by Joel Van Arsdale and Charlotte Al Usta, 17 January 2025

AI's Impact on Payments & Fintech, Part 2: Fraud Management

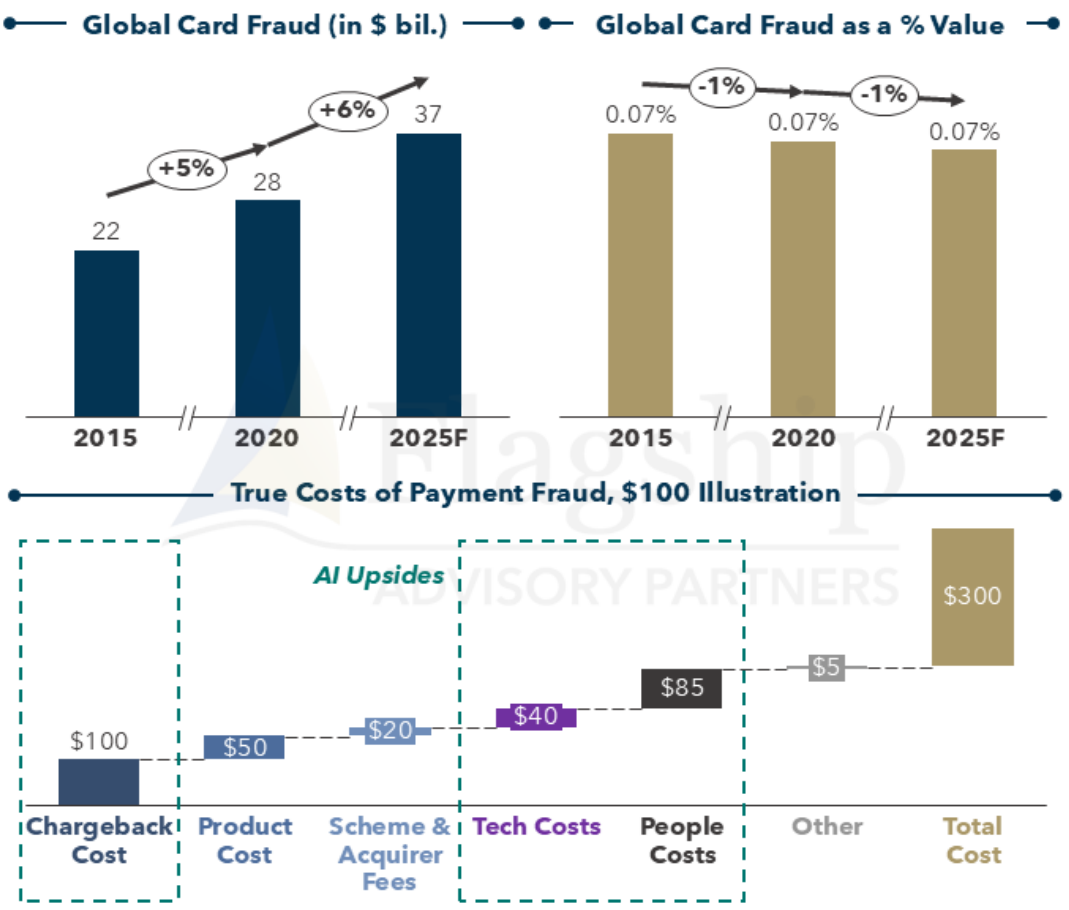
This is Part 2 of Flagship's multi-part series assessing the potential impacts of AI on payments and fintech. Read Part 1 here where we introduce AI, outline the historical context for AI's impact on our industry, and introduce the impacts of AI.

As we assess the broad potential impacts of Artificial Intelligence (AI) in fintech, fraud management is the obvious place to start. AI is a well-established force of innovation in fraud prevention, the most mature application of AI in fintech. Real-time, machine decisioning on payment transactions and account opening and access have been around for decades. More recently, in the last decade (more or less), Machine Learning has been vital to growing beyond reactive, legacy methods for developing and implementing payment decisioning models. Unfortunately, fraudsters also innovate, and AI has helped them to launch attacks (e.g., phishing) at greater scale and levels of efficiency. In this second part of our AI Impact on Payments and Fintech, we cover the evolution of fraud prevention and AI's role in addressing this pressing market need.

