CLOUDERA

Fighting Financial Crime

How Data and Analytics Help in the Fight Against Financial Crime

Table of Contents

Introduction

Financial crime prevention is a continuous, never-ending battle. Criminal networks are creative, collaborative, and ready to exploit any opportunity inside or around the edges of business operations. Sophisticated techniques are used by criminals to breach defenses, profit from stolen data, and launder illicit proceeds throughout the global banking system.

When developing new approaches to protecting against financial crime, the challenge for financial services providers is multi-faceted. They must perform due diligence to know their customer and prove to regulators they have suitable programs in place to mitigate risk. At the same time, their customers expect fast, frictionless interactions with complete protection and privacy of their financial information.

Better data management, analytics and machine learning are proven tools in the battle against fraud. As digital services continue to evolve in the financial services industry, it is paramount to evolve anti-crime initiatives in parallel to maintain the trust and confidence of customers.

Battling Financial Crime requires vigilance and innovation.

Digital Innovations must be Protected

The dynamic and quickly exploding world of global ecommerce, crypto currencies, digital payments and eventually the metaverse strains financial crime measures to keep pace and transform alongside these initiatives. Criminals will exploit and capitalize on any new innovation.

Consumers worldwide are projected to use mobile devices to make more than 30.7B ecommerce transactions by 2026, a **5X** increase over the 6.1B predicted for 2022

NFCW

The global digital payment market size is expected to reach USD **236**.10 billion by 2028 and is projected to register a CAGR of 19.4% from 2021 to 2028.

Business Wire

Synthetic Identity Fraud makes up **85%** of fraud cases

CyberTalk

1,500 names added to a sanctions list could be associated with 15,000 people and entities

Waters Technology

data breach incidents are caused by employees' mistakes

Tessian

Regulations Continue to Evolve

Boundaries are disappearing between the physical world, the virtual world, and points of entry such as payments through mobile and wearable devices. While financial services providers seek to onboard customers using seamless digital interactions, quickly and without friction, they are under increasing pressure to know their customers. Regulatory agencies recognize the multifaceted challenges of financial crime and expect firms to take a proactive, innovative approach to disrupting it.

New Regulations such as the multi-national Multilateral Competent Authority Agreement (MCAA) and the US Corporate Transparency Act are evolving to improve anti-money laundering (AML)

MCAA - OECD

AML - Financial Crimes Enforcement Network

600%

World-Check experienced a **600%** increase in initial sanctions searches after the West announced sanctions against Russia

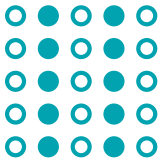
Waters Technology

The UK Financial Conduct Authority (FCA) identify challenger banks as a target for criminals. They are now offering guidelines to improve oversight and set higher standards.

Financial Conduct Authority

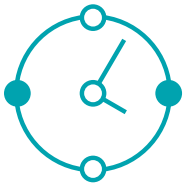
4 Data Pillars in Combating Financial Crime

Advancing the use of data and analytics in fighting financial crime can help firms gain a more holistic view of transactions and customers while enabling greater efficiency to interrogate the massive amounts of information that must be scrutinized. Key pillars of combating financial crime using data and analytics include:



Eliminate Silos

Legacy data warehouses and operating platforms spread across business units cause gaps and inconsistent data sources and processes. Enable a reliable, trusted enterprise data approach using a centralized data lake or APIs to establish the foundation for a comprehensive view of the data. This is critical as a foundation to identifying financial crime.

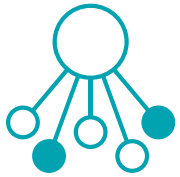


Enable Real-time data

As financial activities become more integrated into everyday activities, new varieties of crime patterns emerge. Streaming data that collects and analyzes data in real-time provides key insights for immediate, actionable intelligence into the factors that contribute to financial crime.

Activate AI

Machine learning techniques used in simulation models prepare firms for potential fraud and can significantly improve existing financial crime detection systems. Artificial intelligence helps increase the effectiveness and efficiency of financial crime investigations and can help to reduce false positives by being more adaptive to customer behavior.



