HOW AI AND MACHINE LEARNING ARE HELPING TO REDUCE TRANSACTION FRAUD AND IMPROVE MERCHANT MONITORING

WHITEPAPER

PaymentsJournal

Brighterion
mastercard

Contents

Intro

Transaction fraud is a continual challenge for acquirers that, if not monitored properly, may cost them a significant amount of money. Many transactions that acquirers identify as fraudulent are actually good transactions. Rejecting too many transactions does not just hurt a merchant's bottom line, but also affects customers who aren't happy when an order is declined as well as credit card issuers that lose on the interest they would have made on those transactions.

For acquirers, there is also a downside. If false declines on transactions are too high, customers become frustrated and stop shopping with certain merchants, which then leads some merchants to switch acquirers, costing acquirers tens of millions of dollars.

Fraud detection has become more streamlined thanks in large part to technology such as artificial intelligence (AI). Knowing where to start and what to look for is key, and having a better understanding of merchant and transactional fraud monitoring is a good starting point, especially when optimizing fraud detection ends up being a win not only for merchants and acquirers, but customers, too. Recent data put together by Brighterion, a Mastercard company, look at how AI tools enable acquirers can assess the risk of a transaction, as well as catch fraudulent transactions in real time. Furthermore, acquirers can leverage merchant risk scores to supplement the efficacy of the enterprise risk management program.

Transaction Fraud Monitoring

"One of the most important facets of payments is that the transaction must be irrefutable. There is a responsibility to ensure that the buyer is who they say they are, and that the transaction is clearly assigned to the authorized account. What's more, managing false positives is a pressing issue in the card industry. It is essential analytic tools are controlled tightly to keep out fraudsters, but the controls must not be so tight that they cost the merchant a sale.

The opposite of a false positive is a false negative. Just as authorization systems must ensure they do not reject transactions that should go through, a balance must be made to ensure that transactions that go through are pure and ready to post.

As the economy continues to go into a tailspin, with surging inflation and climbing interest rates, merchants and card issuers need their fraud controls to be better than ever so that merchants do not lose sales and issuers do not lose transactions."

BRIAN RILEY
Director of Credit,
Mercator Advisory Group

When it comes to fraud monitoring and minimizing false declines, acquirers face a few hurdles. Acquirers want to maximize the approval rates of transactions, thereby improving the customer experience, but certain challenges remain such as first-party fraud that involves dishonest accountholders and account-based fraud committed by professional criminals. As the threat landscape continues to escalate, transaction fraud management models remain the most scalable methods for detecting and preventing various threats that result in losses for financial services providers.

A transaction fraud monitoring market decisioning model is intended to analyze transactions in fractions of a second so that consumers and merchants can complete transactions in near real time. At the point of sale, a customer makes a purchase that quickly goes on a millisecond journey. The transaction processing system first passes the transaction through to an AI model within an integrated application programming interface (API). Then, the risk assessment and scoring are performed so that a transaction authorization (or denial) can be rendered to complete the transaction authorization process.

For an individual merchant, it is difficult to assess how risky a new customer may be. After all, the merchant doesn't have access to the customer's credit card history or mailing history. For acquirers, there is also an information gap; acquirers generally lack information about historical fraud trends for specific portfolios of cards, and for specific merchants. A transaction fraud monitoring model, which is linked to the acquirer, helps alleviate these risk.

For example, Mastercard leverages an internal card network database with records of all confirmed fraud cases from the issuers, merchants, and acquirers it does business with. It uses that information, along with anonymized data about card users, and processes it with AI pattern recognition to predict the fraudulent likelihood of specific transactions.

The AI component of a transaction fraud management system looks at all the different attributes of the transaction, and then the model produces a fraud likelihood score. It gives an acquirer a probabilistic score from 0 to 100 of how likely that individual transaction is to be fraudulent. For example, a score of 0 to 50 is low risk, 50 to 90 is medium risk, and 90 to 100 is high risk.

