

Using Data and Analytics to Fight Financial Crime and Drive Business Outcomes

Four Customer Case Studies

THE
NEXT GEN
FINANCIAL
CRIME
PLATFORM

[Table of Contents](#)

Introduction	2
Customer Case Studies	4
MasterCard Creates New Revenue With An Advanced Anti-Fraud Solution	5
Top US Bank Improves Fraud Capture Rates With An Omni-channel Approach	6
United Overseas Bank Improves AML Detection and Identifies New Revenue Opportunities	7
Bank Danamon Reduces Fraud Rates and Improves Customer Retention	8
Conclusion	9

Next Generation Capabilities to Combat Financial Crime

The next generation financial crime platform 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 ML & AI to support dynamic model updating and monitoring.
- Open source advances to ensure adoption of the latest technologies and algorithms.

Introduction

New Business and Crime Fighting Are Complementary

Over 520 financial organizations, including eight out of the Top 10 Global Banks, rely on Cludera to modernize their enterprise analytics and other big data needs. The customer success stories in this document exemplify how they have been able to leverage Cludera capabilities to **both generate revenue and mitigate risks**, specifically the risks relating to financial crime.

CLOUDERA FINANCIAL SERVICES

Prevailing in Financial Services Over 520 Customers



The Pervasiveness of Financial Crime

Criminals are pervasive in their determination to identify and exploit vulnerabilities throughout the financial services industry. Their ability to collaborate and innovate necessitates a proactive approach towards responding to individual events, while disrupting crime networks.

The approaches taken by the Cludera customers highlighted in this document show that combating financial crime is complementary to generating revenue. The big data analytical capabilities that enable a bank to personalize product offerings also underpin an effective approach to spotting and responding to criminal behavior.

The Limitations of Traditional Financial Crime Platforms

Despite tighter regulations and \$1.28 trillion dollars spent over 12 months by global financial organizations, **only 1% of criminal proceeds are confiscated*** by authorities in the European Union. It is estimated that the combined revenue lost due to financial crime is \$1.45 trillion over 12 months.

Traditional financial crime platforms limit 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. The silos each creates results in intelligence gaps that thwart effective collaboration across internal teams, global institutions, and cross-jurisdictional regulatory agencies.

* [Refinitiv - The true cost of financial crime – a global report \(2018\).](#)

Don't Be Locked In

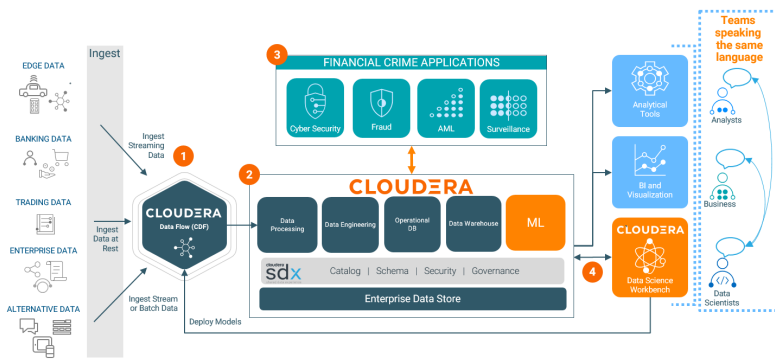
The next generation financial crime platform enables the following:

- 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 adoption of the latest technologies and methods and safely apply them into production.
- Enable flexibility with the ability to securely manage data and analytic workloads within a hybrid environment that supports multiple cloud environments—public or private.

The Next Generation Financial Crime Platform

Today, leading organizations worldwide are adopting the data management and analytics capabilities of Cludera to build the next generation financial crime platform that enables analysts, business units, and data scientists to share a common data and analytics experience while continuing to use their current specialized solutions.

