Machine learning: a silver bullet?

The role of machine learning in fraud management.

CyberSource®
A Visa Solution

In a digital economy, new business models and digital channels mean customers have high expectations.

It has to be quick and easy for people to pay. At the same time, fraudsters are probing the weaknesses of new digital processes.

As the person who can decide whether a transaction is accepted or rejected, fraud managers have a pivotal role. They're not just preventing losses from chargebacks. They're gatekeepers to accepting more revenue. It's a complex job. But get it right, and they enable their business to engage customers better – across devices and places. And that can mean supporting the very growth of the business.

In this landscape, the idea that a technology like machine learning might be the answer to all the industry's needs is attractive. But while machine learning should be a key part of an effective fraud strategy, the truth is that there's no silver bullet. So, in this paper, we'll look at how best to put machine learning to use. By employing it in tandem with expert insight, merchants can use it to accept the optimal number of payments. And make a direct impact on the success of their businesses.

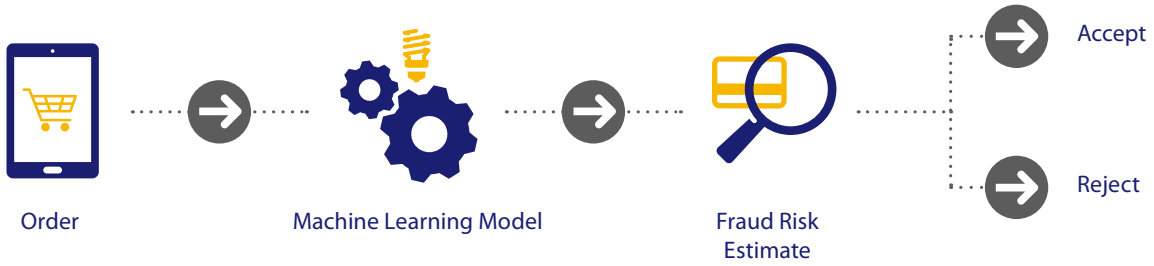
In this white paper, we address questions like:
What is machine learning? What can it do? What can't it do?
What does this mean for merchants?
And how is machine learning integral to CyberSource's Decision Manager?

What machine learning really means.

While machine learning relies on complex statistical methods and high-power computing, it's essentially a very simple concept.

By identifying and examining the statistically high- and low-risk combinations of transaction data, machine learning software can learn to make accurate predictions about what might happen in the future.

Machine learning begins with human-guided computing software that sifts through large volumes of historical data points and identifies the historically relevant data relationships. Then, all this information is fed into a variety of algorithms to arrive at predictions and assumptions. Once in place, these programs continue to consume large amounts of data and gradually get better at identifying the high- and low-risk relationships. This is where the actual learning takes place.



Static models versus self-learning models.

There's a spectrum of key options for merchants to use machine learning.

On one end of the spectrum are static models, which learn how to identify fraud at a point in time by consuming large volumes of historical transaction data. These models are effective at identifying historical fraud patterns, and tend to work well right after they are built. However, their static nature prevents adaptations, and this limits their ability to address new patterns of fraud as they emerge.

At the other end of the spectrum are self-learning models. These continuously consume new transactional data points to recognise and adapt to evolving fraud patterns. While self-learning models have historically been used to identify the latest fraud schemes, the nature of these models makes it very difficult for a human to manage what the machine learns. This difficulty can lead to issues such as rejection of legitimate customer volume.

As we will soon learn, there are pros and cons at each end of the spectrum, and a balance must be struck to maximise the effectiveness of the machine learning functions.

The potential rewards of getting the right balance are great. The fraud pattern of today isn't going to be the fraud pattern of tomorrow. So fraud managers who can pre-empt and adapt could help their businesses gain a competitive edge.

Data sources are key to machine learning

Historical Identity Interactions
Past interactions with similar identities?

Information Validity
Are any identities clearly invalid (e.g. undeliverable address)?