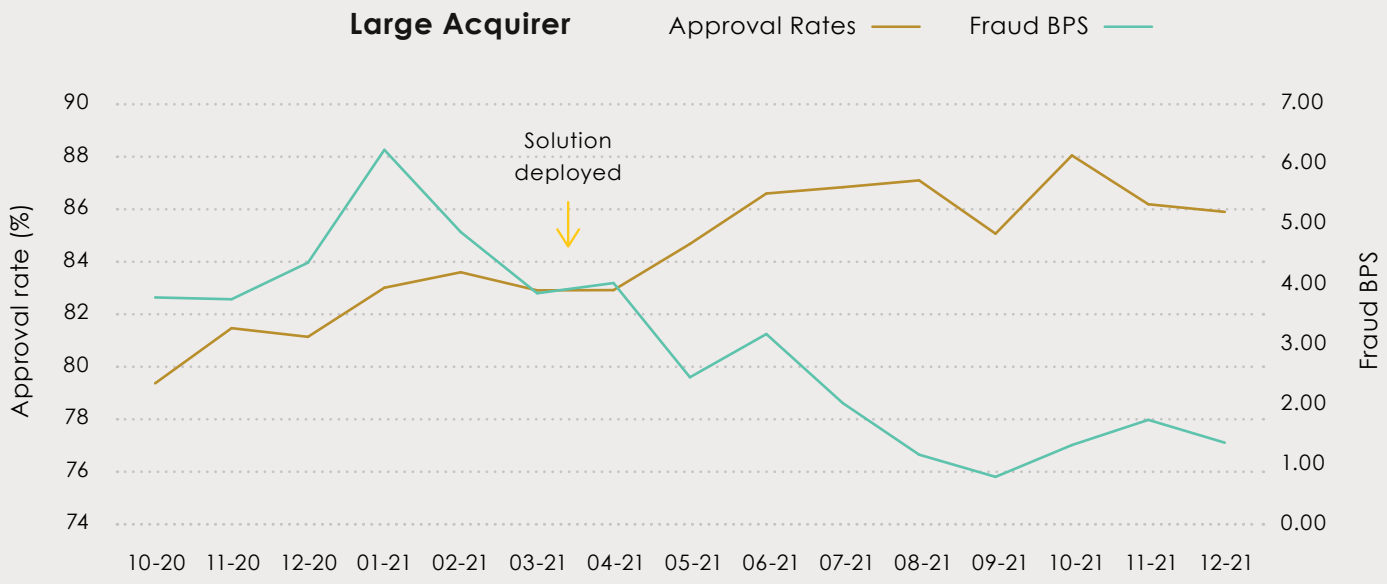
Models such as this provide acquirers with the tools they need to make more informed decisions. Acquirers are able to go through the data, assess the risk score in place, and move forward — whether that's accepting the transaction or rejecting it. To maximize fraud detection efforts, card issuers and acquirers should already be participating in Mastercard's EMV 3-D Secure, which provides an additional security layer for online credit and debit card transactions.

When this kind of authorization system is set up, acquirers automatically apply the approval recommendation in real time and stop fraudulent transactions before they happen. Most of the time, the acquirer makes the decision, passes that back to the merchant, and declines at the point of sale for the merchant. It's important to note that these recommendations are given based on the agreed-upon risk tolerance of the acquirer.

Leveraging historical Mastercard data from the North American region, Brighterion estimates the cost savings based on the fraud screening level an acquirer uses. Depending on the risk scores that the acquirer is willing to accept, there is a different fraud alert rate (telling merchants to decline the transaction) and different rates of fraud detection and savings.

Financial institutions can operationalize model scores so that different actions can be taken at different score levels to balance the trade-off between the cost of false positives to an acquirer's revenue and customer experience. Based on the model, it pays to reject the riskiest scores, but only to a point. When rejecting risk scores that lead to more than a certain transaction decline rate, the revenue losses of not processing valid transactions outweigh the value gained for acquirers. In addition, customer experience is harmed by too many false positives. At a certainpoint, the false positives start to overtake some of the value brought by the extra detection.

Mastercard has already rolled out its Brighterion technology to key acquirers throughout the world, to great effect. In one case, a large acquirer saw a large improvement in its approval rates and its fraud basis points (BPS) since implementing the system. The acquirer rolled out its transaction risk management system in April 2021. As a result, between Quarter 4 of 2020, and Quarter 4 of 2021, that acquirer saw an increase of six percentage points in approval rates (81% to 87%). Over the same time frame, the acquirer saw a 2.7-times drop in fraud BPS (3.98 to 1.46). This results in more value for the acquirer, as more quality transactions are approved and fewer fraudulent transactions occur.



Highlights:

- Brighterion was implemented in Q1/Q2 of 2021
- Between Q4 2020 and Q4 2021, one Acquirer saw an increase of 6 percentage points in approval rates (81% to 87%)
- Over the same timeframe, this Acquirer saw a 2.7x drop in fraud BPS (3.98 to 1.46)

Examples like this reflect how technology such as AI helps acquirers with their bottom line, both directly and indirectly. Acquirers make more money by processing more transactions and lose less money to fraud. The technology also indirectly improves the customer experience, likely leading to reductions in merchant attrition and top of wallet status for the cards that acquirers process.

