ACI UNIVERSAL PAYMENTS℠

MACHINE LEARNING DEMYSTIFIED

INTRODUCTION

Fraud is a growing problem for merchants — one that can cause significant damage to the bottom line. Recent research shows, for example, that retail fraud attempts in the U.S. tripled between 2017 and 2019, and that every dollar of fraud hits merchants with an average of $3.13 in associated costs.[1]

Detecting and preventing fraud is difficult, not least because it's constantly evolving. Machine learning is being hailed as one of the key tools that can turn the tide in the battle against fraudsters. While the technique itself isn't new, technology now enables the pooling and processing of mass data in a way that can boost machine learning power.

Yet machine learning is a very broad discipline, about which many (sometimes extravagant) claims are made. Merchants need to be clear about what machine learning can do, what it can't, what advantages it can deliver to fraud prevention, and how to incorporate machine learning into a strategy that strikes the right balance between minimizing fraud and maximizing conversions.

1 BOTTOM-LINE BENEFITS

In among the millions of transactions being processed by merchants every day, across multiple channels, fraud behaviors are not always obvious and they are constantly changing. Manually reviewing all these transactions is impossibly resource-intensive.

Hard-coded rules in traditional fraud prevention tools are not flexible enough to keep up. Enter machine learning models, which can analyze massive amounts of data, learn quickly from millions of historical transactions and remember behaviors that allow a prediction to be made much faster than a human ever could. These models can identify patterns in the data that are too complex for humans to spot.

When applied to fraud prevention, this means that machine learning models can learn the difference between genuine and fraudulent transactions, using certain attributes to make predictions about future transactions in an automated way. This translates into powerful benefits for merchants, including:

FASTER, MORE ACCURATE FRAUD DETECTION

Machine learning techniques can help merchants to spot trends and trigger relevant reactions. By applying pattern recognition techniques to transaction data (from both fraudulent and genuine transactions), machine learning models build algorithms that can predict the probability of a transaction being fraudulent. Properly trained and tailored machine learning models can help increase fraud detection accuracy by as much as 40-50%.[2]

DRAMATICALLY REDUCED FALSE POSITIVES AND A BETTER CUSTOMER EXPERIENCE

This increased effectiveness also means fewer false positives and ensures that genuine customers are not declined or delayed by manual review processes.

[1] 2019 True Cost of Fraud, LexisNexis
[2] ACI use cases 2018

SAFE ACCEPTANCE OF REAL-TIME PAYMENTS AND FASTER FULFILLMENT

Because machine learning models quickly and efficiently analyze vast amounts of data, they can spot fraud signals in a fraction of a second and combat emerging fraud threats. This can help merchants to safely accept increasingly popular immediate payments options, such as bank transfers, and offer faster fulfillment, including same-day delivery, click & collect or immediate downloads.

2 GETTING THE MOST FROM MACHINE LEARNING

With any machine, what you get out is only as good as what you put in — and this applies to machine learning models. The results that merchants achieve will only be as good as the inputs they provide to the model. The following four key principles are essential to ensure that your machine learning strategy performs optimally:

- **The right data is vital** – For a model to learn and then assess transactions accurately, the data used for training it must be relevant, complete, correct, timely and in mass volumes, based on historical transaction data from within the merchant's own customer base.
- **Broader data is better** – Critical to building rich intelligence is a good understanding of fraud trends within and across market segments and geographies. This can only be achieved with a continuous integration of up-to-date information from both internal and external sources. This is where global fraud intelligence, gathered from across a consortium of merchant businesses, can deliver significant value.
- **Ongoing monitoring is essential** – Machine learning models need to be trained, tested and re-trained as fraud trends evolve. Models can't simply be left to their own devices — they need to be monitored to ensure they are performing as expected, and performance should be expected to degrade over time.

  ACI's **new incremental learning models** have been developed to adapt to the smallest changes in fraud and spending patterns, as they happen. These models can adapt to new behaviors without the need to re-learn everything they already know. This enables them to perform optimally for longer and reduce the time and resources required for re-training.
- **Expert support is critical** – Data scientists and fraud specialists bring years of experience to the monitoring and management of models to define data requirements and build, train and optimize each model.