The diagram below provides a snapshot of the next generation financial crime platform, built on the [Cludera Data Platform](#):



1. Any type of data (streaming from the edge, batch, structured, and unstructured) can be ingested and processed in real-time using [Cludera DataFlow \(CDF\)](#).
2. The [Cludera Data Hub](#) provides a shared, scalable, data store with built-in security, governance, and compliance that can be used by third-party platforms, analysts, data scientists, and businesses.
3. Organizations can run existing best-of-breed financial crime solutions on Cludera while leveraging petabytes of high-fidelity data across organizational boundaries.
4. Machine learning models are developed and tested natively and deployed back to the edge using [Cludera Machine Learning](#).

Customer Case Studies

The stories that follow show how premier organizations like MasterCard, United Overseas Bank, Bank Danamon, and one of the top banks in the United States is using data and analytics to fight financial crime. It also exemplifies that the work and types of data that goes into enhancing customer experience, generating revenue, and mitigating financial crime risk are interdependent and each strengthens the other.

Crime Fighting Applications

- Anti-fraud solution
- Online search

Revenue Generation Applications

- Services expanded to new customer segments.

Data Variety (structured/unstructured)

- Risk detection
- Customer 360
- Location
- Customer engagement
- Economic indicators

Data Scale

- 15 Petabytes
- 2 billion + global cards
- 160 million transactions/hour
- 220 countries
- 30 million merchants

Re-platforming the search capability on Cloudera enables MasterCard to support five times as many searches each year and 25 times more searches per customer each day.



MasterCard Creates New Revenue With An Advanced Anti-Fraud Solution

Background

MasterCard operates the world’s fastest payments processing network, delivering the products and services that make everyday commerce activities—such as shopping, traveling, running a business, and managing finances—easier, more secure, and more efficient.

Challenge

When a financial institution receives an application to form a credit processing agreement with a merchant, the organization, known as the acquirer, has to assess the merchant’s credit risk. This is challenging due to the high volume of small merchants, especially new e-commerce businesses that lack credit history. Because some fraudulent merchants alter their names, addresses, and other identifying information when going from bank to bank, they can go undetected during simple cross-reference checks.

To help acquirers better evaluate merchants, MasterCard created an anti-fraud solution using proprietary MasterCard data on a platform called MATCH that maintains data on hundreds of millions of fraudulent businesses and handles nearly one million inquiries each month.

As the volume of data in its platform grew over the years, MasterCard staff found that its homegrown relational database management system lookup solution was no longer the best option to satisfy the growing and increasingly complex needs of MATCH users.

Solution Deployed

Realizing that there was an opportunity to deliver substantially better value to its customers, MasterCard turned to the [Cloudera Enterprise Data Hub \(EDH\)](#). After successfully building, integrating, and incorporating security into its EDH, MasterCard added [Cloudera Search](#) and other tools and workloads to access, search, and secure more data than ever.

Impact

MasterCard’s work with Cloudera enabled it to gain dynamic scalability and improved performance and allowed MasterCard to accelerate searches, enrich search capabilities, and increase search accuracy of high risk merchants.

As a result, the company increased annual searches by a factor of five, and can now conduct **25 times** more searches per customer.

Ultimately, the ease of use and dramatically improved search accuracy enable MasterCard to **create new business opportunities** by offering its solution to nontraditional customers like online marketplaces.

With the latest technology in hand, and decades of experience in delivering data-driven business value, MasterCard continues to build a new generation of products and services to make smart decisions with big data.

Crime Fighting Applications

- Omnichannel fraud detection

Revenue Generation Applications

- Tens of millions of dollars realized through new revenue and cost avoidance.

Data Variety (structured/unstructured)

- Mainframe
- Legacy fraud platforms
- Transaction and market data warehouses

Data Scale

- 7 million records scored daily, comprised of tens of millions of transactions.



Top US Bank Improves Fraud Capture Rates With An Omni-channel Approach

Background

This Cludera customer is one of the United States’ largest full-service providers of consumer and commercial banking, wealth management, and mortgage products and services. It works every day to make banking easier, more convenient, and more meaningful to its customers through its reach of approximately 1,500 banking offices, 2,000 ATMs, online banking services, and a variety of digital products.

Challenge

Like most financial institutions, fraud has been on the rise as criminals take advantage of near real-time transactions and auto-adjudication across the many channels that customers use to evaluate products, receive support, and make transactions.

