redislabs
HOME OF REDIS

Fighting Financial Fraud with a Real-Time Data Platform

Financial fraud is growing rapidly—the ability to process data quickly and identify patterns with AI and machine learning can help your fraud detection programs meet new challenges.

Introduction

Fraud and other cybercrimes are an ongoing threat, and the situation is getting worse. PwC's 2020 Global Economic Crime and Fraud survey found that 47% of companies had experienced fraud in the past two years at an estimated total cost of $42 billion.

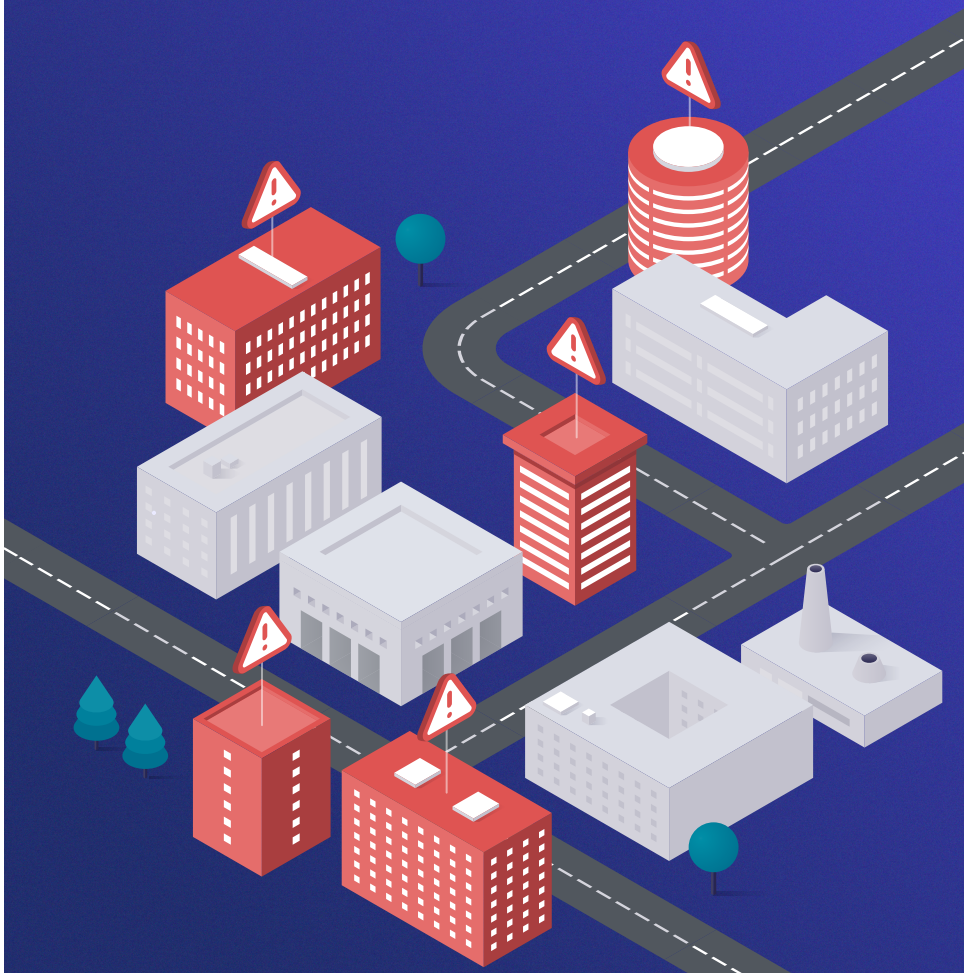
As online banking usage grows, fraud has also expanded. More than a third (35%) of retail banking customers increased their use of online banking during the Covid-19 pandemic, and it's safe to assume that this could become a new normal. As the payments industry continues optimizing transactions for maximum speed, fraud detection platforms have even less time to react.

Given the high costs associated with remediating financial fraud after the event, companies are working hard to improve their ability to detect and prevent fraud from occurring. KYC and anti-money laundering measures have long played a role in detecting fraud, but criminals are constantly devising new ways to game the system. Companies that cannot deploy the latest tools to stay ahead of malicious actors may find themselves targeted more often.