Fraud Remains a Massive Problem, Constantly Evolving

Fraudsters are highly innovative. When you close one loophole, they find another. Compounding this natural to and from, the market demands payment services that are faster, more convenient, and more virtual, all of which broaden fraud vulnerability. For decades now, it has been a constant battle for fraud management professionals in banking and payments to stay one step ahead of fraudsters. AI is a vital weapon in this battle, allowing risk professionals to concentrate their focus on strategy development rather than data manipulation and model building.

Figure 1: Global Card Fraud & Costs of Payment Fraud

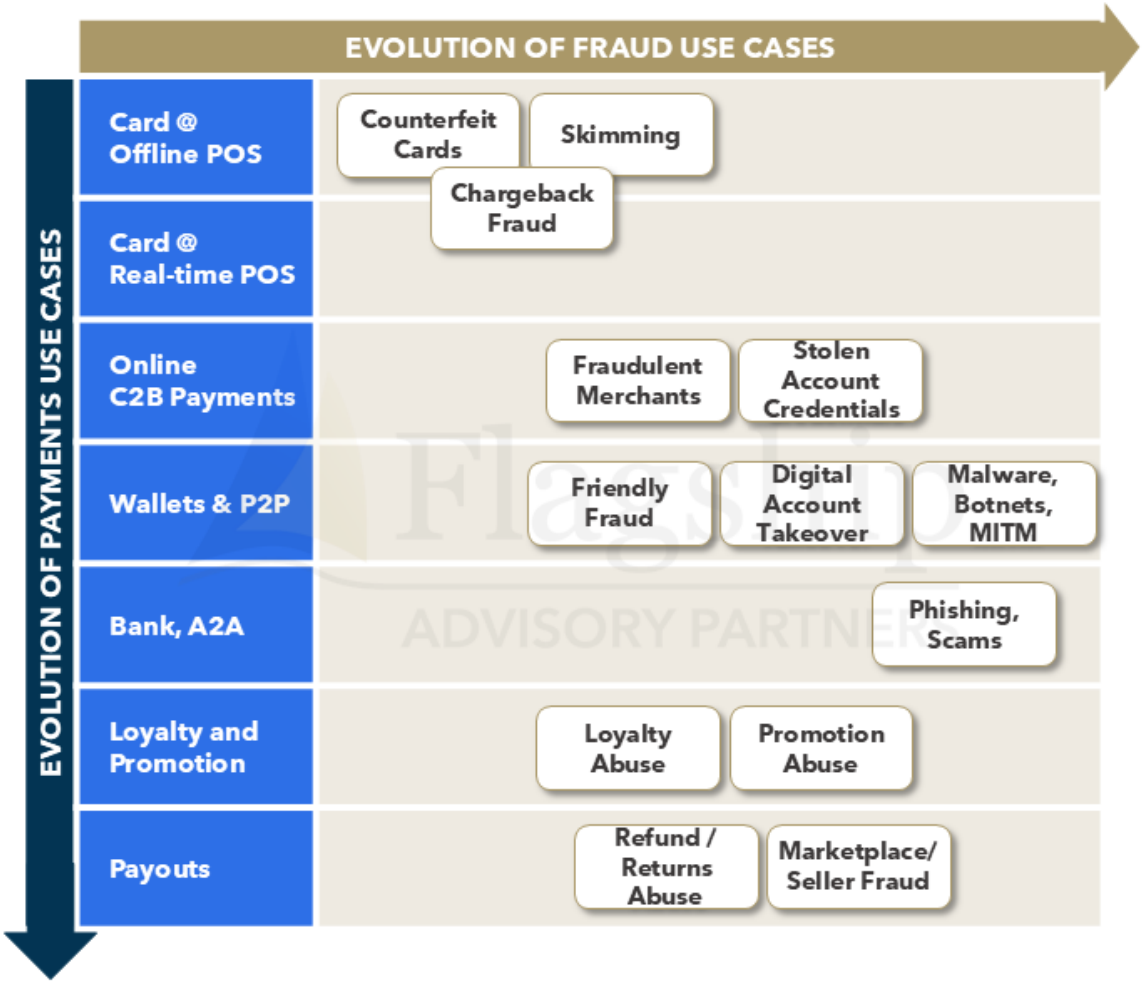


Sources: Nilson Report, Flagship Advisory Partners, LexisNexis "True Cost of Fraud Study 2023"

Fraud remains a massive challenge to the banking and payments industry. Global losses from banking and payments fraud are measured in hundreds of $ billions. As Figure 1 shows, nominal fraud losses on payment cards (a primary category within broader banking fraud) continue to grow. However, fraud rates have shown improvement, noting this varies by country and transaction channel. Virtually all providers of payment fraud prevention solutions and services leverage machine learning. But before we get into how AI is helping to improve fraud management performance, let us first review how payment and banking fraud has evolved.