The challenge for this full-service provider was that legacy fraud detection platforms did not adapt quickly to evolving threats due to the reliance on deterministic rules and limited data sets. Although a team of experienced investigators would evaluate the veracity of each alert and respond accordingly, the quality of alerts did not meet the challenge, generating false positives that diminished productivity.

Solution Deployed

This Cludera customer employed Cludera’s [Enterprise Data Hub \(EDH\)](#) to provide a unified data experience across lines of business. As part of a comprehensive omni-channel approach the data science team used [Cludera Data Science Workbench \(CDSW\)](#) to develop, deploy, and schedule machine learning algorithms on the EDH data to generate precise risk scores used to **augment existing fraud detection platforms with better insights and new rules.**

As this Cludera Customer moves towards real time streaming use cases, [Cludera DataFlow \(CDF\)](#) will become increasingly important and has enabled sophisticated analytics to be embedded within business processes such as fraud operations and commercial relationship management.

Impact

Since implementation, fraud capture **rates have improved by 95%** while the total number of **alerts decreased by 30%** (decreased false positives). Average daily dollar fraud losses fell by 50% and represents tens of millions of dollars of increased revenue and cost avoidance.

Cludera EDH and CDSW has enabled this customer to effectively support a growing team of data scientists that provide products that enable cross functional data capabilities that are embedded within multiple lines of business.



Crime Fighting Applications

- Anti-money laundering

Revenue Generation Applications

- Customer analytics insights
- Sentiment analysis
- Recommendation engines
- Self-service business intelligence

Data Variety (structured/unstructured)

- Deposit
- Loan
- Customer Relationship Management
- Trading
- Text
- Voice

Data Scale

- 2PB of data from dozens of separate systems including voice and text.

Lines of Business

- Compliance
- Retail Banking
- Asset Management
- Wholesale Banking

“Our collaboration with Cloudera enabled us to be sharper in identifying patterns and linkages and to predict outcomes more accurately.”

Richard Lowe, Chief Data Officer, United Overseas Bank



United Overseas Bank Improves AML Detection and Identifies New Revenue Opportunities

Background

United Overseas Bank (UOB) is a leading full-service bank in Asia with a network of more than 500 offices in 19 countries and territories in Asia Pacific, Western Europe, and North America. UOB set up its Big Data Analytics Center in 2017, Singapore’s first centralized big data unit within a bank, to deepen the Bank’s data analytics capabilities and to use data insights to enhance the Bank’s performance.

“Our focus is on providing our customers with a frictionless banking experience and personalized services,” said Richard Lowe, Chief Data Officer at United Overseas Bank.

Challenge

The challenge UOB faced was the data limitations of their legacy systems. “With legacy databases, you’re restricted by the amount of data as well as the variety,” said Lowe. “As a result, you can miss key data attributes that are necessary for anti-money laundering (AML), transaction monitoring, and customer analytics engines to work effectively.”

Solution Deployed

Working with Cloudera, UOB established the [Enterprise Data Hub \(EDH\)](#) as the principal data platform that, every day, ingests 2 petabytes (PB) of transaction, customer, trade, deposit, and loan data and a range of unstructured data, including voice and text.

[Cloudera Data Science Workbench \(CDSW\)](#) is employed as the enterprise data science platform to develop and test machine learning models natively on EDH. This integrated approach provides business staff and data scientists faster access to relevant and quality data for self-service analytics and emerging artificial intelligence (AI) solutions.

Teams across the enterprise such as compliance, retail banking, asset management, and wholesale banking have a more comprehensive view of customer and transaction data to optimize their business processes, to design distinctive customer experiences, and to improve detection of financial crimes.

Impact

“With Cloudera and machine learning technologies, we were able to enhance AML detection and **reduce the time to identify new links from three months to three weeks.**”

Self-service analytics and machine-learning driven insights provide UOB with advanced AML detection capabilities that help analysts detect suspicious transactions earlier based on hidden relationships of shell companies and high-risk individuals.

