FINANCIAL CRIME PREVENTION IN THE AGE OF SILOS AND ADVANCED FRAUD

Key Highlights

Advanced financial crime prevention methods in a variety of formats pose a big risk to financial organizations globally

Technology can help to mitigate risk for criminal activities in a variety of formats

Using data in your journey to advanced analytics and AI is a key way to address this

Financial Services firms have been hit with $36BN in fines related to financial crime since the last financial crisis. Today, almost every financial services organization has a siloed data environment across their financial crime divisions. For example, organizations might have financial crime databases across their anti-money laundering group, fraud group, cybersecurity group and surveillance group. Every one of those is typically individually siloed, not only from an organizational standpoint, but also from a data modelling and analysis perspective. This typically leads organizations to inefficiencies in combating financial crime holistically.

Cloudera and IBM together provide a comprehensive approach to managing your financial crime data, including maintaining data consistency and governance. With this holistic view across financial crime prevention, the ability to coordinate cross-organizational efforts increases, including use of machine learning models and real-time data. Using a holistic approach, financial services organizations are better equipped to stay ahead of criminal activity.

Synthetic ID fraud is one of the fastest growing types of financial crime globally. Criminals create a fake identity from legitimate information such as social security numbers, purchased or stolen data from the dark web. Using this newly created synthetic ID, they apply for a credit card or loan at a financial institution, which gets rejected - but this synthetic ID is then added into the institution's repository. The criminals then build up the profile of that synthetic individual over 6-12 months, until they have an address and other key kinds of information attached to that name - a job, a phone, a social media presence - all the while building up a credit profile. Eventually criminal is able to get access to credit. One of the first large synthetic identity fraud cases prosecuted was in the US in 2013. Thirteen individuals across four US states created 7,000 synthetic IDs, accessing tens of thousands of credit cards and ultimately stealing $200 million out of the financial system. Since then this type of fraud has only been rapidly growing.

McKinsey highlights the problem with synthetic ID fraud is that it's difficult to decipher someone who's real or fake, because it could be someone who has just graduated or someone who has just moved into the country for example: so there is no credit profile existing, but the person is legitimate. McKinsey showed that if you enhanced that data using machine learning, validating the depth of the data and the consistency of it, you can verify the real versus synthetic applicants. For example, the applicant has a Facebook account, but he hasn't used it for the last 6 months, has an email account that has existed for 6 months only and has an address that has only been around for 3 months - this applicant ID is highly likely to be synthetically generated. Using this methodology, McKinsey was able to prove it's possible to segment out the high-risk applicants that are potentially fake.

Large US Bank improves fraud capture rates

An omni-channel approach by this large US bank resulted in a 95% improvement in fraud capture rates and a 30% decrease in number of alerts.

Santander implements a single data platform to combat financial crime

Utilizing Cloudera technology, Santander was able to use a single data platform to protect 3.7 million customers from financial crimes, with 95 new proactive control alerts. Ultimately this reduced capital expenditures by $3.2 million and decreased operating expenses by $650,000.

High precision fraud detection algorithm to discern synthetic identities for this store credit card issuer

Leveraging Cloudera technology, including CDSW, high-precision fraud detection algorithms were built and leveraged to deepen fraud detection and prevention mechanisms and ultimately improve personalized customer experience. The result was 20-30% improved credit line assignments, with fraudulent behaviour uncovered in a matter of seconds versus days previously.

About Cloudera

At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. Cloudera delivers an enterprise data cloud for any data, anywhere, from the Edge to AI. Powered by the relentless innovation of the open source community, Cloudera advances digital transformation for the world's largest enterprises.
Learn more at cloudera.com

KYC, or Know Your Customer, is a mandatory process of identifying the individual or business opening account in order to verify their identity and legitimacy, in addition to continually checking this over time. In Europe, the KYC constraints have a minimum requirement of 22 variables per individual. In order to comply with the European data minimum requirements, a more robust, holistic environment is needed to enhance the existing data using many different data sources. Traditional KYC processes are limited in their ability to identify the layers of relationships that can exist and mask criminal activities. Advanced methodologies using a contextual approach to the data enables a more efficient approach to KYC regulatory compliance.

IBM and Cloudera

Cloudera Data Platform (CDP) is an integrated data platform that is easy to deploy, manage, and use. By simplifying operations, CDP reduces the time to onboard new use cases across the organization. It uses machine learning to intelligently autoscale workloads up and down for more cost-effective use of cloud infrastructure. CDP manages data in any environment, including multiple public clouds, bare metal, private cloud, and hybrid cloud.

Using Cloudera and IBM, the organization can look at this enhanced data from a holistic, enterprise-wide viewpoint - this can have direct benefits on both the retail and corporate side of the bank's business. In addition to benefiting the financial crime efforts of each relevant group within the bank, this could have additional insights and benefits for teams working on customer 360 and customer journey analysis by providing a single comprehensive view of the data. Overall, with the added insights and intelligence provided from the holistic, enhanced platform view of the data, investment is justified across multiple groups and use cases.

Based on the legal permittance of the application of advanced machine learning and AI algorithms in financial crime prevention, this is one of the most beneficial areas for applying Advanced Analytics technologies supplied by IBM and Cloudera. Our joint focus is on supporting customers in their journey to a holistic view of their data, covering AML, fraud, surveillance, cybersecurity and other use cases.

Working in a global partnership, IBM and Cloudera also provide:

- **Freedom of choice** for data environments, including hardware and IBM Cloud
- **Speed to innovation** using the power of the open source community
- **Security and governance** from the Edge to AI
- **One-stop support**, including multi-vendor support services through IBM
- **Faster ROI** with end-to-end capabilities offered
  Industry-expertise with vertical specialists on hand

Learn more at cloudera.com/IBM.

CLOUDERA

Cloudera, Inc. 395 Page Mill Road Palo Alto, CA 94306 USA cloudera.com