Figure 2 illustrates the parallel development of payment use cases and fraud use cases. Years ago, payment fraud was concentrated on counterfeiting physical cards. The mag stripe was easy to emulate, and transaction monitoring controls behind the POS were limited. The market achieved great success in mitigating counterfeit card fraud, leveraging physical encryption and PIN codes along with machine-driven payment monitoring and decisioning engines across multiple points in the transaction journey. However, as this form of fraud ramped down, digital payments to merchants and each other ramped up. Fraudsters were no longer dissuaded by physical controls as stolen payment credentials could be used online. The market again responded with identity verification solutions and better decisioning and monitoring engines. Pure payment fraud (e.g., stolen card numbers) has declined for years because of these solutions.

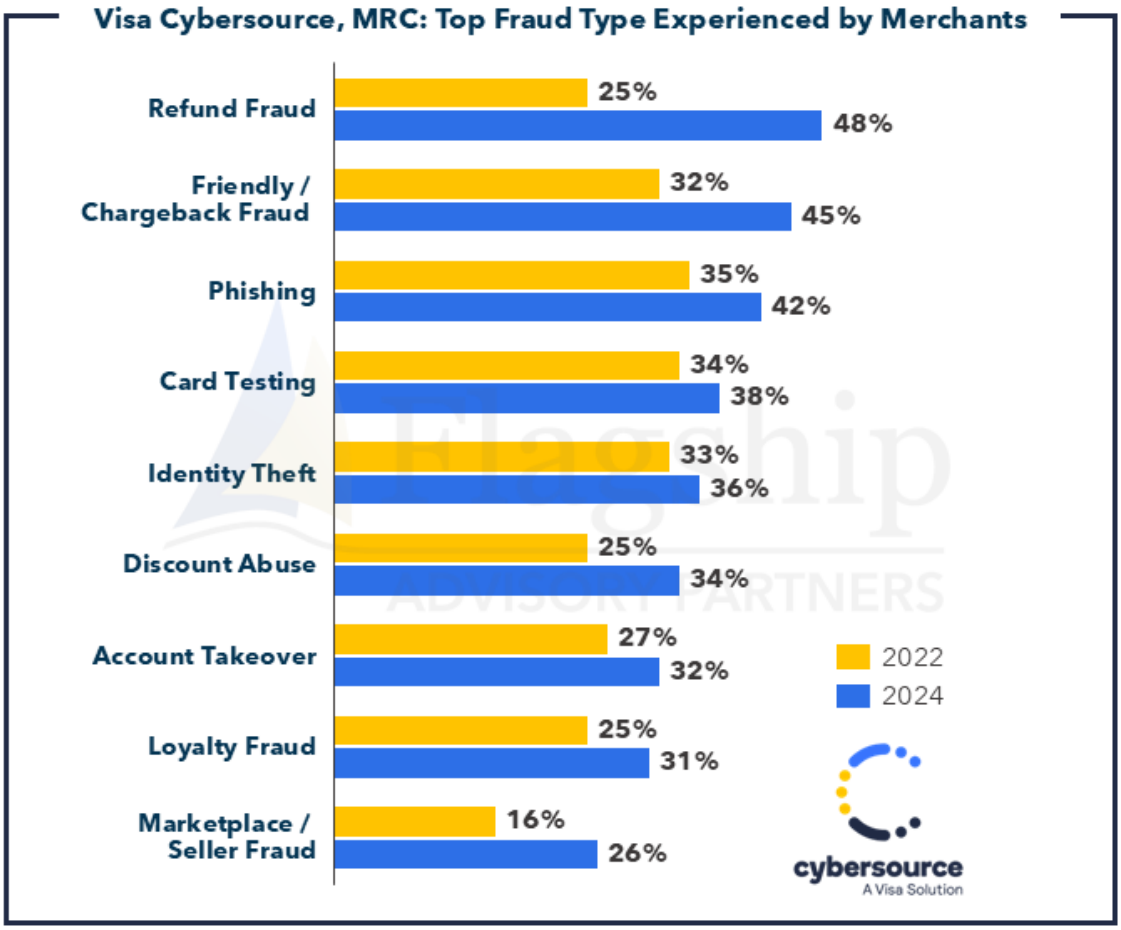
Figure 2: Parallel Evolution of Payment & Fraud Use Cases