Account Activity
Prior activity using this payment information?

Geolocation
Billing and shipping information?

Device Intelligence
Device information (e.g. IP address jailbroken)?

What machine learning can help to do:

- **Facilitate real-time decision-making**
  At the core of many fraud-mitigation platforms is a rule-based system. Such systems rely on people creating rules that will determine which orders to accept, reject or send to manual review. While these systems are often quite effective, they do require a great deal of time-consuming manual interaction. Machine learning can help reduce this time requirement by evaluating large amounts of transactional data in real time.
- **Improve accuracy**
  Criminals are increasingly creating more subtle and non-intuitive patterns to avoid detection. As these subtle patterns become more difficult for humans to identify, machine learning techniques can be incorporated to spot them.
- **Rapidly respond to change**
  Because fraudsters are always changing their tactics, it's a constant cat-and-mouse game. Machine learning is continuously analysing and processing new data, then autonomously updating models to reflect the latest trends.
- **Reduce costs**
  Significant advances in technology have reduced the costs associated with machine learning solutions and the computing systems capable of running them. As machine learning helps improve accuracy, it can also reduce costly false positives, and the time and expense of manual reviews.

What machine learning cannot help to do:

- **Create quality data**
  Machine learning relies on good input data. There must be enough relevant data points to identify legitimate cause-and-effect relationships. Without the appropriate data, the machine may learn the wrong thing and make erroneous or irrelevant fraud assessments.
- **Stand alone without manual inputs**
  Machine learning is only as good as the human data scientists behind it. Even the most advanced technology cannot replace the expertise and judgement it takes to effectively filter and process data and evaluate the meaning of the risk score.
- **Maintain full transparency**
  Machine learning is often a black box, especially when self-learning techniques are employed. The machine can learn the wrong thing. For example, under normal circumstances, orders with overnight shipping might often be considered fraudulent. While that may hold true for most of the year, it could reject a lot of good customers during the holiday season.

A way to counteract the downsides of machine learning is to combine an automated machine learning system with a rules-based approach. Rules can act as a set of guidelines that give businesses more immediate control over fraud decisions.

What does this mean for the merchant?

A merchant looking to harness the power of machine learning should focus on the ability of a machine learning platform to enhance an existing set of rules-based models.

There are several rules-based platforms in the marketplace that do just this. These platforms help merchants lower costs, respond rapidly to change, increase accuracy and facilitate real-time decision-making. In short, they give fraud teams such as yours the tools to help optimise the level of payment acceptance.

When reviewing solution providers based on machine learning functionality, it is important to know what questions to ask. Here are a few valuable examples:

- **Is your vendor using proprietary technology or relying heavily on third-party data sources?**
  Too great a reliance on the latter could lead to unpredictability and loss of some operational control.
- **How much initial lead time is required for models to be considered fully up to speed?**
  Many solution providers promise an average 90-day lead time, while others require longer. Regardless, during this time your models and fraud mitigation functions are not optimised and this can lead to vulnerabilities.
- **How large a data set is available to train models?**
  Merchant-specific data is important. But it's even more important to leverage a large external network of merchant data and risk indicator. The more data available to the merchant, the more accurate the models – and the faster they can get up to speed.

CyberSource's approach to machine learning.

