AEROSPIKE

THE RISE OF PAYMENTS FRAUD

HOW TO SUPERCHARGE FRAUD ENGINES TO BEAT IT!

Despite the best efforts of our industry, payments fraud continues to rise – particularly in the online environment.

The most recent research available from online processing firm Vesta[1] suggests that between 11 and 13 percent of all card-not-present (CNP) transactions are fraud attempts. With each successful fraud costing firms between $108 and $155, Vesta estimate a mid-market firm with five million CNP transactions per year could experience 650,000 fraud events costing $16.25 million annually.

Identifying and preventing fraud is an increasingly difficult proposition given the proliferation of new payment methods such as instant payments (currently growing at 30% each year according to Mordor Intelligence[2]), digital wallets (predicted to account for almost half of all electronic transactions by 2026) and Buy-Now-Pay-Later schemes. Further complexity is added by criminal ingenuity, with new fraud methods such as synthetic ID and account takeover emerging as consumers turn to their mobile devices and laptops for their shopping needs, rather than shopping in-person. And this trend continues, with e-marketer/Insider Intelligence telling us online sales grew by 32% this year, almost double their earlier prediction.

Current first-line fraud defences such as EMV's 3D-Secure v2 (3DS2) to provide more secure, two-factor app-based authentication are helpful, but by no means fully effective. 3DS uses more than 100 transaction data points, risk scoring and elevated authentication to protect card transactions online. While European banks and retailers have experienced some reduction in online fraud using 3DS, it has been less effective in the United States where there is no regulatory mandate for escalated authentication methodologies. What's more, study after study shows that requiring two or three levels of authentication is unpopular with consumers and frequently leads to cart abandonment. Global payments consultancy CMSPI[3] reports that, in September 2021, escalated authentications yielded a failure rate on transactions of 29% in Europe, representing an estimated €90 billion of sales at risk over a 12 month period. This high rate of cart abandonment is unacceptable to most merchants.

[1] See: https://www.vesta.io/news/press-release-card-not-present-fraud-report-2021

[2] See: https://www.mordorintelligence.com/industry-reports/real-time-payments-market

[3] See: https://cmspi.com/eur/resources/sca-assessment-september-2021/

Artificial Intelligence (AI) and Machine Learning (ML): next-level fraud defence

To help combat these negative trends, companies are turning to AI and ML in the fight against fraud. While current AI and ML solutions are more sophisticated and effective than rules-based systems, there's still room for improvement. Fraud specialists surveyed by Brighterion[4] unanimously agree that AI is more effective than a rules-based approach, and that using AI helps to reduce the number of "false positive" fraud identifications (in which *bona fide* transactions are wrongly identified as fraud) as well as reducing fraud attempts and overall dollar losses. Likewise, processor Worldline estimates[5] that its fraud detection capabilities have increased around 30% thanks to the introduction of AI.

Rules-based systems can be slow and cumbersome, and are often one step behind the fraudster. The problem is that the rules are hard-wired into the system (for example, rules may not allow a payment transaction if one occurred on the same credit card within 20 minutes in a different state.) This means they can only deal with known fraud techniques, and not with new fraud methods devised by criminals. Using our example of a rule that declines transactions presented from different US states within a given time period, we can imagine a 'false positive' generated for a genuine transaction if a person living in New Jersey buys a coffee, then takes a train into New York and attempts to buy something else 30 minutes later. This second transaction would be declined – something that happens more frequently than it should with rule-based systems.

Rule-base systems can be quite complex, with some systems having built more than 10,000 fraud rules in their library against which transactions are evaluated. By contrast, an AI-based anti-fraud system examines between 100 and 300 customer and transaction data attributes for anomalies, making them faster and more accurate than previous approaches. These systems can also be self-learning, meaning that they adapt to see new fraud patterns in the data.

However, fine-tuning these systems remains a challenge, with operators forced to make trade-offs between the number of transactions allowed to pass as genuine versus those tagged as potentially fraudulent. If too many "false positives" occur and authentication is escalated or a transaction is declined, then the user often simply switches to another payment method to fulfill their needs, resulting in lost revenue and decreased customer loyalty. Transaction security specialists RiskIdent[6] estimate that sales worth more than $4 billion are lost in the US each year to transactions wrongly tagged as fradulent.

