lynxanalytics

How A Leading Payment Company Used AI to Combat Money Laundering

As international digital payments rise, so does the risk of fraudulent transactions – including money laundering. Hence, it's crucial for payment companies to leverage the appropriate tools and tactics to comply with global financial regulations and maintain the integrity of their business.

Find out how AI helped this cross-border remittance company optimize its transaction monitoring and anti-money laundering efforts.

Cross-border transactions have blossomed into a trillion-dollar industry, with global payment flows forecasted to reach a whopping US$156 trillion in 2022. The industry's growth can be attributed to a combination of globalization, rapid digital transformation, and worldwide Covid-19 restrictions – factors that have encouraged people to turn to speedy, cost-effective, and reliable online platforms to do everything from paying for goods and services to remitting money overseas.

However, the risk of fraudulent transactions and financial crimes, such as money laundering, has also increased and poses a significant threat. Online payment providers must thus ensure that they're employing the right anti-money laundering (AML) solutions to mitigate these risks and comply with financial regulations across various jurisdictions, as money launderers devise increasingly sophisticated ways of gaming the system and evading detection.

To screen for money laundering, many companies rely on tedious manual checks and procedures to detect suspicious transfers. They may further use rigid rule-based software that flags on arbitrary or catch-all thresholds – such as transactions over a specific amount, from particular countries or within certain industries. But these methods lack the ability for targeted analysis, and often result in a high number of false positives (FPs). A more optimal solution would be using AI. Besides reducing the human effort and time needed to screen payments, AI and machine-learning models can offer real-time transaction monitoring and provide a more accurate, granular and streamlined approach that cuts down on the occurrence of FPs.

Addressing the company's challenges and pain points

Transaction monitoring typically consists of a two-step procedure. Based on this workflow, payments are initially screened at the pre-transaction stage, before any processing of funds occurs, and subsequently at the post-transaction stage, after the funds have been released by a bank or similar entity.

The client, a leading payment institution that specializes in domestic and cross-border remittance services, was keen to implement a better system for monitoring suspicious transactions.

It therefore enlisted Lynx Analytics to develop an appropriate data-centric tool that catered to its unique business needs and would help it meet its regulatory and compliance requirements.

Under the company's previous workflow, each transaction was manually screened by an officer from the Legal and Compliance (L&C) team.

This involved extracting information from multiple sources, usually with a significant degree of back-and-forth interactions, which made it a time-consuming and error-prone process.

The manual screening process also made it difficult to align decision-making procedures between different compliance officers.
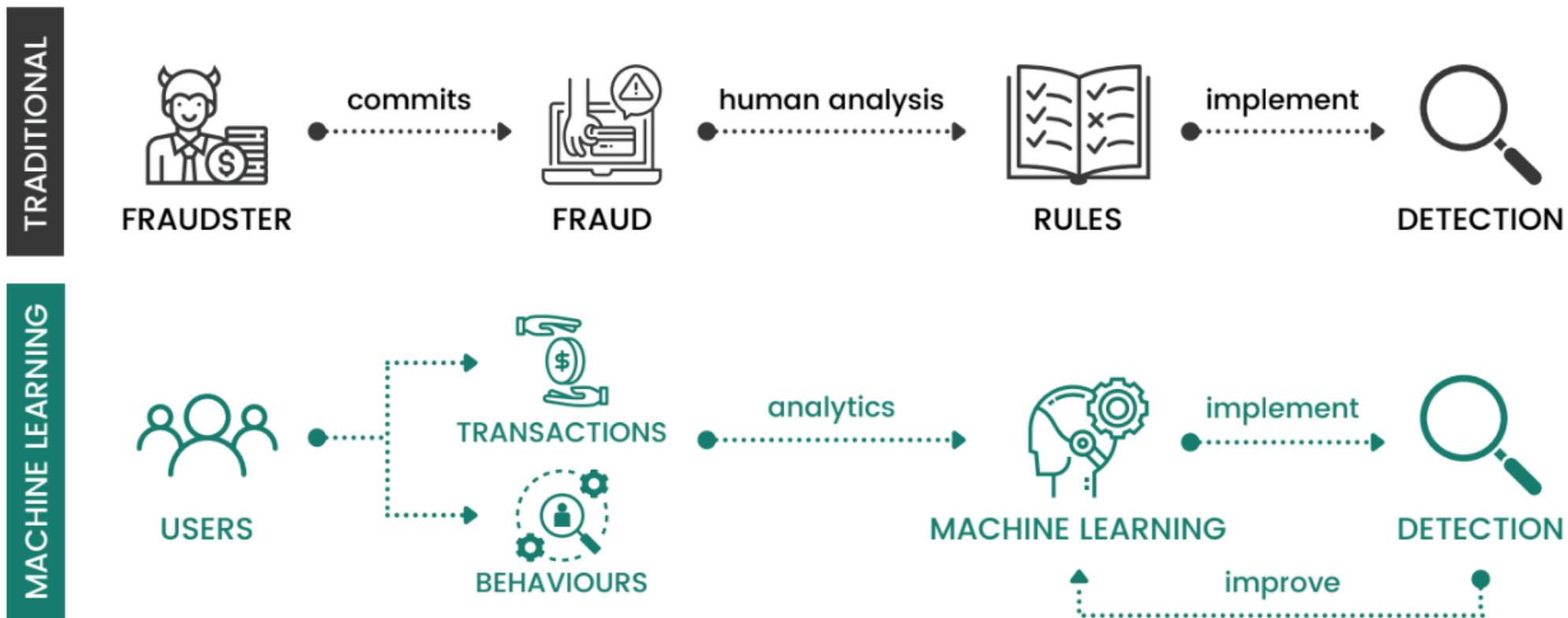
lynxanalytics

