Payment Industry Insights: How AI Has Transformed Fraud Detection and Failed Payments

FlexPay

Table of Contents

Introduction . . . 3

AI and the Evolving Payments Landscape . . . 3

Key Benefits of AI in Payments . . . 4

Threats: The Rise of AI-Powered Fraud . . . 5

How Banks Use AI to Fight Fraud . . . 6

Opportunities: AI-Driven Fraud Prevention for Merchants . . . 7

Regulatory and Compliance Considerations . . . 9

Optimizing Failed Payments with AI . . . 9

Conclusion . . . 11

Introduction

Artificial intelligence (AI) is transforming the payments industry, reshaping fraud detection, customer authentication, and failed payment recovery. While AI presents new opportunities for merchants, it has also created significant challenges, including evolving fraud threats and regulatory complexities. This eBook explores the impact of AI on card payments, and how merchants can leverage AI-driven solutions to fight fraud, recover failed payments, and improve the customer experience.

Using AI and Machine Learning can improve transaction handling and reduces false declines, leading to more successful transactions.

AI and the Evolving Payments Landscape

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines, enabling them to perform tasks such as problem-solving, decision-making, and language understanding. AI systems can analyze data, recognize patterns, and make predictions, often improving over time through experience.

A key component of AI is **Machine Learning (ML)**, a subset that allows computers to learn from data without explicit programming. ML algorithms identify patterns in vast datasets and adjust their responses accordingly, enabling applications like recommendation systems, fraud detection, and predictive analytics. In the payments industry, machine learning can improve transaction handling and reduce false declines, leading to more successful transactions.

AI-driven technologies are revolutionizing the way transactions are processed and secured. Banks, issuers, and merchants are using machine learning algorithms to detect suspicious transactions, reduce fraud rates, and streamline payment approval processes. However, the use of AI is a double-edged sword—while it enhances security, it also introduces new fraud tactics that are increasingly difficult to detect.

Key Benefits of AI in Payments

AI enhances payments in several ways, including:

Optimized Payment Processing: AI dynamically adjusts transaction requests, reducing payment failures and boosting authorization rates.

Advanced Fraud Detection: Machine learning models analyze transaction data to detect and prevent fraud, minimizing risk exposure.

Fewer False Declines: AI-powered fraud detection reduces the chance of a legitimate payment being mistakenly blocked.

Failed Payment Recovery: AI can determine the best strategy to recover a failed payment by analysing reason codes, identifying optimal retry times, and adapting to issuer-specific patterns.

Seamless Authentication: AI improves security while reducing customer friction during transactions.

Predictive Analytics: Businesses can analyze spending patterns to offer personalized recommendations and promotions.

AI-driven technologies are revolutionizing the way transactions are processed and secured.

Threats: The Rise of AI-Powered Fraud

According to Nasdaq, global fraud losses totalled more than $485 billion in 2023, in part from the rise in sophisticated AI tools. While this amount is not all AI-related, AI has made it easier for fraudsters to manipulate payment systems, and AI-driven scams make it harder to trace perpetrators, requiring stronger security measures.

AI-driven fraud tactics include:

- **Refund Fraud:** Fraudsters use AI tools to request refunds before items arrive, exploiting automated customer service systems.
- **Account Takeover Fraud:** AI is used to generate synthetic/deepfake identities, allowing criminals to access and misuse legitimate accounts.

While fraud detection tools are effective, the vast datasets they use to fight fraud actually make them a potential target for cybercriminals looking to steal sensitive information. This is particularly worrisome since a breach in an AI system handling credit card payments could lead to massive data leaks.

Attackers can also exploit vulnerabilities in AI models and manipulate input data to deceive the AI system into making incorrect decisions, potentially leading to unauthorized transactions.

These scenarios highlight the ongoing need for heightened data privacy and security.

While fraud detection tools are effective, the vast datasets they use to fight fraud actually make them a potential target for cybercriminals looking to steal sensitive information.

Unsettled transactions contribute to a merchant's fraud ratio, encouraging the adoption of fraud prevention systems.

How Banks Use AI to Fight Fraud

Banks employ AI fraud screening tools to identify compromised cards and detect unauthorized transactions, and issuer processors actively monitor the dark web for leaked card information to help them prevent fraudulent purchases. While banks use AI to detect fraud, they are unable to use it in real-time authorization decisions due to Mastercard and Visa service level agreements (SLA). Because of these limitations, they will approve a transaction and then pass it through their AI fraud tool where it could get flagged as fraud. If it is identified as fraudulent, the bank then generates a chargeback on the merchant. Even though the chargeback didn't come from the customer, it is still painful for the merchant.

In the effort to measure fraud, regulations are expected to be in place later this year that will require banks to report fraud incidents on transactions that do not settle, such as those declined due to non-sufficient funds (NSF) or security risks. These unsettled transactions will count towards a merchant's fraud ratio. This creates an incentive for merchants to implement fraud prevention systems so they can avoid submitting compromised transactions that may negatively impact their fraud ratio.

