A Finextra Research whitepaper
in association with Mastercard
July 2024

APIs, AUTOMATION, AND AI: AN ARSENAL TO DEFEND AGAINST CARD TRANSACTION FRAUD

01 Introduction

Fraudsters are no longer individuals who are looking to infiltrate gaps or weaknesses in how our businesses are set up. They are expert technologists and strategists that steal customer data, take over accounts and break into tough security measures. Every ecommerce website, every transaction, every new account, and every click is an entry point for the well-armed fraudster. With online transactions ever growing, fraudsters have more opportunities than ever before to commit crimes.

There is no doubt that ecommerce fraud across the globe is increasing, with losses to merchants reaching $41 million in 2022 and exceeding $48 billion in 2023, according to Juniper research. This global issue permeates in Europe, with Germany and France being the hardest hit across the continent. North America has the highest fraudulent transaction value globally and accounts for 42% of ecommerce fraud, while Latin America sees 20% revenue lost to fraud.

Between 2023 and 2027, merchants are expected to lose a total of $343 billion to online payment fraud, driving home the point that the time is now for technology to be leveraged to reduce card transaction fraud, which is growing in numbers and complexity. Layers of modern and emerging technologies are needed because legacy systems are no longer fit for purpose and cannot host data in a way where it can be efficiently harnessed – based on its quantity or quality.

Banks must set themselves a goal to invest in infrastructure modernisation with the aim of unifying siloed data that informs their fraud prevention solutions. APIs, automation, and AI are all integral to an effective fraud mitigation strategy in 2024, because these technologies – if used in the right way – can support financial institutions evolve to emerging threats with increased speed and accuracy.

02 APIs

Fast-paced ecommerce has transformed how merchants and acquiring banks operate, welcoming a new era of efficiency but shedding light on the need to safeguard the financial ecosystem from fraudsters that are working at the same pace. A key tool in achieving this is APIs, which can support acquiring banks establish a foundation for comprehensive financial analysis and strengthening risk management initiatives.

This became evident following the implementation of the Payments Services Directive (PSD2) in 2018, which aimed to break apart banks' monopoly over consumer data and allow bank customers – individuals and merchants – to use APIs from third party providers to manage their finances. However, this created a new attack surface.

The risk of digital transaction fraud cannot be avoided, and under PSD2, payments services providers are expected to collect and report data on payments transactions, whether they are fraudulent or not. With consistent fraud data reporting in place, a holistic and transparent view of fraud activity is now available which can be used to further improve security and protection of data.

2023 European Central Bank research revealed that since 2021, card fraud has fallen to its lowest level since data collection began. It made up 0.028% of the total value of card payments made using cards issued in the SEPA, amounting to €1.53 billion from a total value of €5.40 trillion. By comparison, card fraud in 2019 amounted to €1.87 billion from a total value of €5.16 trillion and the highest share of card fraud observed to date was 0.048% in 2008.

In 2023, the European Commission (EC) also published a draft for the third iteration of the Payment Services Directive (PSD3) together with a draft for a new Payment Services Regulation (PSR) which attempts to establish trust by improving the security and reliability of payments. The new directive and regulation demands providers to combat payment fraud and limits reliance on technical data interfaces.

> **“… card fraud in 2019 amounted to €1.87 billion from a total value of €5.16 trillion and the highest share of card fraud observed to date was 0.048% in 2008.”**

While other technologies aim to disrupt traditional financial frameworks, APIs are at the crux of modern software development, enabling, communicating and allowing organisations to share data seamlessly and in real-time, across platforms. Banks no longer need to sift through static reports and periodic audits from their merchants to manage their risk appetite; integrating APIs permits organisations to respond to market changes immediately.

APIs are the connectors within anti-fraud models, and while they are nothing new, their viability and ubiquity in linking organisations’ systems and workflows in recent years has led to a step-change in financial services and a gateway to a whole new technological way of working. Their use by banks has also grown in recent years because of their ability to connect internal systems with direct data exchange as well as external systems, linking third parties and facilitating all manner of partnerships, data insights and as a result, new products and services for both businesses and consumer.

APIs also link datasets and fraud scores, allowing the speedy and secure weaving of a rich tapestry of defence. They can also be used to tailor anti-fraud methodologies to merchants in geographies where there is a requirement for on-premise or in-house storage of certain data. Rules management intelligence can in turn be fed into models via APIs, looping in a business or regulatory expert to create an even greater framework of knowledge and insight on which to produce more accurate screening decisions.

As a result, and in combination with shrewder case management, businesses are more empowered, may become more ambitious or aggressive in their growth strategies on account of increased confidence to alter their risk appetite regarding their definition of a false positive. It is their prerogative to tighten or weaken those parameters based on how much loss is worth it or even expected.

03 Automation

Merchants with large sales volume will rely on automated systems to process most transactions, with only a very small percentage being selected for manual review. AI can improve the performance of automated systems, but those who operate them must consider the evolving market conditions and have the capacity to leverage all the tools and expertise available to them.