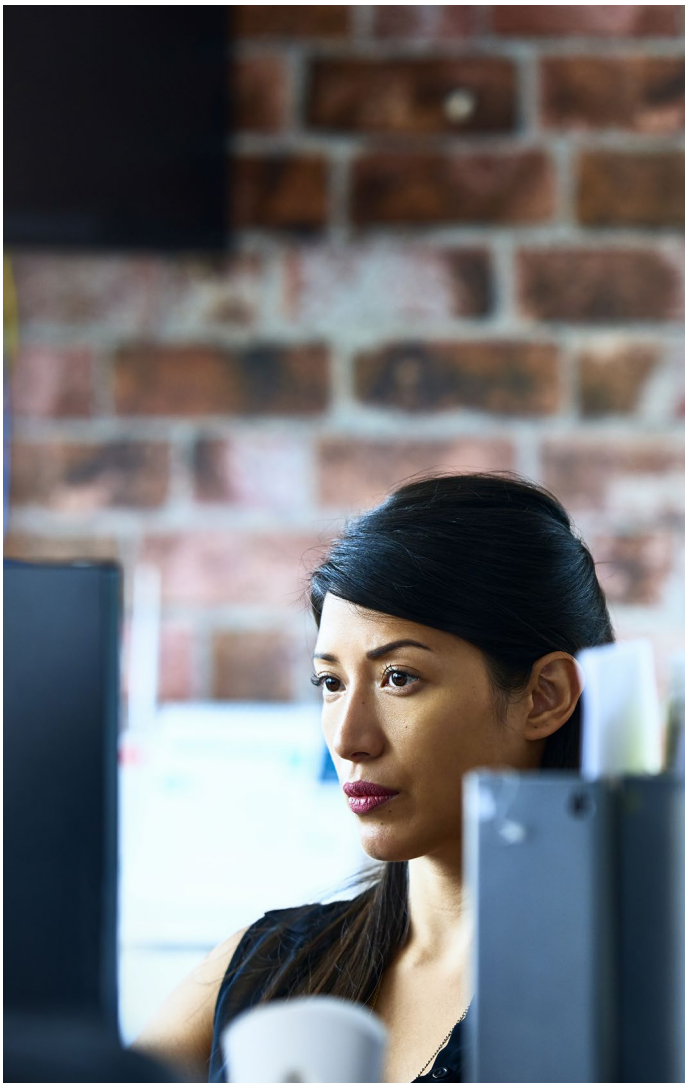
Machine learning has served as a core part of CyberSource's Decision Manager since 1999.

Even prior to Visa's acquisition of CyberSource, the companies were co-developing risk solutions supported by machine learning. Today, the CyberSource fraud management solution serves as a testament to this continued wave of development. Not only are there now more than 260 anomaly detectors, but there are 15 region-, channel- and industry-specific risk models, each optimised to identify fraud in different scenarios. A multifaceted fraud strategy is a should-have for a modern merchant. Fraud is different across markets, devices and channels. For fraud managers, agility is stability.

Meanwhile, machine learning has become ingrained in CyberSource's fraud-fighting capabilities and is the centerpiece of Decision Manager's approach to fraud scoring. It combines the proven effectiveness of conventional static models with the more agile data analysis of today's most advanced self-learning models. By doing so, it helps businesses manage and detect fraud more effectively and efficiently.

Importantly, the CyberSource Decision Manager platform doesn't just rely on one machine learning method to generate its risk assessments. That is because no single model works best in all situations – effectiveness depends on the type and amount of data, the requirements of the user, and other factors.

In addition, CyberSource's rules-based engine ensures the business is the ultimate decision-maker. Businesses have the flexibility to set and adjust rules at any time through a user interface. The rules engine provides added transparency, since businesses can easily see what rules were triggered in a decision. CyberSource's machine learning model, in tandem with a flexible rules engine, represents a powerful combination that allows for swift and accurate responses to unique or emerging fraud trends. By refining a fraud strategy faster, you can minimise losses. But you can also maximise the number of payments from legitimate customers. And in doing so, you can help protect the customer experience that your business needs to compete.



Find out more about our machine learning at
www.cybersource.co.uk/strengthenyournumbers

Contact us

Email. europe@cybersource.com www.cybersource.co.uk

CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast $427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues and mitigating risk. For acquirer partners, CyberSource provides a technology platform, payments expertise and support services that help them grow and manage their merchant portfolio to fulfill their brand promise. For more information, please visit www.cybersource.com

CyberSource®
A Visa Solution