The industry clearly recognizes it has a problem, and financial services companies are investing in advanced tools to solve it. Forrester predicts that enterprise spending on cloud security tools, for example, will reach $12.6 billion by 2023, up from $5.6 billion in 2018. But what tools should they invest in, and what trends should they focus on? This white paper examines the latest trends in financial fraud, suggests areas where companies can fight back effectively, and explains how Redis is helping businesses achieve these goals.

47% of companies had experienced fraud in the past two years at an estimated total cost of

$42 Billion



Transaction fraud

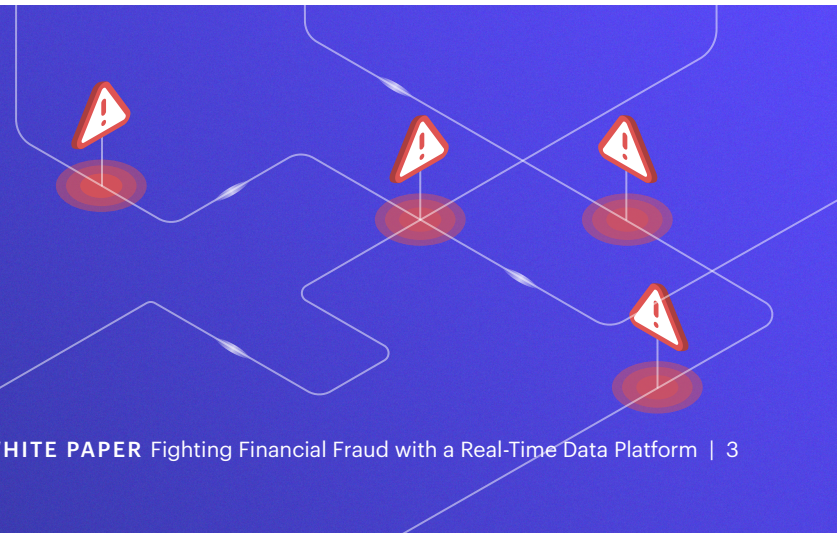
With the growing speed and scale of online banking, fraud of all types is becoming more common. Losses from account takeovers increased by 72% between 2018 and 2019, and in the same year identity fraud hit its highest level since 2013, accounting for losses of $16.9 billion in 2019. Retailers and financial services providers are also having to combat chargeback fraud, merchant fraud, and international payment fraud. The last one is particularly hard to track because companies often don't have a unified view of transactions across all markets, and fraud detection tools and methods frequently differ between countries.

All of this leads to a growing number of fraudulent transactions, and many existing online fraud detection services cannot process data quickly enough to identify these transactions as they happen. As a result, many firms are turning to artificial intelligence (AI) and machine learning (ML) to provide automated transaction scoring designed for the speed and scale of online banking. Some 70% of all financial services firms are already using machine learning for predicting transactions, adjusting credit scores and detecting fraud. But to be effective, AI and ML will have to be applied with greater speed and at a larger scale because of the needle-in-a-haystack nature of the problem.

As that metaphor suggests, there are many legitimate transactions for every fraudulent one, and inspecting every transaction takes effort and cost. And no system is perfect. Businesses frequently have to decide whether it is cost effective to inspect more transactions in detail, or just accept a certain level of fraud—and financial institutions routinely choose the latter. Advanced statistical analysis is the key to making these types of decisions as accurately as possible.

By efficiently examining patterns in data to determine the likelihood that a transaction is fraudulent, AI-based platforms can automate decision-making. In some cases they are up to 40% faster than simpler rules-based fraud detection systems, with the same rate of false positives. In the case of ***supervised learning***, labeled data (which is organized in some way, for example, to identity name, address, and phone number) is used to train an AI model to predict whether a transaction is fraudulent or not. ***Unsupervised learning***, on the other hand, uses unlabeled data (where the data is not organized or explained, for example, audio recordings or photos) and is better at finding new patterns of fraud. To make this kind of detection possible, the AI engine needs continuous access to reference data—in the form of transaction details, user profiles, geospatial information, device metadata, and so on—that tells it what fraudulent activity looks like.