Technology being utilised within financial services has gone beyond early data analysis tools and binary automation. Digital transformation is now a pre-requisite to modern operations and has become a continuum, with adaptation being the only way to survive in today's payments marketplace. It is also important to reiterate that financial transaction data is structured data, and as a result, mature automation has come to the fore in anti-fraud system development and transaction monitoring.

The volumes of data that are produced - not only in-house but around the world - can play a huge part in providing context for increasingly accurate decisions and judgments about financial transactions. The processing and storage of these internally and the accessing of external data stores, however, is currently beyond manual and traditional capability.

With automation, historical transactions and customer data can be applied to match current or active transactions to known fraudulent patterns, and can be trained to extract the key information, depositing it in the correct format elsewhere. For merchants who have historical data to hand, this could be considered a breakthrough to shape new models, combat fraudulent activity and glean business insights. Integrating acquirer anti-fraud systems with a reliable foundation of data is not only a nice-to-have, but a fundamental game-changer.

Machine learning algorithms can get better and better at detecting fraud, can be used to automatically decline orders that are highly likely to be fraudulent, or to flag suspicious transactions for further investigation in manual review, helping merchants stay one step ahead of fraudsters.

> **“AI can improve the performance of automated systems, but those who operate them must consider the evolving market conditions and have the capacity to leverage all the tools and expertise available to them.”**

Most merchants will curate and build their business with the help of additional acquiring bank services. Acquirers have evolved to be able to onboard merchants in a radically improved fashion and in a way where models and tools can much more efficiently be deployed, drawing upon new, raw data being generated by the business, as well as pulling in data and insights from all manner of other repositories.

In this way, what begins as a fraud monitoring endeavour can become a holistic and intuitive business strategy, as additional datasets from eclectic sources begin to inform more sophisticated case management processes. Applying automation to new and old data builds a more advanced and accurate picture of transaction activity for analysts to interpret. In turn, the human in the loop becomes more specialised, while simultaneously feeding back into the system new and more accurate outcomes all the time. It becomes a story of continual advancement over which the merchant has increased control.

Data volumes, in the terabytes, processed at real time speeds, with accompanying analysis and decisioning, requires the kind of compute power and elasticity that only a cloud environment can provide. Equally, the resilience and security inherent in cloud infrastructure make key operational considerations such as regulatory compliance and cost much less of a burdensome factor.

Huge amounts of data are required to train any model, and to not only refine, but continually learn from and improve upon the risk indicators that will flag suspicious activity. An approach that trains a model based upon layers of data analysis - including fraud data analysis - is one method by which to produce a more sophisticated and accurate measure.

04
AI

From fraud prevention to merchant monitoring, AI has proven to be the most effective tool for high transaction volume businesses. The new wave of fraud detection models, crafted with AI can deliver radically reduced false positives and increased approvals, but the additional benefits to such systems and the empowerment that handling data brings can mean greater overall business insight and commercial prowess.

To set the scene, it is important to call out that acquiring banks are in dire need of reducing their operating costs, and AI has historically presented itself as a tool to support revenue growth. The technology is already used to monitor merchants, in addition to data mining, rules-based algorithms, case-based reasoning, fuzzy logic and neural networks. Further to this, AI can stop fraud before it happens.

Banks cannot delay investment into AI and must make AI adoption a priority. Moreover, with AI expected to become ubiquitous across the industry, financial institutions that do not leverage AI technology risk being left behind and disintermediated. Without AI, competitors are likely to win the race, particularly because they are the most secure, can detect fraud earlier, and revenue losses are fewer and far between.

For merchants and acquiring banks alike, partnering with a third party AI provider is their best option. By outsourcing the technology, organisations do not have to invest in building the systems from scratch and can rely on the provider to upgrade systems in accordance with upcoming regulations or standards.

When choosing a third party AI provider, overall fraud detection is the most important metric to consider. In addition to this, false positive reduction rate, and whether they can offer additional analytics to detect new types of fraud must also be looked into. Further, AI providers can also offer risk assessments when onboarding new merchants among other value-added services such as visualisations of suspicious activity.

05 Conclusion

We are now fully immersed in the AI era. AI-driven risk assessments have become a crucial step for financial institutions onboarding new merchants and this technology is seen as the most effective tool for high transaction volume businesses.

With these high transaction volumes comes layers upon layers of data, and models trained on granular and up-to-date data can remedy issues around sophistication of analysis, and accuracy.

The parameters to which transactions are analysed must always be shifting based on the case, because the environment in which both merchants and banks are operating is continually adapting.

The e-commerce boom has revolutionised the operations of merchants and acquiring banks, ushering in a new era of data and scale. While this has enabled rapid innovation of fraud detection systems, fraudsters are advancing in sophistication as well, making AI fraud detection solutions that can scale with the industry more important than ever.

06 About

Finextra

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.

Mastercard (NYSE: MA)

Mastercard is a global technology company in the payments industry. Our mission is to connect and power an inclusive, digital economy that benefits everyone, everywhere by making transactions safe, simple, smart and accessible. Using secure data and networks, partnerships and passion, our innovations and solutions help individuals, financial institutions, governments and businesses realize their greatest potential. With connections across more than 210 countries and territories, we are building a sustainable world that unlocks priceless possibilities for all.

Finextra

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

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com