3 AMPLIFYING THE EFFECT

OPTIMIZING MACHINE LEARNING AS PART OF A MULTI-LAYERED APPROACH TO FRAUD MANAGEMENT

The speed and accuracy of machine learning models can have a strong, positive impact on fraud rates and detection costs, as well as supporting a better customer experience. Yet, however well it's implemented, machine learning is not a silver bullet nor an infallible solution to payments fraud.

That's because machine learning models make predictions based on behavior and patterns they have learned from a specific data set of transactions. This presents a few challenges:

- Not all fraudulent or high-risk transactions are associated with clearly suspicious behavior that would stimulate the model to flag the transaction
- Fraudulent transactions represent a small fraction of total transactions at any merchant, which means the data that models are trained on is necessarily limited
- Both fraudster and genuine shopper behavior changes over time, due to seasonal peaks, market changes and new attack strategies — something that machine learning models do not always manage well without extra measures or interventions

It is also fair to say that, however sophisticated your machine learning strategy, a single-layered fraud solution doesn't always present a sufficient challenge to today's professional and tech-savvy fraudsters. Relying on any single tool to detect fraud can leave the door open to fraudsters, and leave merchants open to fraud loss.

MULTI-LAYERED STRATEGIES THAT CLOSE THE NET ON FRAUDSTERS

While rules are commonly used in conjunction with models, they also play an important supplementary role in capturing fraudulent transactions that are not associated with clearly suspicious behavior.

They are significantly more efficient to implement where merchants want to include specific instructions, such as *"block transactions where the customer email address is on a black list,"* or where you want to factor in timely information from a domain expert, such as suspicious activities that have been seen in a specific location in recent days.

Another advantage of rules is that they can be readily tailored by product, sector, channel or geography, and adjusted to cater to product launches, promotions or time of day if this is indicated by fraud intelligence. They can be deployed in real time to counter fraud attacks as they happen, or in silent mode to test and enhance fraud strategies.

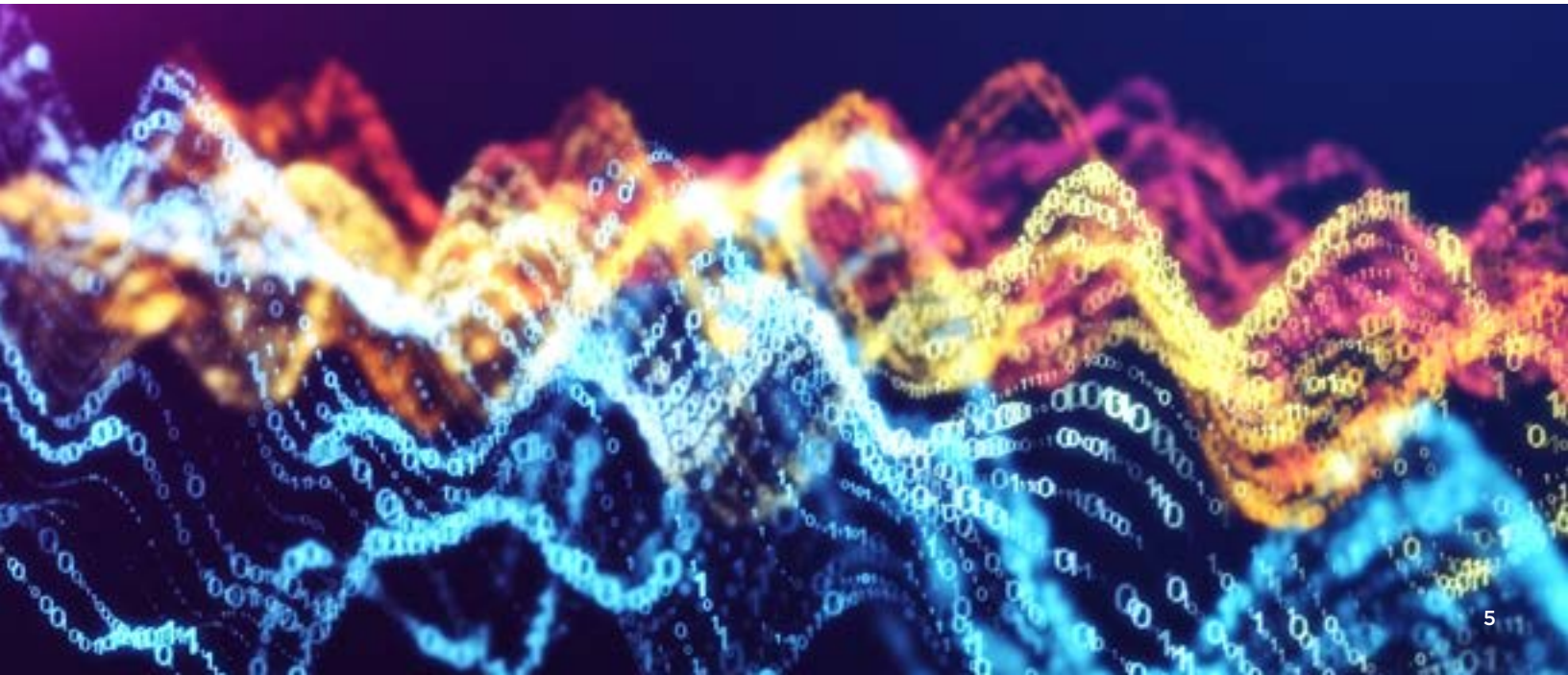
As closely integrated components of a fraud prevention strategy, machine learning and rules are a powerful combination, supporting one another to provide enhanced fraud prevention performance. They can, and should, be supplemented by a range of other tools and processes to optimize detection and boost genuine sales.