This introduced the chance that disparate standards were being applied to flag out suspicious transactions, resulting in a lack of consistency.

What's more, as the client was using fixed rule-based software to pinpoint anomalous transfers, it was encountering a high number of FPs at the post-transaction monitoring (post- TM) stage.

This led to an increased workload for the L&C team, which had to manually resolve these issues, and affected the customer experience.

Additionally, the company wanted to improve its ability to identify possible money laundering activities at the pre-transaction monitoring (pre-TM) stage, rather than leave it to the post-TM stage when these transfers would have already occurred, and it may be too late to act.

They also wanted to combine multiple systems and information sources into a single, centralized database for a broad and integrated overview of all transactions.

TRADITIONAL

FRAUDSTER → commits → FRAUD → human analysis → RULES → implement → DETECTION

MACHINE LEARNING

USERS → TRANSACTIONS / BEHAVIOURS → analytics → MACHINE LEARNING → implement → DETECTION → improve →

TRADITIONAL	VS	MACHINE LEARNING
Tries to understand fraud based on fraudster (unknown to bank)		Approach the fraud problem based on the client (very well known by bank)
One rule is created by analyzing one type of fraud, and new frauds will not be detected until they happen. Updating rules is very difficult and many false positives if rules are too generic.		Straight-to-detection. New fraud is caught automatically as fraud detection is based on transaction pattern analysis, hence it is not dependent on being first detected.
Long implementation cycle		No long implementation cycles

lynxanalytics

Improving transaction monitoring with AI

After assessing the payment provider's data and data infrastructure, Lynx Analytics developed a tool to improve their transaction monitoring and AML controls, with a focus on the pre-TM aspect.

The solution split the pre-TM process into two stages: Level 1 and Level 2.

At Level 1, Lynx Analytics' custom-built machine-learning model enabled the speedy, automated approval or denial of transfers without the need for human involvement.

Rather than base its analysis on broad categorizations and thresholds, as with many traditional rule-based solutions, the model's dynamic and flexible filtering mechanism considered a range of factors – such as an individual's or company's historical transaction data with the client and registration profile – to set thresholds.

Behavioral segmentation – as opposed to conventional demographic segmentation – was applied to group customers into clusters, thereby facilitating a more precise, granular, and contextualized screening process.

These rules were automatically generated by the tool and were manually adjustable to cater to changing business conditions and customer profiles.

Transactions that were denied at Level 1 of the pre-TM stage were then sent to Level 2 for manual review.

Here, additional supporting evidence would be collected by the company's L&C officers and used to review and potentially override decisions made in Level 1.
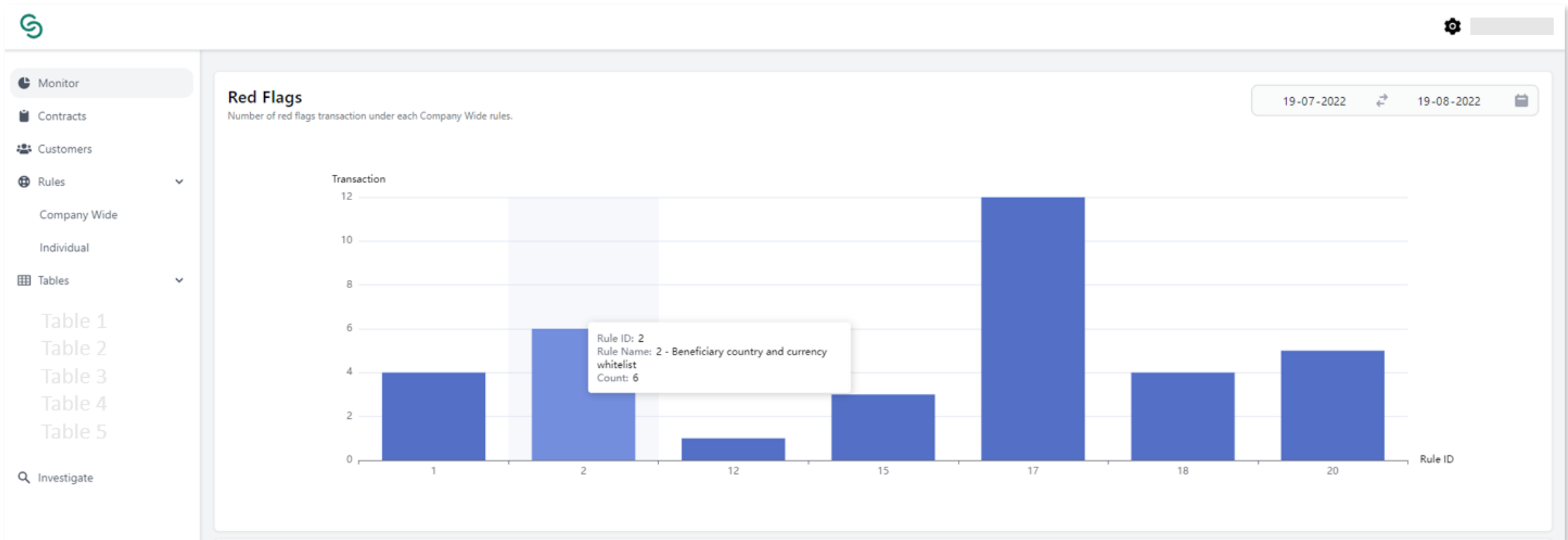
lynxanalytics