Source: Flagship Advisory Partners

Unfortunately, fraud finds a way, and today, it increasingly comes in the form of identity theft and account takeover. In these cases, the payment credentials are not abused in isolation but as part of a broader identity hijacking. In the case of account takeover, a simple risk algorithm built on payment transaction fields is not a highly capable solution for fraud prevention. Beyond identity theft, other forms of identity abuse, such as promotion or loyalty abuse, are also flourishing. Figure 3 illustrates the changing mix of fraud by type.

Figure 3: Visa Cybersource - Types of Fraud Experienced
(data sourced directly from Visa Cybersource, MRC survey 2022 and 2024)



Sources: Flagship Advisory Partners, MRC Visa Cybersource et al. "2024 Global eCommerce Payments & Fraud Report"; Visa Cybersource "2022 Global Fraud and Payments Report"

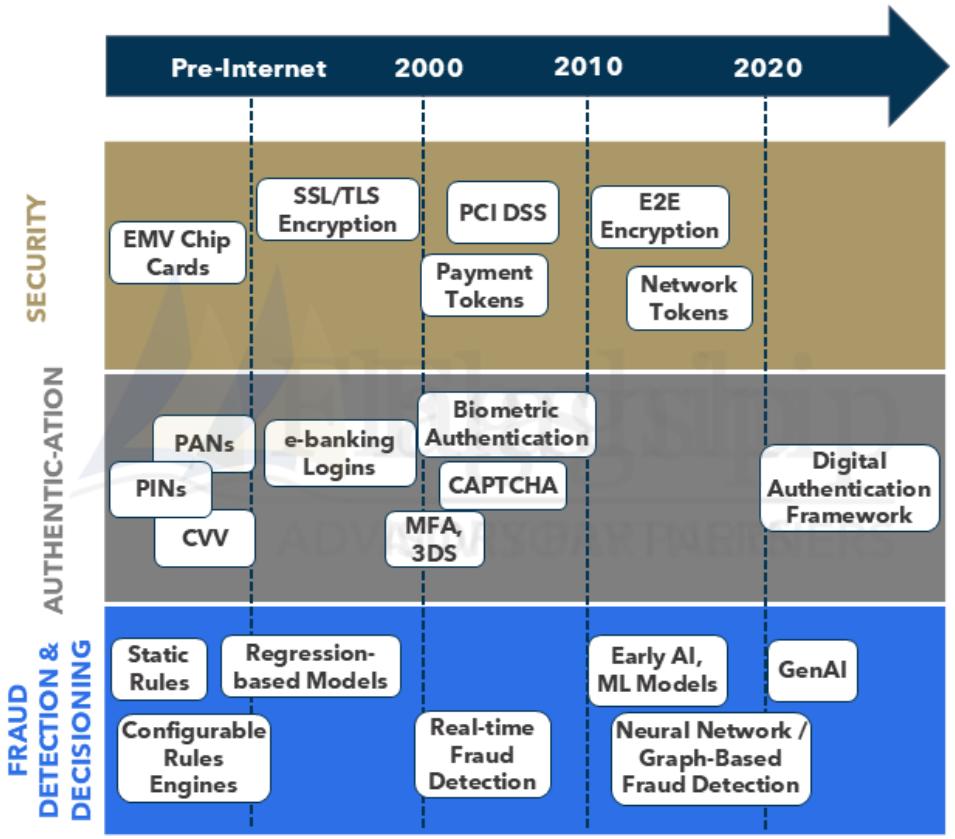
AI Is Ideally Suited for Managing Fraud

AI is a superior foundational technology for combating identity theft and account takeover. Detecting potential identity theft requires a much bigger and broader scope of data. Machine learning models built to prevent account takeover don't just rely on the dozens of fields in a payment transaction file. Rather, these ML models effectively consume the entire estate of available data from the start of a fraudster journey, thousands and thousands of indicators (web page navigation, etc.). AI gives us virtually boundless scope for data consumption and usage. AI is also good at pattern recognition, much better than any person could be at monitoring and reacting in people's time while carrying people's biases.

