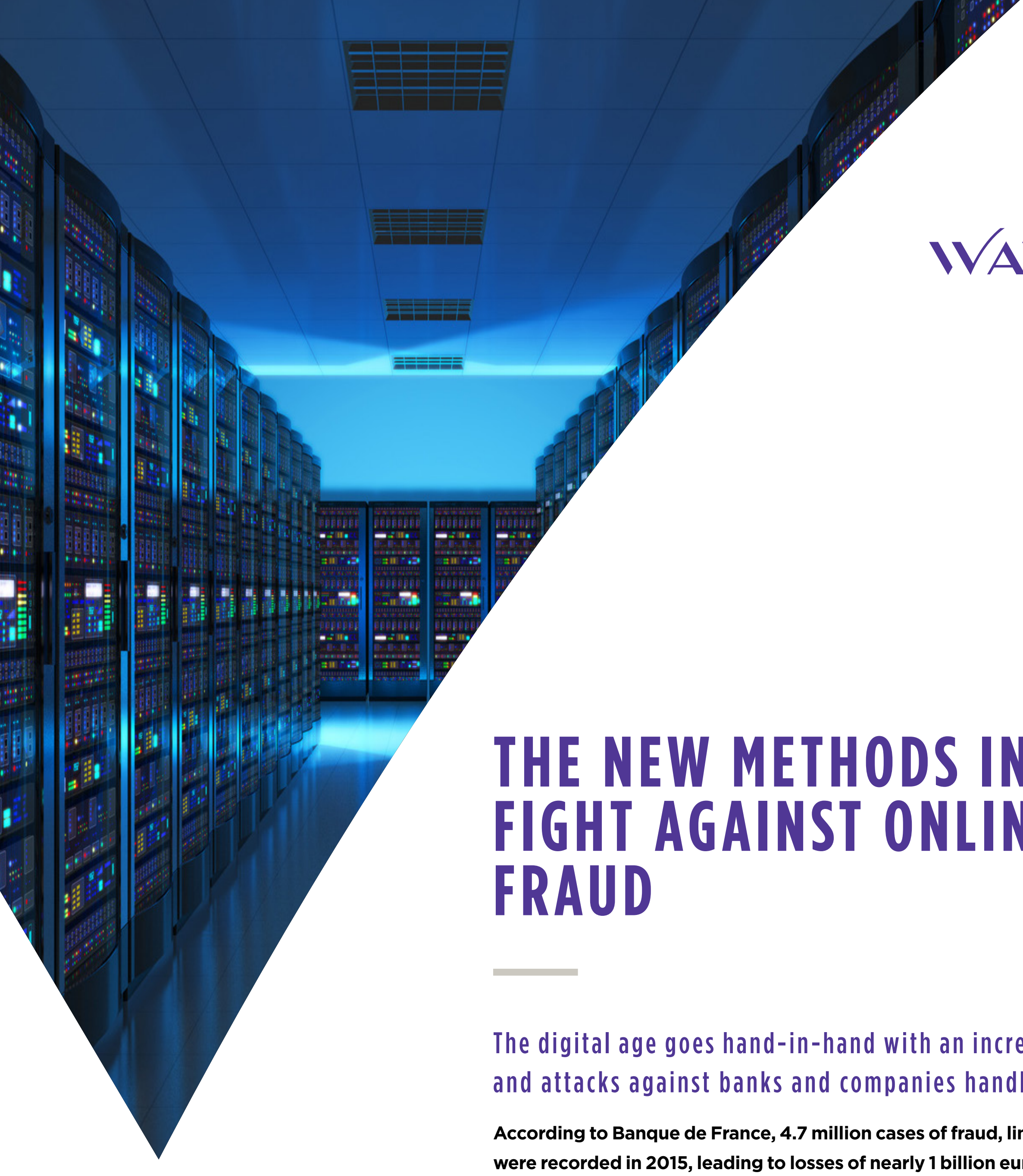


THE NEW METHODS IN THE FIGHT AGAINST ONLINE BANK FRAUD

The digital age goes hand-in-hand with an increasing number of crimes and attacks against banks and companies handling banking data.

