

THE TECHNOLOGICAL REVOLUTION: WHAT DOES IT HOLD FOR THE FIGHT AGAINST FRAUD?

The protection of assets, especially against theft or misappropriation, has long been a major issue for companies. Anti-fraud measures are based on three main pillars: prevention, detection and response. These traditional approaches are now facing a number of developments, something that also offers unprecedented opportunities that companies must seize.

Experiences and experiments in the banking sector, which is at the forefront on these issues, offer a view of future prospects and therefore provide a lens through which other sectors can be analysed.

THREATS, USE CASES, AND REGULATIONS: THREE MAJOR DEVELOPMENTS THAT MEAN ANTI-FRAUD APPROACHES NEED TO ADAPT

The business and technological transformations taking place in all sectors have generated changes that directly impact traditional anti-fraud approaches.

The threats are evolving and **anti-fraud practices have become increasingly professionalised**—adopting new tools and practices. Take phishing, for example: even without specialist IT skills, a trained fraud cell can now buy a ready-to-use phishing kit and take, on average, just three minutes between making a fraudulent connection and successfully withdrawing money. As a result, **attempts to commit fraud have increased significantly** in recent years.

CONTACTS



Martin DESCAZEUX
martin.descazeaux@wavestone.com



Mathieu COUTURIER
mathieu.couturier@wavestone.com

At the same time, use cases are evolving toward **greater digitalisation**, at times driven directly by **regulatory changes** aimed at both customers and employees. For example, Instant Payment deployment in Europe (like the Faster Payment System in the UK) and the second European Payment Services Directive (PSD2) now make provisions for instant transfers. These new use cases accelerate financial transactions between players, which, at the same time, leads to a **need for an instant risk assessment** for fraud. In addition, the ever-increasing number of payment channels results in an **increase in the attack surface**, including the diversification of banking malware to mobile applications, as well as the emergence of complex **multichannel** social engineering practices, which draw on a detailed understanding of the business processes involved.

The diversification of fraud, the associated rise in volumes, and a greater need for instant transfers, makes manual anti-fraud control processing virtually impossible. Even creating more restrictive rules for alerts to minimise volumes, would still run the risk of missing a great deal of fraudulent activity.

In this new landscape, where fraud is becoming ever-more technologically advanced and has a multitude of origins (customers, contractors, subcontractors, suppliers, and administrators), detection strategies must evolve. It must move from the reactive detection of known fraud to the proactive detection of unknown threats.

NEW TECHNOLOGIES: THE FUTURE OF ANTI-FRAUD MEASURES TO COPE WITH THESE NEW REALITIES

The traditional approach to fraud detection is based primarily on the definition of unit rules that generate an alert when non-compliance with one of the criteria and a correlation of events occurs. This consists of implementing ever-more advanced business rules that take into account several sources of data to generate an alert when there are indications that a known fraud scenario is unfolding.

While this approach is still effective in detecting known frauds—for example, the fight against phishing—it's no longer good enough to cope with recent developments. An enhanced, hybrid approach

The number of variables manipulated by algorithms can easily exceed fifty, whereas static rules struggle to integrate a dozen parameters

is needed, one that harnesses the new technologies on the market (artificial intelligence/machine learning, behavioral biometrics, etc.). These technologies offer two major ways to strengthen current approaches.





1 - Moving from mass detection to much more granular, individualised detection that focuses on behavioral changes.

Machine learning offers the option of creating individual profiles for each customer. These profiles are made up of variables developed from the data collected that enable behavior to be modeled. Here, the algorithms used compare the profile of a customer (and therefore their habits) with a given event, and, by doing so, signal an anomaly if a mismatch occurs. In this approach, it's quite typical for several dozens of variables to be manipulated, in comparison to static rules, which can only integrate a handful of parameters. This is an advantage that enables detection potential to be increased and the number of false positives to be reduced.

2 - Increasing the scope of coverage by taking advantage of the economies of scale that these technologies offer (the pooling of big data infrastructures, big data analytics and automation which saves time for analysts, etc.).