Manage Data Security and Governance

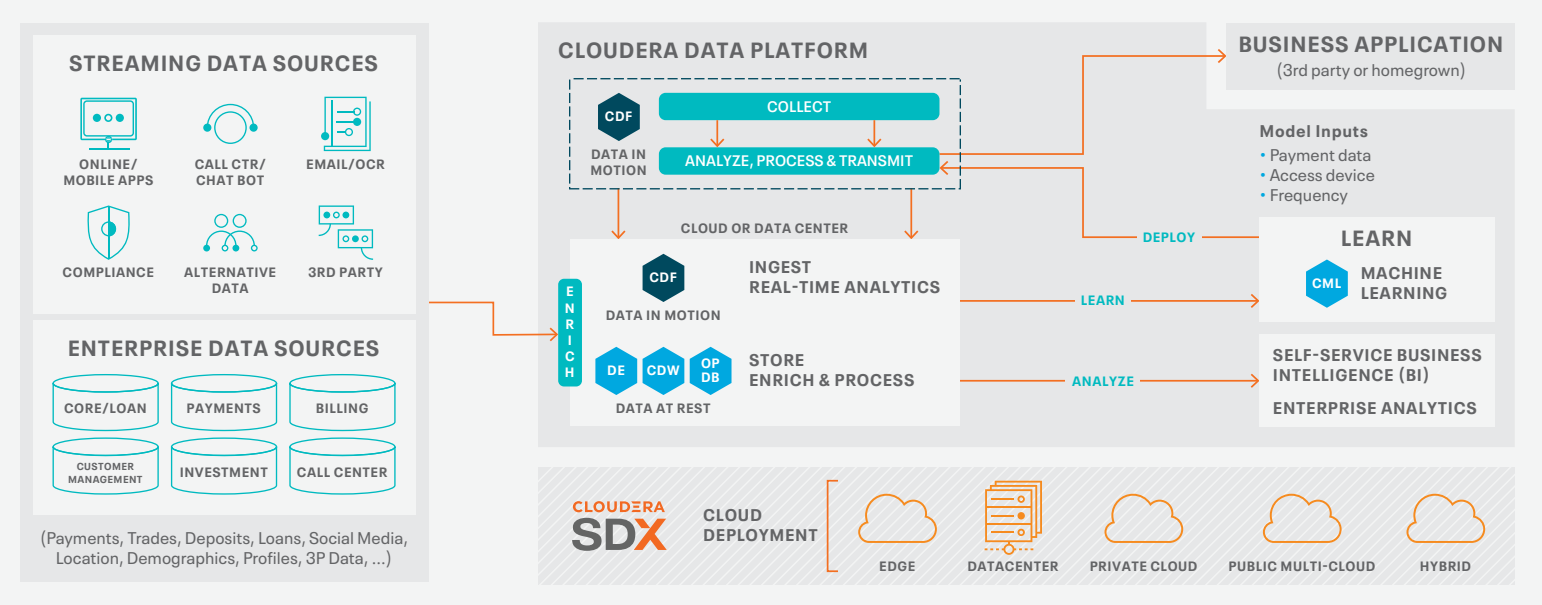
Poor data security and governance lead to reduced productivity and expose a firm to multiple risks and regulatory compliance issues. For financial crime protection to be effective, firms must have the right levels of data security and governance in place. Subject matter experts and analysts need access and appropriate permissions to analyze the data.

Data-driven Financial Crime Prevention Enabled by Cloudera

Cloudera Data Platform (CDP) is a hybrid data and analytics platform. CDP provides a suite of data services including data collection, data engineering, data warehouse, operational database and machine learning. As an enterprise data foundation, it enables data-driven business objectives such as financial crime prevention, customer experience enhancements, compliance and risk management.

Cloudera Data Platform

Enabling Financial Crime prevention with an end to end Data Lifecycle



Cloudera Data Flow (CDF) - Collect any type of data (customer channels, payment engines, credit scoring or fraud consortiums) in batch or streaming modes.

Data Engineering (DE) - Normalize raw data into a common representation for downstream application use.

Cloudera Data Warehouse (CDW) - Store all transactional data, enterprise data and related elements to create a historical reference repository, or access using APIs.

Operational Database (OPDB) - Update your proprietary applications with a modern open source database.

Cloudera Machine Learning (CML) - Build and train models, create behavioral scoring model to identify anomalies based on customer data (i.e. savings, loans, typical payments (frequency, amount, time of day), deposits, payroll). Apply network and/or graph analysis to anticipate and predict unlikely behavior.

SDX - Enable a Shared Data Experience; consistent security and governance.

Accelerate Deployment with Cloudera AMPs

Applied Machine Learning Prototypes (AMPs) are Machine Learning projects that can be deployed with one click directly from Cloudera Machine Learning (CML). AMPs enable data scientists to go from an idea to a fully working ML use case in a fraction of the time. It provides an end-to-end framework for building and deploying ML fraud detection capabilities instantly.

- Prototypes encode best practices for solving machine problems.
- Each step in the solution (e.g. data ingest, model training, model serving etc.) is declared in a yaml configuration file.
- Run examples locally or automatically deploy steps within your configuration file using Cloudera Machine Learning.

Learn more and Try the Deep Learning for Anomaly Detection AMP.

