an opportunity to significantly improve innovation, reduce fraudulent activity and enhance customer experience.

# About

## Finextra Research

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to www.finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers.

The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information:

Visit **www.finextra.com** and become a member,
follow **@finextra** or reach us via **contact@finextra.com**.

## Brighterion

Brighterion, a Mastercard company, was founded in 2000 and acquired by Mastercard in 2017. Brighterion provides enterprise AI applications for payment service providers, financial institutions, and healthcare payers. More than 2,000 companies worldwide and 74/100 of the largest U.S. banks use technology powered by Brighterion AI to protect against fraud and risk. Brighterion's solutions offer value-added Mastercard network intelligence to further enhance performance beyond a client's own data. Using a full-stack, state-of-the-art machine learning toolkit, Brighterion AI creates off-the-shelf market models that are production-ready and custom models in 6-8 weeks. With unrivaled deployment and scalability, customers can easily implement AI that delivers near real-time response times and resiliency. Brighterion has received multiple awards including Fintech Nexus' 2023 Top Service Provider Award, Business Intelligence Group's 2023 Artificial Intelligence Excellence Award (second consecutive year), US FinTech Award's 2022 Banking Tech of the Year, the 2021 Business Transformation 150 and the 2020 Fortress Cyber Security Award for Threat Detection.

# For more information

**Finextra Research**
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
**+44 (0)20 3100 3670**

Email
**contact@finextra.com**

Follow
**@finextra**

Web
**www.finextra.com**