> "According to RiskIdent, more than $4 billion in US sales is lost to *false positive* fraud identifications each year."

[4] See: https://www.forbes.com/sites/louiscolumbus/2019/09/05/how-ai-is-protecting-against-payments-fraud/?sh=1199cb1c4d29

[5] See: https://worldline.com/en/home/knowledgehub/navigating-digital-payments.html

[6] See: https://riskident.com/en/news/how-fraud-prevention-affects-online-shopping-cart-abandonment-rates/

Fighting fraud with neural networks: next-level defence

Neural networks, also known as artificial neural networks (ANNs) or simulated neural networks (SNNs), are a subset of AI and sit at the heart of deep learning algorithms. Inspired by the way the human brain learns, neural networks rely on training data to learn and improve their accuracy over time. However, once these learning algorithms are fine-tuned, they enable data to be classified and clustered at a high velocity. As neural networks develop, they are increasingly being used to enhance the AI used to fight fraud and deliver a quantum leap in anti-fraud performance.

> “Neural networks are increasingly being used to deliver a quantum leap in anti-fraud performance.”

Neural networks get much of their power from their ability to ingest and process enormous amounts of data, hence they are sometimes also referred to as ‘deep learning’ systems. When applied to payments, some neural networks draw in data from up to 20 million attributes. These include everything from credit scoring histories to demographic and geolocation data, as well as the practice of “clustering”, or comparing an individual’s shopping behaviours to that of similar individuals. By drawing in data from a broader time range and a wider palette of sources, neural networks can make better decisions about which transactions to pass and which to flag as potentially fraudulent. In turn, this decreases cart abandonment as fewer transactions are identified as “false positives”, meaning that overall revenue is enhanced. Meanwhile, using neural networks leads to better identification of actual fraud and reduces revenue dollars lost to fraud as a result.

> “using neural networks leads to better identification of fraud and reduces revenue lost to fraud, with lower levels of *false positives.*”

Fraud defences fit for the digital economy

As digital commerce becomes a mainstay of everyday life, better automation in monitoring transactions for fraud is a necessity. At present, some 90% of commercial enterprises are engaged in the process of digitizing their systems – and AI, supercharged with neural networks, is essential to ensuring that fraud detection systems are fit for purpose in today's fast-moving environment. Forward-thinking enterprises are already switching to neural networks for better results, including better fraud capture, dramatic reductions in false positives, and much richer data to support decision making, inform your future anti-fraud strategy and resolve disputed transactions. Some of the most advanced firms are even incorporating their customer fraud/risk metrics into their customer360 profiles to be able to fine-tune their product recommendations and pricing at the individual level.

Aerospike's NoSQL data platform currently powers some of the highest-performing anti-fraud systems in the world. With the ability to process data at extreme speed (less than 20 miliseconds) across enormous datasets from Terabytes to Petabytes and beyond, Aerospike has saved one major payments company more than $5 million per day in potential revenue lost to fraud. For a leading bank, we have introduced a single, unified system system across the different bank silos that monitors more than ten million credit card transactions daily and increased data throughput by 400%.

Aerospike NoSQL minimizes complexity by reducing the number of servers required to deliver optimal performance and can be deployed in any private or public cloud network, serving as a global data hub for your business. Such power and flexibility means our systems are able to handle the heaviest demands, including monitoring instant payments and analytics enquiries from multiple users.

For more about how your organisation can benefit from next-generation fraud defence supercharged with AI and neural networks, contact us.

Stuart Tarmy
Global Director, Financial Services Industry Solutions

starmy@aerospike.com

Aerospike Hybrid Memory Architecture™

PATENTED FLASH OPTIMIZED STORAGE LAYER

✓ Significantly higher performance & IOPS

STORAGE INDICES IN DRAM DATA ON OPTIMIZED SSD'S

✓ Predictable Performance regardless of scale

MULTI-THREADED MASSIVELY PARALLEL

✓ 'Scale up' and 'Scale out'

SELF-HEALING CLUSTERS

✓ Superior Uptime, Availability and Reliability

✓ Single-hop to data

AEROSPIKE

AEROSPIKE.COM

LEADING BUSINESSES RELY ON AEROSPIKE TO ACT IN REAL TIME AND SERVE AS THEIR FOUNDATION FOR THE FUTURE

PayPal experian DBS LexisNexis RISK SOLUTIONS