CLOUDERA

SOLUTION BRIEF

Moving Towards the Next Gen Financial Crime Platform

"...the full force of both the public and private sectors will be employed to reduce the impact of economic crime...and bring to justice those criminals who act with impunity."
Her Majesty's Government,
"Economic Crime Plan 2019-22"

The Challenges of Evolving Crime Patterns

Synthetic identity fraud - where criminals combine real and fake information to create a new identity - is the fastest growing area of financial crime in the United States.

- Real people have long standing behaviors that aren't replicated by synthetic identities. Alternative data sources allow banks to deepen their understanding of their customers through holistic KYC.

Human trafficking Is one of the most profitable ways to generate money, which is then laundered through the banking systems.

- The victim's personal bank account is often the starting point. Behavioral signs of distress need to be considered in addition to monitoring deposit and withdrawal transactions.

The edges of financial networks are a greenfield of crime opportunities.

- Wearable and device based contactless payments can kick off a number of new crime patterns. Integrated machine learning with edge devices tightens the loop between detecting and countering new fraud patterns.

Financial Crime is Pervasive

Financial crime permeates all levels of the financial services industry because criminal networks are creative, connected, collaborative, and ready to exploit any opportunity inside or around the edges of financial business operations. They are opportunistic and do not organize their work within the neat boundaries of business functions or typical crime classifications.

In contrast, the financial services industry works best in structured environments that have clear boundaries of business functions, methods, and technologies. Rules, regulations, and the solutions that are meant to combat financial crime have created silos of specialization, including:

1. **Fraud prevention** mitigates financial losses due to fraudulent activities through account takeovers, stolen credit card data, and fake deposits.
2. **Anti-money laundering** monitors the movement of illicit funds through the financial system.
3. **Cybersecurity** protects the organization from digital intrusion and, in a world of FinTech digital transformation, is part of the financial crime paradigm.
4. **Internal surveillance** monitors employee communications and transactions to deter rogue and inappropriate behavior in order to preserve reputational integrity.

These siloed business functions are problematic for two reasons. First, they provide opportunities for criminals to sneak into the financial system and spread rapidly, and second, intelligence gaps keep us from stitching together events and behaviors that could disrupt criminal networks. As a result, the current state of combating financial crime is one of high costs, too many false positives, large losses, and little progress towards solving the problem.

- **$1.28 trillion over 12 months** is what global financial institutions have spent combating financial crime.
- **$1.45 trillion over 12 months** is the estimated revenue lost due to financial crime.
- **Only 1% of criminal proceeds are confiscated** by authorities in the European Union, despite tighter regulation and major investment[1].

[1] Revealing the True Cost of Financial Crime, Refinitive 2018

New Approaches Have Taken Shape

Regulatory and enforcement agencies understand the limitations of current anti-crime regimes in the financial sector. In response, public-private partnerships have been established to fill intelligence gaps and to encourage innovation.
Two examples:

UK Joint Money Laundering Intelligence Taskforce (JMLIT)[2]

- Public–private taskforce, sharing tactical information linked to several crime typologies.
- Provides infrastructure to link intelligence and response.

Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (December 2018)[3]

- Encourages banks to consider, evaluate, and implement innovative approaches to meet AML and other illicit financial crime obligations.
- Pilot programs that expose gaps in a compliance program will not necessarily result in supervisory action.

One Investigation Launches a Chain of Events

Regulatory and enforcement agencies have developed effective global cross jurisdictional enforcement regimes, often thanking each other in press releases that announce alleged infractions that go back a decade.

It Adds Up: A Billion Dollar Fine for Just One Bank

The table below describes enforcement actions recently taken against a large global bank.

Agency	Reason	Fines Levied
US Office of Foreign Assets Control	Violation of sanctions against multiple countries as part of a global criminal network.	$657 Million
US Federal Reserve	Poor processes in place and no disclosure of potential risks.	$164 Million
US Department of Justice	Bank fraud.	$150 Million
UK Financial Conduct Authority	Neglected to collaborate with other banks, ignoring previously reported red flags and failed to track and vet physical assets.	$129 Million
	Total for one bank	**$1.1 Billion**

Limitations of Traditional Financial Crime Platforms

Traditional financial crime platforms have a limiting effect on our capability to combat financial crime. Much of that comes from the specialization each platform has towards a specific crime type, the rigid structure of the technology employed, and the cost and complexity of retrofitting those platforms to counter new crime patterns.