> "Many existing online fraud detection services cannot process data quickly enough to identify these transactions as they happen."

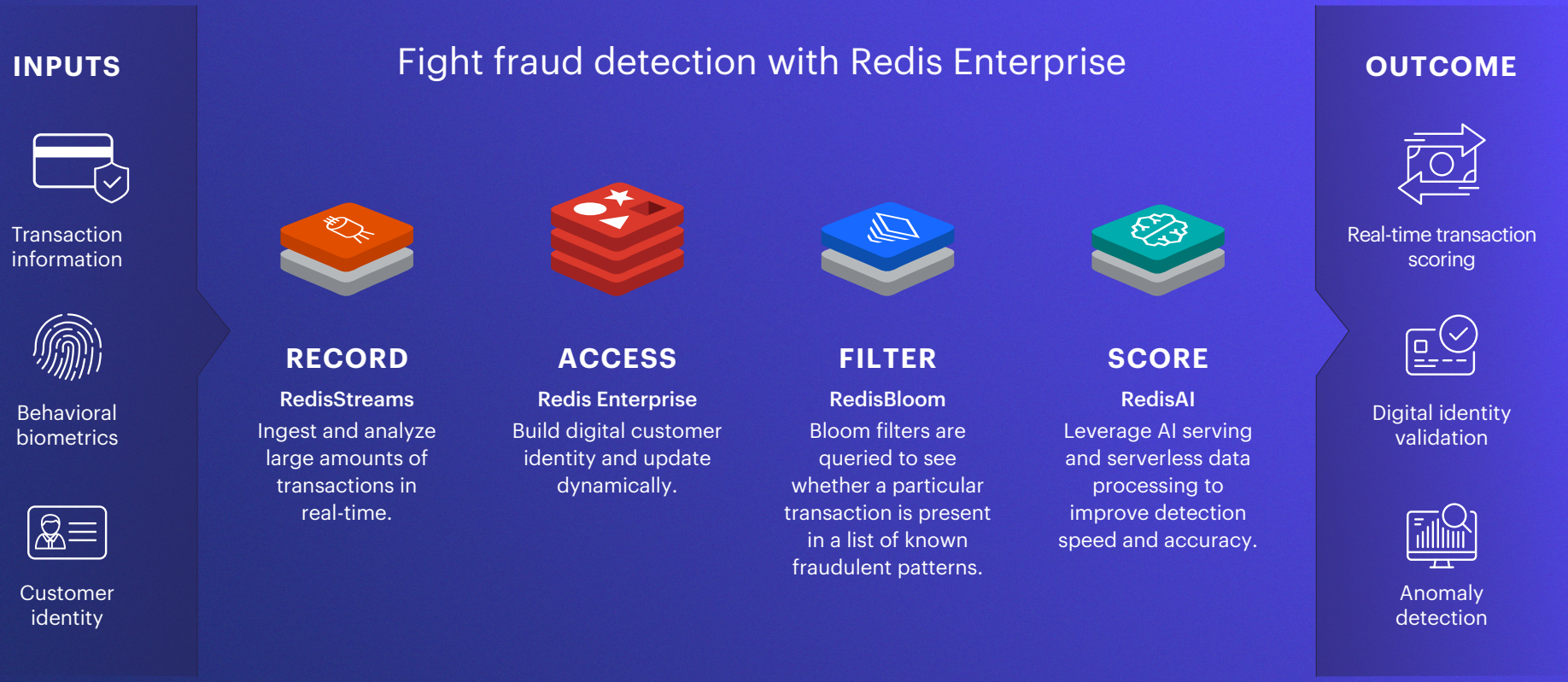


However, the further that data is—in internet terms—from the AI engine, the longer the process takes. The differences in human terms are tiny, but criminals can launch thousands of attacks per second. Storing inference data as close as possible to the systems serving AI models for transaction scoring eliminates a significant amount of computational and networking overhead, giving transaction scoring platforms a better chance of keeping up.