Success in fraud management is about balance; the more restrictive the avoidance controls, the higher the collateral damage (i.e., false positives). It is this balance that AI is also particularly well suited to optimize. Legacy fraud controls, such as rule sets, are naturally rigid and often improperly tuned. For these controls to improve, a human must constantly monitor and adjust. And in making these adjustments, humans tend to be

biased, often turning the dials too tight or too loose in pursuit of specific fraud patterns. AI, on the other hand, trains itself continuously while solving for a broader set of objectives, such as the delicate balance between too much and too little fraud risk. Note that today, AI models still often require consistent human intervention for optimization, but human dependencies should dissipate in time.

Figure 4: Payment Security & Fraud Prevention Innovation Timeline
(non-exhaustive; select innovations)



Source: Flagship Advisory Partners Market Research and Observations, Desk Research

AI is computing power and data needy, but it is less constrained by people resources. Staffing the risk function and executing the manual review queue in a timely manner are two of the leading challenges for payment-accepting merchants and banks. LexisNexis[1] cited requirements for more people resources as the most common driver of increased fraud costs in 2023. AI solutions allow for smaller risk teams and the concentration of those experts on higher-value activities.

Risk controls, including ML-based solutions, remain complex and challenging for SMBs to use. Designing risk tools that are simple to use, effective, and ideally chargeable products for SMBs has been a challenge since the dawn of e-commerce. SMBs are simply not big enough to employ risk experts. The market is now leveraging AI to make these controls more usable by non-experts. Stripe Radar Assistance, for example, constructs and adapts risk rules based on simple natural language instructions.

[1] https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study

AI A Double-Edged Sword, A Tool For Fraudsters As Well

Regrettably, fraudsters also leverage AI as a valuable weapon to exploit digital vulnerabilities. Technology-driven mass attacks such as phishing, malware, and deepfakes are growing. Fraudsters are learning to use AI to train and improve these attacks. According to a 2023 Deloitte study[2]AI-generated content contributed to $12 billion in fraud losses in 2023, and this is expected to grow beyond $40 billion by 2027. Fraudsters use AI to better target their phishing attacks and to create more compelling content and virtual identities (deepfakes) capable of tricking vulnerable people.

Adapting to phishing and deepfakes is now a central challenge for providers of financial accounts. Less sophisticated financial institutions relying on legacy fraud controls are exposed to the potential liabilities of growing scam sophistication. According to PYMNTS[3], scam-related fraud jumped 56%, and financial losses from these scams grew 121% in 2024. According to the Harvard Business Review[4]AI-orchestrated phishing attacks are already equally capable as hum-orchestrated attacks, but they are executed at only 5% of the cost/effort.

Conclusions

AI, particularly machine learning detection models, is already vital to ongoing improvement in combating payment and banking fraud. Fraudsters learn and adapt, and legacy fraud tools are not well suited for today's evolving use cases (increasingly powered by malicious AI). AI has advantages over humans; it is not limited by resources, hours in the day, or the scope of human observation lenses. To be clear, machine learning models still need plenty of human intervention today, but as the technology evolves, AI will grow out of much of this dependency. This will allow fintech providers and users to refocus valuable, expert resources on higher-value activities.

In the next part of our AI series, published in the coming weeks, we will cover AI's Impact on Efficiency in Fintech. Till then, you can read our Part 1 introduction and plans for this insights series **here**.

Please do not hesitate to contact Joel Van Arsdale at Joel@FlagshipAP.com or Charlotte Al Usta at Charlotte@FlagshipAP.com with comments or questions.

---

[2] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-advisory-deloitte-digital-fraud.pdf

[3] https://www.pymnts.com/news/security-and-risk/2024/scam-related-fraud-jumped-56percent-surpassing-digital-payment-crimes/#:~:text=The%20share%20of%20scam%2Drelated,scams%20responsible%20for%20most%20losses.

[4] https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams