Fighting fraud the smart way — with data analytics and artificial intelligence

For Mastercard and other global payments processors, AI systems are a watchdog that never sleeps

ABSTRACT

By using sophisticated technologies and massive amounts of data, the payment-processing industry is fighting back against credit card fraud in innovative ways. The technologies that go into fraud-prevention systems enable players in the industry to instantly analyze data while continually training algorithms to help them improve their ability to recognize fraudulent activities. Parallel efforts are helping the industry ward off bad players on the merchant side.

July 2018

TABLE OF CONTENTS

A GROWING PROBLEM

Payments card fraud is also a growing problem and constant concern for merchants around the world. A 2018 study by the credit-reporting firm Experian found that almost three-quarters of surveyed businesses cite fraud as a growing concern over the past 12 months and nearly two-thirds reported the same or higher levels of fraudulent losses over that same period.[1] Consumers, too, are worried. The Experian study found that lack of visible security was the No. 1 reason customers abandoned transactions.

Credit card fraud is a problem with a massive price tag. The Nilson Report, a publication that covers the worldwide payments system, predicts that worldwide losses as a result of credit card fraud will exceed $31 billion in 2018. That's an amount equal to 7.3 cents for every 100 U.S. dollars of total card volume.[2]

As high as it is, the cost of card fraud would be much higher were payment processors not waging a constant fight against fraud, using all the tools at their disposal. These tools include machine-learning technologies, artificial intelligence algorithms and high-performance computing systems that examine every transaction in a matter of milliseconds.

ONE COMPANY'S FIGHT AGAINST CARD FRAUD

Mastercard is among the payment-processing companies fighting back against fraud every second of every day, using a war chest filled with sophisticated technologies. A case in point: To identify and stop fraudulent transactions, Mastercard leverages machine-learning algorithms running on HPC systems to process large data sets at lightning-fast speeds. In an interview with the tech-industry program theCube, Nick Curcuru, vice president of the big data practice at Mastercard Advisors, said the goal is to stop fraud in its tracks without disrupting or delaying legitimate transactions.[3]

While that's a challenging proposition for any company involved in retail sales, the scale at which Mastercard operates makes the problem all but unfathomable. According to Curcuru, Mastercard has 2.2 billion cards in use in 330 countries. It processes 160 million transactions per hour, using machine-learning algorithms and applying 1.9 million rules to examine each transaction. It all happens in a matter of milliseconds.

The horsepower for this fraud-prevention engine is a secure, Payment Card Industry (PCI)-certified Apache™ Hadoop® cluster based on high-performance computing systems from Dell EMC. This fraud-detection machine-learning system uses supervised learning to look for established fraud patterns and unsupervised learning to identify emerging fraud patterns in real time.

With every transaction, the machine-learning algorithms examine things like a cardholder's buying habits, geographic location and travel patterns, along with real-time data on card usage — such as what they are trying to buy, where they are trying to buy it and what else they bought in the same day. Each transaction is analyzed in terms of the rules that relate to what a valid transaction looks like and what a fraudulent transaction looks like. The name of the game is to outsmart some really smart people with criminal intent.

1 Experian, "The 2018 Global Fraud and Identity Report," January 2018.
2 The Nilson Report, "Card Fraud Worldwide," October 2016.
3 Interview with theCUBE conducted at Dell EMC World 2017.

"For us, it's a question of how can we stay one step ahead, because the fraudsters themselves are just as smart as we are," Curcuru told theCube. "They are graduating from some of the top universities worldwide. They are doing big data analytics themselves. This is a big business for fraudsters worldwide."[2]

To keep ahead of the bad guys, the machine-learning algorithms are always learning, so they can get continually better at what they do. "It's all about learning," Curcuru says. "It's not just one and done. The algorithms have to be constantly updated — in real time in some cases — so you're constantly in a learning phase."[4]

PUTTING BIOMETRICS TO WORK

On another front, Mastercard is increasingly using biometrics, such as fingerprint, iris and facial recognition, as another tool to verify the identity of card users. For example, the Mastercard Identity Check service allows online shoppers to authenticate a purchase by touching the screen of a smartphone or simply showing their faces to the device and blinking — a concept sometimes referred to as "selfie pay."[5]

WARDING OFF RISKY MERCHANTS

Fraud-prevention efforts also focus on warding off risky merchants. That's the case with a Mastercard solution that helps financial institutions evaluate a merchant's credit risk. The solution — called MATCH, for Mastercard Alert to Control High-risk Merchants — leverages a database with data on known and potentially fraudulent businesses. Mastercard acquirers use MATCH to find out whether other acquirers have terminated a merchant in the past and the reasons for the terminations. This helps financial institutions make informed decisions about onboarding merchants. Mastercard acquirers submit nearly a million inquiries to the database each month.

In its latest iteration, the MATCH platform leverages Cloudera Enterprise and Cloudera Search running on Dell EMC Ready Bundles for Hadoop. The Cloudera enterprise data hub delivers the dynamic scalability and high performance Mastercard needs to accelerate searches and expand its user base, using Cloudera Search to provide acquirers with enriched searching capabilities and increased search accuracy, according to a Cloudera case study.[6]

The solution can index, match and sort results using several search algorithms and new scoring capabilities that were previously impractical to implement on a legacy platform. Additionally, the Mastercard staff can better tune data indexing to improve search performance. And with greater scalability and flexibility, the platform will enable Mastercard to expand its dataset and incorporate new data as industry trends and opportunities emerge.

4 Interview with theCUBE conducted at Dell EMC World 2016.
5 TechCrunch.com, "MasterCard launches its 'selfie pay' biometric authentication app in Europe," October 4, 2016.
6 Cloudera case study, "MasterCard: Creating New Revenue Streams with an Advanced Anti-fraud Solution," May 23, 2016.

CAPITALIZING ON HADOOP

None of this would be possible without the processing power and fast throughput of today's HPC clusters. These systems work together with data analytics tools and software frameworks, such as Hadoop, to enable the distributed storage, processing and analysis of huge amounts of data. And they often draw on the processing power of accelerators, such as a FPGAs, as well as leading-edge many-core CPUs, such as those in the Intel® Xeon® and Intel® Xeon Phi™ processor families.

When everything is connected with a high-speed, low-latency, next-generation fabric, such as the Intel® Omni-Path Architecture (Intel® OPA), payment processors have a system that can complete millions of tasks in the blink of an eye — and that's what it takes to detect and prevent the growing problem of payment-card fraud.

KEY TAKEAWAYS

With today's tools for capturing and analyzing enormous amounts of data, the payment-processing industry is fighting back against fraudsters in new ways. The technologies that go into fraud-prevention systems enable players in the industry to instantly analyze data while continually training algorithms to help them improve their recognition of fraudulent activities. Parallel efforts are helping the industry ward off bad players on the merchant side.

The end result of these efforts is a more trustworthy transaction experience for legitimate cardholders and merchants and more digital barriers to stop the criminals who try to exploit vulnerabilities in the payment systems.

For additional information, visit DellEMC.com/AI.

To learn more, visit: DellEMC.com/AI