CASE STUDY
CORRESPONDENT BANKING

A BANK'S WORST NIGHTMARE

In 2017 a newspaper report claimed that some large European banks had processed hundreds of millions of dollars in a money laundering scheme.

The banks performed an internal investigation and recognized that the issue stemmed from money transfers involving correspondent banking, where they lacked both visibility and control. Unable to determine the source of the money while the scheme was going on, investigators realized that the European banks continued to process transaction after transaction of "dirty" money.

Processing that money violated European anti-money laundering laws. The banks were approached by the regulators and asked to explain how they allowed such a big scheme run for years undetected. Looking for ways to assess the size of the issue and protect itself from future money laundering cases, one of the banks turned to ThetaRay for help.

The bank provided ThetaRay with all the relevant data from that time period, and asked ThetaRay to check whether or not the data contained any red flags that they should have noticed.

Before using ThetaRay, the bank's team of analysts spent six months reviewing hundreds of millions of transaction details. They identified several hundred transactions that seemed relevant, but were unable to understand the scheme.

> **Within two weeks, ThetaRay's AI** provided an on-premises analysis that revealed the underlying scheme and identified the bad actors involved in the money laundering.

ThetaRay analyzed the bank's investigative results, and ran the bank's data through its intuitive AI solution. Within two weeks, ThetaRay's AI provided an on-premises analysis that revealed the underlying scheme and identified the bad actors involved in the money laundering.

Most importantly, ThetaRay's report provided the European bank with a better understanding of the situation. They were able to use that information to manage the crisis and explain what happened to both internal and external stakeholders.

PARSING THE DATA

The money laundering scheme that had struck the European bank was sophisticated. It switched off between using a rotation scheme – moving money through a number of correspondent banks to make it look clean – and sending the money directly to European bank.

Additionally, transactions came from a number of different business accounts, in £300,000-700,000 per transaction increments, keeping it below the radar of investigators. The money launderers seemingly had avoided any activities that could flag their transactions.

ThetaRay's team used their intuitive AI engine and processed all the data, including all SWIFT messages, amounts, and geographies involved. The system quickly learned to identify which behavior was considered "normal" banking behavior. Then, it was able to look out and detect anomalies holding suspicious activity related to money-laundering. These were handed over to an investigator through ThetaRay's Investigation Center for a closer look.

> **ThetaRay's intuitive AI** engine can identify previously unknown patterns of suspicious activity.

THE THETARAY ADVANTAGE

Using multiple algorithms, ThetaRay processes data from a number of different perspectives to create a multi-dimension analysis. It doesn't simply identify and flag high-risk countries or transactions. It is capable of looking deeper into the data, allowing it to connect the dots in a large dataset, understand the transactions that took place, and provide a coherent unified report that outlines the suspicious activity for an investigator.

This system provided the bank's investigative teams with two advantages. First, while most data processers can only identify something that it's looking for, ThetaRay's intuitive AI engine can identify previously unknown patterns of suspicious activity. This ability enhances the system's effectiveness, especially while protecting the bank from previously unseen financial crime typologies.

Second, most anti-money laundering software follow user-generated rules to flag high-risk transactions. This technique provides coverage for limited, almost binary dimensionality of the data and activity, to indicate whether or not the transaction(s) is/are suspicious. This results in a high number of false positives, leading investigators to look at every transaction that emanated from a pre-defined high-risk scenario, even though most transactions are legitimate. This is bad all-around; it is advantageous to bad actors - who know how to bypass the rules, and it ensures that investigators are consumed with redundant work.. In contrast, ThetaRay doesn't use user-directed rules while scanning data. ThetaRay looks for anomalies of suspicious activities and behaviors rather than specific transactions, which significantly limits the number of false positives. The regulatory expectation is that unusual cases are detected and investigated, but rules-based systems do not address this.

DELIVERING VALUE TO THE EUROPEAN BANK

When money laundering accusations appear, banks with sterling reputations lose their luster, and when investigations reveal weak AML processes and tools in place, the cost to a bank's reputations can be irreparable. Banks realize that the old way does not work and therefore are looking to harness the power of AI.

ThetaRay provides banks with the strongest, most powerful line of defense against money laundering and other financial crimes. ThetaRay's solution allows banks to use fewer investigative resources while improving their ability to track illicit transfers and protect themselves from long-running money laundering schemes. ThetaRay's system can quickly and effectively identify unseen financial improprieties, provide early detection for money-laundering suspicious activities as they occur, and produce a manageable alert rate that helps banks mitigate risk and stay within their operational budget.

> It identified and alerted **8,400 suspicious anomalies** related to 56 customers during the time period under investigation.

THETARAY'S RESULTS

ThetaRay's AI-led system scanned through all the data of more than 200 million transactions provided by the European bank. ThetaRay identified and alerted 8,400 suspicious anomalies related to 56 customers during the time period under investigation. It recognized that the bad actors were using 9 different schemes for slightly different circumstances, enabling them send money between one originating account to a specific destination account. In total, each generating account sent 56 transactions per month using this bank alone. The bad actors, however, were using the same scheme to target several European banks.

ThetaRay provided the results to the European bank, which then delivered Suspicious Activity Reports (SAR) to the Financial Intelligence Unit (FIU).