Financial and Economic Crime: Challenges and Best Practices

Financial and economic crime is evolving faster than ever, posing complex challenges for banks worldwide. Illegal activities carried out by individuals or organisations for financial gain, typically involving deception, abuse of trust or misuse of financial systems. Examples include money laundering, terrorist financing, fraud, corruption, tax evasion, bribery and the misuse of corporate structures or financial products to conceal illicit funds. These crimes undermine the integrity of the financial system, distort markets and pose serious risks.

Banks carry an essential responsibility: acting as gatekeepers of the financial system and protecting society from money laundering and the financing of terrorism. Achieving this requires a careful, multidisciplinary approach that combines technology, regulatory compliance, cooperation and human expertise. Three of our consultants have been working within this department for a large Dutch bank to be part of the gatekeeper role.

How do banks comply with regulations?

In the Netherlands, banks must comply with the Wwft (*Wet ter voorkoming van witwassen en financieren van terrorisme*), the law aimed at preventing money laundering and terrorist financing. It requires banks to understand who their customers are, where their funds come from and how they intend to use financial services. KYC (Know Your Customer) is a core part of Wwft. It helps banks ensure they only serve legitimate customers and detect unusual or suspicious activity through identity verification, risk assessments and ongoing monitoring. Supervision is carried out by regulatory banks such as De Nederlandsche Bank (DNB) in the Netherlands. Compliance is critical for banks, as non-compliance has led to hundreds of millions of euros in fines between 2018 and 2021 for the large Dutch banks.

What makes detecting financial crime so difficult?

The difficulty in detecting financial crime lies not only in the enormous volume of daily transactions but also in identifying patterns within this data that may signal suspicious behaviour. Context is also crucial. Consider a customer depositing €10,000 in cash in a single month. For a wealthy entrepreneur with a profitable company, such liquidity may be completely normal. However, for an individual with a monthly income of €2,000, this deposit may raise questions about the source of funds. Hence, the real challenge lies in determining whether these activities are genuinely fraudulent or simply explainable and legitimate based on the customer's profile and circumstances. This critical task falls to the bank's analysts, who must apply their expertise and judgement to interpret these patterns, something automated systems alone cannot fully achieve. Moreover, criminals continually adapt their methods, requiring banks to update detection strategies to stay ahead of evolving schemes.

How is AI going to help?

Banks are investing more heavily in AI to enhance operational efficiency and achieve greater cost effectiveness. AI systems can automate documentation, generate structured reports, standardise formats and provide clear overviews of relevant information. Human analysts,

however, remain essential for assessing potential fraudulent cases. They are trained to recognize complex patterns through experience, shared expertise and continuous development programs. By taking over time-consuming administrative tasks, AI allows analysts to focus on the nuanced judgement calls that machines cannot make. As a result, the time required to complete each case is reduced, fewer analysts are needed to handle the same workload and the overall process becomes more efficient.

How do we stay effective without building up a backlog?
This is precisely the purpose of the Capacity Management team, in which two of our colleagues are actively involved. The team's objective is to ensure that the right person is in the right place at the right time to manage the workload effectively. To achieve this, the team develops data-driven insights into the inflow of potential fraudulent cases and produces forecasts to anticipate future demand. At the same time, they analyse the available FTE within the analyst workforce. By combining these insights, the team can determine whether the department is likely to face overstaffing or understaffing. This enables proactive planning and performance management that facilitates efficient resource allocation.

Can banks collaborate effectively with law enforcement?
Yes. Banks report suspicious transactions when there is enough evidence of financial and economic crime. One example is through MOT reports (*Melding Ongebruikelijke Transacties*) to the FIOD (*Fiscale Inlichtingen en OpsporingsDienst*), which provide law enforcement with crucial information. Law enforcement can also share guidance, typologies, and red-flag indicators to help banks improve detection and compliance. All information is exchanged within legal limits to ensure confidentiality and compliance with regulations like AVG (*Algemene Verordening Gegevensbescherming*). When collaboration is well-organized with clear communication, specialised compliance teams and proper escalation procedures, it becomes highly effective. Together, banks and law enforcement can prevent criminal activity and identify networks more efficiently.

To Summarize
Detecting financial and economic crime is a complex, ongoing challenge that requires expert human analysis, technology, and strict compliance with regulations such as the Wwft. AI and automated systems help streamline processes and handle administrative tasks. However, human judgement remains essential to identify suspicious activities. Supervision by regulatory bodies like DNB ensures banks maintain compliance and integrity. Collaboration with law enforcement, for example through MOT reports to the FIOD, strengthens banks' ability to prevent crime and detect illicit networks. Data-driven insights, forecasting, and capacity management, help allocate people to manage workloads efficiently. Together, these measures enable banks to respond effectively and proactively to financial crime.

If you have any questions or would like to learn more about how we can assist with detecting financial and economic crime, feel free to contact us!