By using data lakes, these technologies have the capacity to integrate and correlate large volumes of raw data, both technical and commercial (application logs, knowledge of customers, financial transactions, etc.). They also offer the potential to enrich them with additional external data (watch lists, the conversion of IP addresses into physical locations, etc.). To maximise the benefit from an anti-fraud system, a data lake must be able to draw on an archive of relevant data, processed in compliance with laws

The main detection methods

Known patterns	
 <p>Unit detection</p> <ul style="list-style-type: none"> • Detection of characteristic elements (IBAN, IP, etc.) • Integration of external sources (blacklist, etc.) 	 <p>Correlation of events</p> <ul style="list-style-type: none"> • Detection of known fraud scenarios • Based on actions and/or context
Known and unknown patterns Behavioral analysis	
 <p>Machine Learning</p> <ul style="list-style-type: none"> • Analysis of an action that deviates from the customer's habits • Self-learning model to integrate feedback from investigators 	 <p>Behavioral biometry</p> <ul style="list-style-type: none"> • Analysis of the interaction of customers with their terminals (mouse movements, typing, etc.)

and regulations; to be precise, 13 months of data for individuals and six months for companies or other entities.

These technologies can't then just "magically" provide results: they must have both the right quality and quantity of data to carry out the essential preparatory work on the construction of the variables, which, in turn, underpin the algorithms' detection capacities. This construction phase requires the contribution of both business and technological expertise (data science, developers, etc.).

The choice of algorithms is important too, especially from the perspective of transparency. In fact, some tools are based on algorithms whose results are difficult to justify. The lack of visibility on the criteria used to establish results causes alerts to be generated in "black-box" fashion, meaning that the blocking actions affecting customers are not always justifiable. When such alerts have direct consequences for customers, it can result in legal implications or may even be illegal.

DILEMMAS IN THE DEVELOPMENT OF ANTI-FRAUD APPROACHES: WHAT ARE THE LEVERS THAT CAN INTEGRATE THESE TECHNOLOGIES?

Given the particularities of each company, and the investments already made in big data infrastructures and machine learning



THE NEW OBJECTIVE TO BE REACHED: A SEAMLESS APPROACH THAT ENCOMPASSES BOTH TECHNOLOGY AND BUSINESS FUNCTIONS

Faced with these new challenges, and the contribution emerging technologies can make, there is now a need to define a new anti-fraud strategy.

The establishment of a **sound global detection system will need to be based on five key principles.**

- / Efficiency and automation: Multi-criteria detection (using rules engines and machine learning), as well as optimised operational efficiency through the automation of actions that range from increasing in the level of authentication requested to the freezing of transfers.
- / Scalability and omnichannel operation: Integrate several areas of detection, taking a seamless approach between the cyber and non-cyber worlds. It will be designed to allow the integration of new data when it becomes available (for example, data from behavioural biometrics).
- / Visibility and exploitability: Provide visibility (through reporting) and be able to explain detection results to anti-fraud teams, customers and also to regulators.
- / Compliance and security: Comply with requirements for detection methods and regulations (such as the GDPR), as well as addressing the inherent risks of using machine learning (attempts at poisoning, the understanding of the model by an attacker, etc.).
- / Cross-functional governance covering cybersecurity and business functions: Enable close collaboration between the cyber threat detection and anti-fraud teams, breaking down silos that are still all too common. This will allow for a coordinated response with a 360° view of threats that makes the best use of available data.

To benefit from all the advantages offered by this new detection strategy, it will also be important to carefully consider the associated investigation and response systems.

Partially decentralising anti-fraud activities and involving banking advisers will

enable increased investigation capacity. They are an asset in the investigation process, as they have an in-depth knowledge of their customers.

In addition, behavioural biometrics and machine learning will enable better visibility on the level of trust that can be granted to a user. Once this degree of trust has been defined, the authentication levels requested can be adapted accordingly. The tailored and progressive involvement of users will thus reduce the number of alerts raised.

The establishment of a new approach to tackling fraud isn't just about putting in place a response to a changing backdrop, it's also about anticipating the tidal wave of change that has already begun. The detection of fraud will become more and more complex in the future as a result of the continued acceleration of digitalisation—especially in terms of payment methods. The emergence of new players, such as the fintechs and the growing disintermediation of banks, will lead to a degradation of available data. Therefore, anti-fraud approaches are destined to evolve fundamentally, if they are to maintain and develop their effectiveness.

WAVESTONE

www.wavestone.com

In a world where successful transformation is the key to success, Wavestone aims to offer its clients unique responses that will clarify and guide their most strategic decisions. Wavestone's network consists of 2,800 professionals across four continents. It is one of Europe's leading independent consultancies, and France's number one independent consulting firm.