"When a merchant and an acquirer send a higher percentage of genuine transactions to the issuer in the network, then that merchant and that acquirer are seen as more genuine processors, and the issuer and the network reject fewer of their transactions," said Paul Reed, product manager at Brighterion.

Merchant Fraud Monitoring

"The vast array of fraud detection tools available today in the financial services marketplace should be consumed with necessary care to ensure that each technical contribution can work together with a strong AI /Machine Learning decision engine.

As more consumers adopt payment methods that extend the flexibility of their debit and credit cards, their expectations for rapid and frictionless payment experiences continue to be top-of-mind for merchants and card issuers looking to increase non-interest income and client satisfaction—the backbone of every robust payment authorization process.

Digital growth and consumer adoption have demonstrated the need for most companies to leverage large amounts of data to make strong decisions. Post-pandemic recovery has also pressurized talent acquisition to the extent that every organization has to rely on automation as a means of maintaining adequate fraud prevention practices. These challenges, while daunting, have to be solved by deploying a fraud detection platform that incorporates card issuer, merchant acquirer, and dispute resolution data into a singular decision engine whenever possible."

JOHN BUZZARD
Lead Fraud & Security Analyst,
Javelin Strategy & Research

Acquirers have a limited number of resources to devote to manual investigations of potentially fraudulent merchants. Acquirers need help to balance revenue growth with fraudulent merchants by assessing the risk of ongoing and newly onboarded merchants. With this in mind, there are new-merchant fraud monitoring systems that can rank the risk level of each merchant similar to how it is done for transaction fraud. These models are helpful in deciding which fraud investigations to prioritize.

For example, Brighterion has produced a merchant monitoring model that uses AI to assess the riskiness of merchants, and provides a merchant fraud score to the acquirer for each merchant.

The merchant monitoring model is still transaction-based, but analyzes the transactions that come through by merchant instead of by customer. Merchant monitoring is not implemented in real time like transaction fraud is, but instead is used when investigating risky merchants after the fact.

Anytime a merchant transaction is scored above a certain value, say 70 out of 100, an associated case management software automatically creates an investigation case. Those cases are then ordered by highest risk, and the acquirer's analysts work their way down through the day, and whichever ones they don't get to, they close. The analysts start the process over again the next day, which allows them to focus their investigation on the highest-risk merchants. This in turn allows acquirers to manage their merchant fraud risk with smaller teams of investigators, leading to savings.

AI automates case reviews such as this, and streamlines what was once a very manual process. For example, Brighterion has a case management platform that has automatic case creation, queue management, auto routing to certain groups, and grouping by risk scores.

Merchant fraud monitoring can be done with or without API integration. When API integration is used, it works very similarly to the transaction fraud monitoring previously discussed. For example, Mastercard integrates via API the transactional data received, and they send back a score, which is then integrated into the case management platform.

Acquirer Worldpay adopted a comprehensive solution encompassing a merchant monitoring AI model combined with rules and case management focused on detecting fraudulent merchants. The company found that because of the efficiencies created by the software, it was able to reallocate staff to its team that can work cases, because it's now far more optimized in the way its manual reviews go. Worldpay further reported that having merchants listed by risk score made it easier to prioritize manual investigations, and, therefore, be more efficient.

Other examples highlight the cash savings involved in optimizing fraud investigation with merchant risk models. Through initial portfolios deployed with a top-five US acquirer, Mastercard identified roughly $6 million in incremental annual savings after it reduced exposure to fraudulent merchants.

Conclusion

Large data sets, AI, and large computing power are revolutionizing the entire economy, and fraud detection is no exception. Optimizing approval rates for transactions while minimizing fraud is what many companies are striving toward. Advanced risk management tools are also making it possible for companies to get closer to this goal.

For acquirers, transaction fraud management is a positive step in the right direction because it enables them to assess the risk posed by customers, with the help of credit card data privately held by credit card companies and the expertise to parse it. In particular, transaction fraud management allows merchants to accept more transactions than ever, thereby producing more sales and keeping more customers. This in turn is good for the acquirer, which benefits from processing the increased number of transactions

On the fraud investigation end, merchant fraud risk management tools allow acquirers to optimize their manual fraud investigations, leading to efficiencies and savings.