Multi-layered decisioning enables merchants to take advantage of a range of information that is available at or before authentication and during authorization. Tools such as device information, geo or IP location, and behavioral biometrics, for example, provide a wealth of opportunities to determine the risk associated with a transaction and to increase protection against attacks through enhanced accuracy and flexibility. Advanced customer profiling can play a significant role by enabling and easing the path of genuine customers. The support of risk experts can also be critical in tailoring fraud strategies to respond to changing threats and customer behavior.

4 SIX ACTIONABLE INSIGHTS FROM ACI'S DATA SCIENCE TEAM

1. **Prepare the right data:** Machine learning models will analyze the data provided to understand the difference between a good transaction and a bad transaction. The model needs to have sufficient, relevant examples of fraudulent transactions to understand what fraud "looks like." This also necessitates having good quality labels in the data. If a fraudulent transaction is not correctly labeled as fraud, it can confuse the model. Having good quality labels is crucial to identifying fraud patterns.
2. **Spend time on feature engineering:** Some data points can contribute valuable but complex information. Deconstructing those values into new attributes could help a machine learning model to identify the most important information in transaction data. For example, date and time values can be separated into weekday/weekend or morning/afternoon/evening, or a new attribute could be created to measure the time elapsed between the previous transaction and the new one.
3. **Use forward thinking when training:** Machine learning models will make predictions based on the fraud patterns they are shown in the training phase. If the training sample is significantly different from the test or validation sample, the prediction will not be accurate. For example, if we teach the model the difference between fraud and genuine transactions based only on December transactions, the performance of this model on the following months may not be optimal, since shopping behavior in December is very different.
4. **Make use of domain expertise:** More data is not always better. If too much information is fed to the model, the valuable information may be lost. A domain expert can help identify the most appropriate and valuable data for fraud detection and model training.
5. **Track performance:** Fraud patterns are constantly changing and it is important to test and track the performance of every model over time. As new fraud behaviors emerge, it may well be necessary to re-train the model to maintain optimal performance. Consider incremental learning models to reduce the amount of re-training required.
6. **Include machine learning within a multi-layered approach to fraud prevention:** Use a combination of tools and techniques, and the support of expert analysts, to ensure you stay one step ahead of the fraudsters.

To learn more about machine learning and ACI's advanced incremental learning capabilities, contact merchantpayments@aciworldwide.com.



ACI UNIVERSAL PAYMENTS

ACI Worldwide®, the Universal Payments® (UP®) company, powers electronic payments for more than 6,000 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers' premises or through ACI's private cloud, we provide real-time, immediate payments capabilities and enable the industry's most complete omni-channel payments experience.

LEARN MORE

WWW.ACIWORLDWIDE.COM

@ACI_WORLDWIDE

CONTACT@ACIWORLDWIDE.COM

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL7197 06-20