Actions taken at this stage would be used to inform and update the screening rules enacted by the model at Level 1 to further enhance its accuracy and effectiveness over time.

Lynx Analytics also created an easy-to-use API that was integrated with the company's customer portal.

This provided a centralized overview of each customer's risk profile and more information on flagged transfers; allowed the client to monitor payments in real-time and quickly look up sender, beneficiary, and transaction information; and functioned as a case management interface to review past incidents.

By reducing the manual effort involved in data collection, the client has freed up a substantial amount of valuable manpower.

This additional time saved on data consolidation can be repurposed for more high-value tasks, such as analysis and the generation of insights to be discussed at the monthly S&OP forums.

Red Flags

Number of red flags transaction under each Company Wide rules.

19-07-2022 ⇄ 19-08-2022

Rule ID: 2
Rule Name: 2 - Beneficiary country and currency whitelist
Count: 6

RULES	SPECIFICITY	OVERRIDE	EXCEPTION	ACTIVE	CREATED AT
Custom transaction limit Flag transaction if the amount of transaction exceeds transaction limit threshold of 200% of salary cap	Individual	YES	0	⬤	2022-08-19
1 - High risk beneficiary countries blacklist Flag transaction if beneficiary banking address or country address is included in Blacklist Bene Countries Table	Company	NO	0	YES	2022-08-15
2 - Beneficiary country and currency whitelist Flag transaction if beneficiary address country / bank country - remittance currency pairing is not included in Whitelist Bene Address CC / Whitelist Bene Bank CC	Company	NO	0	YES	2022-08-15

Monitor

Contracts

Customers

Rules
- Company Wide
- Individual

Tables
- Table 1
- Table 2
- Table 3
- Table 4
- Table 5

Investigate

lynxanalytics

Rule Editor for All Companies

Rule Name:

17 - Transaction limit

Rule Description:

Flag transaction if the amount of transaction exceeds transaction limit of 100% of annual turnover ✓

Rule Conditions

AND ▾ ＋

```
SELECT sum_txn_value_365d FROM customer_metrics + sgdAmt FROM payment_envelope
  >
SELECT account_limit FROM customer_metrics * 1 FROM constant
```

lynxanalytics

Benefits of Lynx Analytics' data-driven

With the help of the model devised by Lynx Analytics, the client was able to achieve greater efficiency across its transaction monitoring process.

By automating much of the pre-TM stage, the payment provider reduced the number of transactions that required manual review by 80%.

Use of the solution drastically cut down on the time spent by L&C officers to assess obvious cases, thus freeing them up to focus on suspicious transfers that truly warranted a deeper look.

As pre-TM screening was done in a speedy manner, there was also no degradation to the customer experience.

Reliability was enhanced with the standardization and consolidation of all risk and screening decisions and supporting evidence on a single platform, rather than being carried out by

various L&C officers with potentially conflicting standards. And with more efficient screening at the pre-TM stage, the client was less reliant on the post-TM stage, and could obtain greater cost savings on its existing post-TM solution.

Additionally, by leveraging machine learning to flag out anomalous transactions, Lynx Analytics' tool reduced the incidence of FPs by 80% compared to the payment provider's previous system.

This is crucial to help them meet the requirements for money changing and remittance licenses; adhere to more stringent regulatory guidelines from worldwide monetary authorities; and cope with the expected greater frequency and volume of remittances as more businesses shift to digital channels.

lynxanalytics

Applications of the tool across other sectors

Besides cross-border remittance providers, other services that are vulnerable to money laundering would stand to gain from employing such data-powered solutions.

For instance, cryptocurrency platforms can draw on it to screen conversions from cryptocurrency into fiat currency for withdrawal; while exchanges trading in stocks and commodities can harness it to better analyze and assess trades to identify anomalous transactions.

With up to an estimated US$2 trillion laundered globally each year, it's important for organizations to shore up their transaction screening systems and avoid running afoul of regulators – and to do so in an effective manner. By harnessing AI, businesses can optimize their transaction monitoring and AML efforts, which will benefit both the customer experience and their business as a whole.

lynxanalytics