Risk scoring tools analyze transaction patterns and flag unusual activity before it leads to fraud.

Opportunities: AI-Driven Fraud Prevention for Merchants

Enhanced Fraud Detection and Prevention

Risk scoring tools are in the best position to use AI to look for patterns and identify potential fraud. And as more data becomes available, these tools will become even more effective. These tools are essential for merchants that accept card-not-present transactions. By analyzing transaction patterns in real time and flagging unusual activity before it leads to fraud, these tools reduce unauthorized transactions and create better customer experiences.

Not every business wants to use a third-party solution, however. Major platforms like Checkout.com and Shopify have developed their own in-house fraud solutions tailored for their merchants. These solutions analyze transaction history to detect potential fraud patterns and use consumer insights—such as IP addresses and device information—to validate transactions.

While risk scoring tools are well known for reducing customer-initiated chargebacks, they are also capable of preventing unwanted issuer-generated chargebacks. A service level agreement (SLA) limits the technical capabilities of issuers and issuer processors returning authorization decisions, but risk scoring tools have much more latitude and can spend a few more seconds to provide an authorization answer. This is important because issuers have been known to change their minds after giving approval and the only way to decline the transaction is to issue a chargeback on behalf of the card, even though the cardholder didn't ask for this. Using a risk scoring tool provides a small buffer of time that could prevent this type of chargeback.

Improved Customer Authentication

AI-driven Multi-Factor Authentication (MFA) enhances security by incorporating biometric authentication methods, such as facial recognition, fingerprint scanning, and voice recognition, providing an additional layer of security and reducing the risk of unauthorized access. But despite its benefits, some merchants hesitate to implement MFA due to concerns about customer abandonment rates. They would rather have the order and risk the chance of fraud.

AI also enables merchants to implement adaptive authentication strategies (also known as risk-based authentication), where low-risk transactions require minimal security checks while high-risk transactions trigger additional verification measures. This may be a work around for those merchants leery about implementing MFA.

Biometric authentication methods provide an additional layer of security and reduce the risk of unauthorized access.

Advanced Data Analytics and Predictive Insights

AI can forecast potential fraud trends by analyzing historical transaction data, and it can find patterns in your payments data and pinpoint anything that could be dragging your acceptance rates. These predictive analytics help increase card acceptance rates and lower your risk of fraud.

AI can also segment your customers based on their transaction behaviors and risk profiles. This customer segmentation helps you tailor fraud prevention strategies to different groups, ensuring a more targeted and effective approach.

Regulatory and Compliance Considerations

The integration of AI into the payments system introduces complex regulatory challenges for merchants and financial institutions, such as the need to adhere to data protection laws, including General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Transparency in all AI decision-making processes must be maintained.

The use of AI in payment systems also raises ethical issues, such as the potential for bias in AI algorithms. Ensuring that AI systems make fair and unbiased decisions is crucial to maintaining trust in the payment system.

Optimizing Failed Payments with AI

Businesses must optimize payments to reduce churn and the financial strain that goes along with it. A case in point: research from Checkout.com shows that 45% of consumers won't retry a payment after a single false decline while our own research shows that more than a quarter of subscribers have experienced a failed payment in the past 12 months. Using AI tools reduces the risk of churn and improves customer retention.

Research from Checkout.com shows that 45% of consumers won't retry a payment after a single false decline.

AI tools that include Machine Learning (ML) are best suited for failed payment optimization because ML models continuously learn from the data it uses and performance improves over time. This machine learning technology can increase approval rates by improving transaction requests and strategically managing retries. By adjusting payment data—such as modifying formatting, including or omitting specific details, and aligning with issuer preferences—AI increases the likelihood of approval. AI also adapts to changing network conditions, including issuer requirements, regulatory updates, and industry rules, which helps businesses eliminate formatting inconsistencies or data entry mistakes that could cause payment declines.

When a transaction does fail, AI enhances retry strategies by determining the most effect way to recover the payment. Advanced solutions like FlexPay's Invisible Recovery™ work directly with payment systems, using AI to recover failed payments before the customer is even aware of the issue. AI is needed to solve failed payments because of the complexity of the problem—there are hundreds of decline codes and more than twenty-five thousand banks, each with its own authorization decision logic. FlexPay's AI is so effective because it learns and adapts to solve for each of these factors, making it uniquely suited to solve the problem.

AI-powered payment optimization increases approval rates by improving transaction requests and strategically managing retries.

Conclusion

The use of AI in payment processing is rapidly evolving, bringing both opportunities and risks. While some merchants may hold back on using AI tools, it's important to take advantage of all the available technology to stay competitive, prevent fraud, and improve failed payment recovery. By using intelligent AI-based solutions, businesses can protect revenue, enhance security, and create a seamless payment experience for customers.

Want to learn more?
Contact the FlexPay team to minimize involuntary churn and maximize your revenue.

For more information contact us.

✉ sales@flexpay.io ☎ 1-800-273-4689 FlexPay.io LinkedIn/FlexPay