We are caught in a loop of reacting to enforcement actions instead of proactively disrupting criminal networks today and anticipating the challenges of tomorrow. This is due to:

- **Siloed environments:** The specialized nature of platforms and people results in disparate data sources and data management processes. This duplicates efforts and divides the business, risk, and crime teams, limiting collaboration opportunities.
- **Dependency on historic data:** Deterministic rules based solutions flag known or old types of illicit activity. These rules are difficult to revise on the fly in order to be effective on newer, sophisticated attacks. Organizations need new analytical approaches driven by machine learning and AI to fight financial crime.
- **Events targeted but not behaviors:** Criminals and victims behave differently. Without understanding behavior, we only detect events by criminals without disrupting their networks.
- **Expensive to keep up:** It is expensive and cumbersome to update and maintain legacy, best-of-breed platforms, especially as the scale and volume of data continues to grow.
- **Inundated with false positives:** The limitations described above results in financial crime units being inundated with false positives, making it difficult, if not impossible to prioritize current and high value suspicious activities.

[2] The National Economic Crime Center

[3] Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, The Federal Reserve 2018

Don't Be Locked In

Criminal networks are pervasive in their efforts to identify and exploit business vulnerabilities.

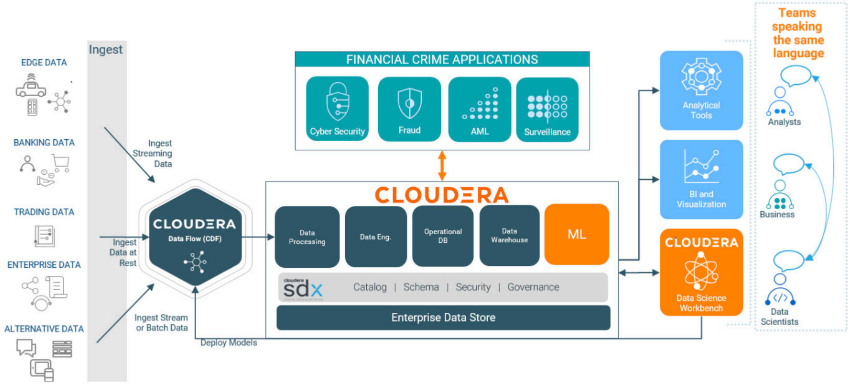
The ways and means by which they work are endless, including the ability to convince unsuspecting people to do the dirty work for them.

To keep up with the latest crime patterns and to anticipate future challenges, financial teams can't be limited to what worked yesterday and today. The next generation financial crime platform enables the following:

- Mitigate vendor lock-in by enabling third party best-of-breed platforms to share a secure common data experience.
- Support and facilitate open-source advances to ensure safe adoption and implementation of the latest technologies and methods.
- Enable choice and flexibility by offering the ability to securely manage data and analytic workloads within a hybrid environment that supports different cloud environments—public or private.

The Next Gen Financial Crime Platform

The diagram below provides a snapshot of the next generation financial crime platform, built on Cloudera.



From the left, any type of data (streaming from the edge, batch, structured, and unstructured) can be ingested and processed in real-time using Cloudera DataFlow (CDF). The Cloudera Data Hub provides a shared, scalable, data store with security, governance, and compliance built in that can be utilized by third party platforms, analysts, data scientists, and businesses. Financial services organizations can run their existing best-of-breed financial crime solutions and applications on Cloudera, by leveraging petabytes of high fidelity data across organizational boundaries. Machine learning models are developed and tested natively and deployed back to the edge using Cloudera Machine Learning.

Cloudera Data Platform (CDP)

Cloudera Data Platform (CDP) is an enterprise data platform that transcends silos by supporting shared analytics and collaboration across teams. It also enables the unification of data and security across third party fraud prevention, anti-money laundering, cybersecurity, and surveillance solutions. Attributes unique to CDP include:

- **Hybrid and multi-cloud** – provides choice to manage, analyze and experiment with data either in the data center and/or in any public or private cloud environments for maximum choice and flexibility.
- **Multi-function** – solves the most demanding business use cases – applying real-time stream processing, data warehousing, data science and iterative machine learning across shared data at scale.
- **Secure and governed** – simplifies data privacy and compliance for diverse enterprise data with a common security model and governance (powered by SDX) to control data on any on-premise, cloud – public, private - or hybrid environments.
- **Open** – facilitates the continuous innovation of the open source community, the choice of open storage and compute architectures, and the confidence and flexibility of a broad ecosystem.

New Revenue Streams with an Advanced Anti-fraud Solution

Below is an example of how Cloudera enabled one of the leading credit card providers to solve a challenge that also enabled new business opportunities.

mastercard

Challenge: The search capabilities for a fraud prevention platform did not satisfy increasingly complex customer queries on hundreds of millions of fraudulent businesses.