Applications can also use Bloom filters to check whether something is or is not present in a given set of items. For example, a Bloom filter might be used to determine whether a given transaction ID was present in a list of known fraudulent patterns, or to track customer passwords and prevent the reuse of old ones. **Probabilistic** supports Bloom filters that let users efficiently query data for set membership in Redis without directly storing sensitive information.

That can help fraud detection platforms filter through large volumes of transactions in real-time without compromising customer information. As transactions speed up, automation is vital. Fraud is impossible to eliminate entirely, but AI and ML enable financial services companies to construct the best possible defense.

Fight fraud detection with Redis Enterprise



Know Your Customer

In mid-2014, a man named Rojo Filho opened at least 17 bank accounts in his own name and, according to prosecutors, used them to run a fraudulent investment scheme. Filho had previous fraud convictions before he opened any of these accounts and should have been detected by KYC rules designed to limit money laundering, fraud, corruption, and funding for illegal organizations. His case illustrates just how easily even a convicted criminal can slip through the cracks.

Banks have been required to follow KYC regulations for some time. They are vital to fraud prevention and for maintaining customer trust. However, many still rely on knowledge-based authentication (KBA), which uses attributes such as names, addresses, Social Security numbers, and security questions to verify a person's identity. This so-called "static information" is updated relatively infrequently and is vulnerable to data breaches and theft.

That's why banks are turning to increasingly sophisticated means of verifying identity, combining that data with existing customer information. For example, document verification and face or fingerprint records can be combined with behavioral patterns, such as the types of transactions a customer makes most frequently or how they type on a touchscreen phone. Blending traditional customer information with alternative data sources means financial institutions can create a digital identity for their clients that is not only harder to fake, but can be updated dynamically.

With multiple sources and types of data comprising a digital identity, the challenge lies in updating everything quickly enough to stay ahead of criminals and avoid frustrating customers. The more quickly a customer's digital identity can be updated, the more effective it will be.

"With multiple sources and types of data comprising a digital identity, the challenge lies in updating everything quickly enough to stay ahead of criminals and avoid frustrating customers."

Unfortunately, as digital identity has grown more sophisticated, so too has the ability for criminals to steal or fake them. Synthetic identity theft, where real and fake information is combined to create a new identity, was behind 20% of credit losses by US lenders in 2016 and has been described as the fastest-growing type of financial crime in the US. Blending multiple pieces of real customer information into wholly new identities results in fraud that is nearly impossible to detect using traditional KYC techniques. Because no actual consumer exists to report fraudulent activity, fraudsters can operate credit card and loan accounts legally for long enough to appear legitimate and improve their credit standing, then max out the line of credit and disappear.

Graph databases are particularly useful in fighting synthetic identity theft and improving KYC procedures. Representing and storing data as a series of nodes and edges that model the relationships between data points can be faster and more flexible than traditional databases for certain types of queries, including identifying suspicious transactions. Graph databases are based on relationships between entities, which makes them very useful for uncovering suspicious patterns or uncovering connections between suspicious entities.

Redis Enterprise provides a number of options for financial institutions looking to strengthen their KYC procedures and fight back against sophisticated identity fraud. First, it can act as a fast in-memory database to deliver the low latency and high write throughput required to keep digital identities updated in real time. BioCatch, an Israeli firm that provides behavioral biometrics technology used to protect account openings and prevent identity fraud, uses Redis Enterprise as a database handling a variety of mission-critical information across the organization, including behavioral data captured during active user sessions, predetermined profiles on fraudulent behavior, geolocation data, and system configurations.

Employing multiple tools gives financial services companies their best chance to identify customers correctly. While identifying fraudulent actors is a challenging problem, companies that are able to do it most effectively will reduce the number of fraudulent transactions they deal with, taking pressure off other parts of their business.

Probabilistic supports Bloom filters that let users efficiently query data for set membership in Redis without directly storing sensitive information.

Anti-money laundering

Anti-money laundering (AML) is a regulatory requirement for financial institutions and there are stiff penalties for non-compliance. US regulators have traditionally taken a tough stance, but in 2019 European authorities issued criminal penalties exceeding those levied by the US. It is estimated that as much as 5% of global GDP, or up to $2 trillion, is laundered globally every year.