It also enables corporate relationship managers to better understand global client networks and identify new revenue opportunities. “This project not only led to a very large uplift in leads, it also **saved relationship managers more than 1,000 hours** in manually reviewing documents.”

Crime Fighting Applications

- Real-time fraud detection
- Anti-money laundering

Revenue Generation Applications

- Real-time recommendation engine
- Business intelligence

Data Variety (structured/unstructured)

- Transactional
- Product
- Internet banking
- Mobile banking
- Credit card
- Customer care
- Voice
- Digital logs
- Social media
- Socioeconomic
- Other 3rd party/external data

Data Scale

- More than 1TB of streaming and batch data is processed daily.

"We've increased the conversion rate by more than 300 percent for our marketing campaigns, improved customer retention, and reduced the number of fraud incidents by 30 percent, all while significantly lowering costs."

Billie Setiawan, Head of Decision Management Data and Analytics, Bank Danamon Indonesia



Bank Danamon Reduces Fraud Rates and Improves Customer Retention

Background

Bank Danamon is one of Indonesia's largest financial institutions, offering corporate and small business banking, consumer banking, trade finance, cash management, treasury and capital markets.

Challenge

Around the globe, a new generation of tech-savvy customers put pressure on financial institutions to deliver innovative consumer-centric digital services. These new services represent a massive opportunity as well as a massive risk as more consumers connect to products and services digitally.

To advance digital transformation and to protect the bank and its customers from financial crime, it is necessary to gain a holistic view of customer behavior across the bank.

The challenge was that each line of business had their own data mart, so there were a lot of data silos and no efficient mechanism by which to apply machine learning algorithms across data assets.

Solution Deployed

Bank Danamon uses a machine learning platform powered by Cloudera for real-time customer marketing, fraud detection, and anti-money laundering (AML) activities. The platform integrates data from about 50 different systems and drives machine learning applications to:

1. Uncover new suspected fraud patterns and develop preventive triggers to identify fraud incidents;
2. Predict customer needs and determine in real time which offers to give each customer; and
3. Send alerts to customers in real time about potential fraud to improve customer experience and reduce customer complaints.

Impact

Bank Danamon now has the insights to interact with customers in a meaningful way. For example, staff can deliver real-time, localized, and personalized interactions to each customer at the right time, with the right content, using the right channels. The bank can also observe the performance of interactions in real time, and, based on feedback, self-correct and learn.

Using machine learning on aggregated behavior and transaction data in real time has helped Bank Danamon reduce marketing costs, identify new patterns of fraud, and deepen customer relationships. This has led to:

- **300 percent increase** in conversion rate and increased customer retention.
- **30 percent reduction** in the number of fraud incidents.
- Lowered capital expense cost per terabyte.

About Cloudera

Cloudera delivers the modern platform for machine learning and advanced analytics built on the latest open source technologies. The world's leading organizations trust Cloudera to help solve their most challenging business problems by efficiently capturing, storing, processing, and analyzing vast amounts of data.

Learn more at cloudera.com

Conclusion

With only a 1% success rate in recovering illicit funds, the financial services industry has realized that traditional approaches to dealing with financial crime are not working. Across the ecosystem, regulatory authorities, enforcement agencies, and financial institutions are working together to disrupt financial crime. This requires a proactive approach to predict and manage the risks posed to people and organizations and not merely to comply with rules and regulations.

Cloudera provides the next generation data management and analytics platform that enables best-of-breed financial crime 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 methodologies that are needed to disrupt crime and proactively mitigate risk.

An effective response to financial crime goes beyond best-of-breed platforms that specialize in specific types of crime such as fraud, AML, and cybersecurity. The customer stories in this paper show that success is derived from a holistic approach. Enhancing customer experience, generating revenue, and mitigating financial crime risk are complementary endeavors and each strengthens the other. Today, leading financial industry organizations worldwide are leveraging the Cloudera platform to use data and analytics to fight financial crime and drive positive business outcomes.

To learn more, watch our OnDemand webinar on [Moving Towards the Next Gen Financial Crime Platform](#).

Learn more about how Cloudera is transforming [Financial Services](#) today.