Detecting Fraud Using Deep Learning
- Watch the Webinar

Financial Crime Analytics in Action

Financial Services firms around the globe use the Cloudera Data Platform as a foundation to prevent financial crime - all with a holistic approach to financial crime prevention and protection that has data and analytics at its core.

REGIONS

The growth of digital banking has opened new doors for criminals to try innovative ways to steal from banks and their customers. Identifying fraud – at the account and transaction level – is imperative to thwarting these efforts. Regions Bank's previous big data environment was used as an operational data store with fragmented data and no centralization. Fraud detection and prevention was a critical component, but account-based fraud detection models maximized at about 5 million records, transaction data includes billions of records, so processing this volume for fraud models was a significant challenge.

To solve this challenge, Regions built an enterprise data science platform powered by Cloudera Data Platform. With advanced analytics, fraudulent transactions are more easily identified and addressed. Operationally, with fewer alerts to manage, manual interactions focus on suspicious transactions and rules are informed by the models and adjusted dynamically when new fraud schemes arise.

Read the full Regions Bank story.

95%

A production ML model for risk scoring improved fraud capture rates by **95%**, decreased false-positive alerts by **30%**, and resulted in a **50%** reduction in average daily dollar losses.

UOB 大華銀行

United Overseas Bank set up its Big Data Analytics Center to deepen the bank's data analytics capabilities and to use data insights to enhance the bank's performance.

UOB has a big data platform that gives business staff and data scientists faster access to relevant and quality data for self-service analytics, machine learning, and emerging artificial intelligence (AI) solutions. Thousands of files - from transaction, customer, trade, deposit, and loan systems – are loaded into the Cloudera platform every day.

Advanced AML detection capabilities help analysts detect suspicious transactions earlier based on hidden relationships of shell companies and high-risk individuals. With Cloudera and machine learning technologies, the bank was able to enhance AML detection and reduce the time to identify new links from three months to three weeks.

Read the full UOB story.

3 WEEKS

Enhanced AML detection and reduced time to identify new relationships from three months to **three weeks**.

Santander

Santander UK had a large number of legacy data warehouses spread across its many business units. The company found that comprehensive customer insights were impossible due to "multiple versions of the truth" resulting from inconsistent data sources and processes.

With Cloudera, Santander implemented a single data platform that supports all workloads including self-service analytics, operational analytics, and data science. As a result, the company improved the customer experience with greater personalization and relevancy drawn from more than 40 million customer records, streaming transaction data, and ten years of historical data. In addition, the company found 95 new proactive control alerts which protect 3.7 million individual customers from poor outcomes due to financial crimes.

Read the full Santander UK story.

3.7M

Protected **3.7M** customers from poor outcomes from financial crimes with **95** new proactive control alerts.

BRI developed a real-time fraud detection service, BRIForce, powered by Cloudera and Kafka, to address the rising concern around data security from regulators and consumers. BRI's data scientists developed a machine learning model for fraud detection by creating a behavioral scoring model based on customer savings, loan transactions, deposits, payroll and other financial data. BRI automated the processing of data from multiple customer touch points such as ATMs, electronic data capture, and internet banking channels enabling the identification of anomalies (which could potentially be fraudulent transactions) in real time.

Since BRIForce is a machine learning model trained with various datasets, it allows [the bank] to quickly automate the process of highlighting anomalies found in the stream of events coming from multiple customer touch points to a few seconds.

Read the full PT BRI story.

40%

Automated anomaly detection and realized a **40%** reduction in fraud.

Cloudera Data Platform for Financial Services

Battling financial crime proactively and efficiently requires a modern, flexible approach to managing customer and transactional information. Effective data management means the ability to collect, process, store, and analyze any type of data, including structured and unstructured, whether it lives at the edge, in the data center, public cloud, or a hybrid cloud. With the ability to analyze batch and streaming data, financial services organizations can use machine learning, advanced analytics, and AI technologies to identify patterns, detect anomalies, and predict potential outcomes for their business.

Cloudera Data Platform empowers financial services firms to get clear and actionable insights from complex data anywhere. It provides the flexibility to run modern analytic workloads anywhere, regardless of where the data resides. It offers the ability to move those workloads to different cloud environments—public or private—to avoid concentration and lock-in. And it has a common security and governance framework to enable data privacy and compliance.

Any Cloud

Multi-Function

Secure & Governed

Open

Learn More

Data, analytics and machine learning are critical weapons in the fight against financial crime. Visit Cloudera.com/Financial Services to learn more about how Cloudera supports Financial Services.

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 a hybrid data platform 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 | US: +1 888 789 1488 | Outside the US: +1 650 362 0488

CLOUDERA