The challenge for institutions is to identify the ultimate beneficial owner—the person actually controlling or benefiting from a transaction—and what their business is, while monitoring customer behavior to identify suspicious activity. Additionally, firms must manage disparate databases and systems and deal with a high level of false positives in detecting illicit transactions: more than 95% by some estimates.

Some banks are becoming increasingly sophisticated in their approaches to identifying suspicious activity, commensurate with corporate risk profiles, for example, by building or enhancing internal financial intelligence units devoted to identifying more complex and strategic illicit finance threats. Banks are also exploring how artificial intelligence and digital identity technologies can be applied to AML compliance programs. These innovations can strengthen AML compliance approaches, as well as enhance transaction monitoring systems.

Customer segmentation and risk-rating are often used to fight AML, but they can often be inaccurate, so organizations are looking for new ways to reduce false positives and negatives. Network analytics can help find hidden links between entities that might be missed by traditional models, and transaction scoring is getting smarter with the help of AI technology.

A real-time transaction monitoring system acts as the cornerstone of an effective AML compliance program. An AML solution should be able to conduct transaction scoring for credit, debit, ATM, and prepaid cards (including digital wallets) for card-present and card-not-present payments, as well as automated clearing house (ACH), wire, and peer-to-peer transactions. As with other anti-fraud use cases, processing large amounts of information quickly and accurately is a major challenge. This is where a fast in-memory database like Redis Enterprise can help.

However, the global money laundering problem can be difficult for a company to tackle alone, regardless of the technology available. Even as new AML solutions are developed, financial services companies would benefit from greater collaboration to help them identify and prevent the problem.

> "It is estimated that as much as 5% of global GDP, or up to **$2 trillion, is laundered globally every year.**"

Tackling fraud while keeping customers happy

Financial institutions are constantly balancing the need to detect fraud and cybercrime while ensuring that legitimate customers enjoy speedy and efficient service. The ability to quickly process data and identify patterns is vital to combating all of the types of fraud described in this paper.

Redis Enterprise provides fraud detection platforms with the real-time access to data needed for financial institutions to quickly examine patterns in transactions, strengthen their KYC programs with new tools for digital identity, and fight back against AML and other more sophisticated forms of financial crime. Partnering with Redis Labs can enable your organization to focus on rapid innovation, rather than routine toil.

The challenge of financial fraud will continue to persist as more banking takes place in the digital world, but the companies that best manage their response now will gain immediate competitive advantage and set themselves up to develop even more robust fraud detection systems in the future.

> "Redis Enterprise provides fraud detection platforms with the real-time access to data needed for institutions to fight back against financial crime."

redislabs
HOME OF REDIS

To learn more about how companies power fraud detection platforms with Redis Enterprise, visit our page on **Redis Enterprise for Fraud Detection**.

To get started, try Redis Enterprise in the cloud, or download Redis Enterprise Software for a free trial now.

redislabs.com/try-free

About Redis Labs

Modern businesses depend on the power of real-time data. With Redis Labs, organizations deliver instant experiences in a highly reliable and scalable manner.

Redis Labs is the home of Redis, the world's most popular in-memory database, and commercial provider of Redis Enterprise, which delivers superior performance, matchless reliability, and unparalleled flexibility for personalization, machine learning, IoT, search, e-commerce, social, and metering solutions worldwide.

Redis Labs, consistently ranked as a leader in top analyst reports on NoSQL, in-memory databases, operational databases, and database-as-a-service (DBaaS), is trusted by more than 7,400 enterprise customers, including five Fortune 10 companies, three of the four credit card issuers, three of the top five communication companies, three of the top five healthcare companies, six of the top eight technology companies, and four of the top seven retailers.

Redis Enterprise, available as a service in public and private clouds, as downloadable software, in containers, and for hybrid cloud/on-premises deployments, powers popular Redis use cases such as high-speed transactions, job and queue management, user session stores, real time data ingest, notifications, content caching, and time-series data.

redislabs.com