Solution: Delivered dynamic scalability and improved performance to accelerate searches, enrich searching capabilities and increase search accuracy.

Impact: 5x increase in annual searches and 25x more daily searches per customer are now easily supported.

Opportunity: The ease of use and dramatically improved search accuracy enable MasterCard to offer its solution to non-traditional customers such as online marketplaces.

Cloudera DataFlow (CDF)

Cloudera DataFlow (CDF) is a scalable, real-time streaming data platform that collects, curates, and analyzes data, providing immediate actionable intelligence. CDF enables organizations to:

- Ingest and process real-time data streaming at high volume and high scale;
- Drive stream processing and analytics on data-in-motion;
- Track data provenance and lineage of streaming data, and
- Manage and monitor edge applications and streaming sources.

Cloudera Data Science Workbench (CDSW)

Cloudera Data Science Workbench (CDSW) accelerates machine learning from research to production in the following ways:

- Helps accelerate data science at scale to build, test, iterate, and deploy machine learning models in production.
- Experiment faster, using R, Python, or Scala with on-demand compute and secure data access.
- Enables data scientists to push these models out to the edge to continuously monitor digital signatures from connected data sources and drive action in real-time.

Key Partner Solutions

Below is a small sample of innovative partners in the Cloudera eco-system who have implemented cutting edge financial crime solutions that utilize the power of the Cloudera platform.

Key Partners	Overview
Simudyne Fraud simulation utilizing Agent Based Model (ABM) generated synthetic transaction data.	Simulate potential fraud scenarios in a cost-effective, GDPR compliant virtual environment to significantly improve your financial crime detection systems. Simudyne identifies future fraud typologies from millions of simulations that can be used to dynamically train new machine learning algorithms for enhanced fraud identification. See: Solutions Gallery > Computational Simulation.
quantexa Connecting data, minimizing risk, empowering decisions.	Quantexa connects the dots within your data, using dynamic entity resolution and advanced network analytics to create context around your customers. This enables you to see the bigger picture and automatically assess potential criminal behavior. Watch the Cloudera financial crime webinar featuring Quantexa
accenture Transform BSA/AML operations and improve collaboration.	Provides an AML utility to participants with access to a leading stack of analytic technology. This transforms the BSA/AML operating paradigm by leveraging data science to improve program efficiency and connect the dots between key stakeholders. See: Accenture/Cloudera Alliance Overview.

Next Gen Capabilities

The next generation financial crime platform built on Cloudera enables the following:

- Unified data and analytics platform that supports shared analytics and collaboration across specialized financial crime units.
- Holistic enterprise view of all customer and financial crime related data, systems, models and processes.
- Hybrid architecture (on-prem & cloud) with support for multi-cloud environments.
- Unification of best-of-breed vendor solutions for cybersecurity, fraud, anti-money laundering, and surveillance.
- Integration with cutting edge FinTech firms that provide unique crime detection and prevention capabilities.
- Real time streaming, embedded analytics, alerts and dynamic transaction scoring.
- Industrialization of machine learning & AI to support dynamic model updating and monitoring.
- Open source advances to ensure adoption of the latest technologies and algorithms.

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

Business Innovation and Crime Fighting Goes Together

The table below provides key examples of how customers implemented pro-business and crime fighting solutions on the Cloudera platform.

Customer	Business Innovation	Crime Fighting
UOB	**Customer 360** Customer analytics insights enable relationship managers to better understand global client networks and identify new revenue opportunities.	**AML** The time needed to identify suspicious and previously hidden customer relationships was **reduced from months to weeks.**
Santander	**Personalization** Improved customer experience with greater personalization is drawn from 40+ million customer records, streaming transaction data, and 10 years of historical data.	**Fraud Prevention** 95 new proactive control alerts protect **3.7 million** individual customers from poor outcomes due to financial crime.
NYSE ICE	**Business Insights** Advanced business intelligence across the organization by incorporating new data sources and machine learning.	**Surveillance** Real-time insights improve market surveillance and confirm member compliance on 20 PB of data with **30+ TB** of fresh data added daily.

Conclusion

An effective response to financial crime goes beyond best-of-breed platforms that specialize in specific types of crime. Without change, an outdated silo mentality will continue to result in intelligence gaps that thwart effective collaboration across internal teams, global institutions, and cross-jurisdictional regulatory and enforcement agencies.

Cloudera provides the next generation financial crime platform that enables best-of-breed applications, analysts, business units, and data scientists to share a common data and analytics experience. An enterprise paradigm such as this enables financial institutions to enhance current investments with the latest machine learning and advanced analytical methods that are needed to disrupt crime and proactively mitigate risk.