According to Banque de France, 4.7 million cases of fraud, linked to payment transactions, were recorded in 2015, leading to losses of nearly 1 billion euros. At the end of 2016, British bank Tesco Bank was the victim of a cyberattack which affected 40,000 of its customers' accounts. A post-analysis of the attack has shown that there was fraudulent movements on 9,000 accounts, leading to the online transaction system being frozen for 48 hours and refunds being issued to all affected customers.

It is clear that inadequate management of the risks of fraudulent activity can have extremely damaging consequences: **financial impacts** of undetected fraudulent transactions, **impacts on image, customer confidence, and operations** (fraud management unit, crisis management, etc.). Like fraudulent modes of operation, anti-fraud measures must continually evolve, in order to increase effectiveness without affecting customer experience.

THREE MAIN THREADS IN THE FIGHT AGAINST FRAUD

To reduce fraud, there are three major threads to be pursued:

/ **The protection of the customer journey,** in order to ensure secure processing of sensitive financial operations through the putting in place of protective measures and the development of customer awareness;

/ **Fraud detection,** whose objectives are to detect both past and ongoing fraud;

/ **Fraud response,** in order to alert, investigate, and respond quickly in the event of fraud, following the alerts raised by detection systems.

AUTHORS

MARTIN DESCAZEAUX
martin.descazeaux@wavestone.com

MATHIEU COUTURIER
mathieu.couturier@wavestone.com

YASMINE EL HIMDI
yasmine.el-himdi@wavestone.com

INTERVIEW

FRÉDÉRIC GERMAIN (SOCIETE GENERALE)

The traditional approach to the protection of the customer journey is based on multiple solutions such as **authentication** (single or two-factor) which provides a first layer of essential security. The use of two-factor stage authentication is being expanded as it offers a much greater guarantee of security than other types of authentication, particularly for payments and sensitive online bank transactions.

However, while authentication is often the first level of security to be experienced by clients, it is also the first one to be attacked or bypassed. Additional means of protection do exist (such as making fewer options available to customers, time delays in effecting operations, and so on) but these place limits on the customer experience, working against the concept of a simple and rapid customer journey, which is what these companies are seeking.

Therefore, as the degree of protection is quite limited in many cases, businesses have started to invest in systems which are **better able to detect and respond rapidly to fraud**, while continuing to offer a satisfying customer experience. This approach must also comply with regulatory guidelines which, today, require that financial institutions go further than mere authentication, by being capable of detecting suspicious or fraudulent events in real time.

TRENDS IN ONLINE FRAUD DETECTION

From traditional approach to machine learning

The traditional approach to fraud detection, which is still the most common today, relies on the **detection of fraud patterns which have already been identified in the past**. This approach is mainly based on the application of pre-defined rules to the transactional flows:

/ **Unit-based detection,** which consists of defining a business rule where a failure against a criterion can generate an alert (for example, an electronic transfer to an IBAN that is under surveillance);

/ **Event correlation,** which consists of implementing more advanced business rules correlating multiple types of data (for example, the completion of a transaction from a country under surveillance, and the breaching of a cumulative threshold, over a 24-hour period). The definition of these rules is mainly based on the history of previous frauds.

In some cases, when the threat level is not very high and the risk of a sophisticated fraud is low, **these solutions may be sufficient**, and have **proven to be effective** in the case of conventional fraud.

However, given the complexity and diversity of attacks, detection strategies are evolving toward deeper customer knowledge. This use of data has given **rise to new, innovative approaches** based on algorithms and analytical technologies, where large volumes of data can be rapidly generated and processed. These technologies can detect previously known fraud patterns, but can also respond proactively when faced with potentially fraudulent situations that have not been identified previously.

Proactive detection through machine learning

Machine learning makes use of algorithms that can **learn from examples**. This learning is achieved via a statistical model based on correlations developed from representative samples of data. These algorithms are developed in versions that vary in nature and complexity by using the latest advanced techniques, including artificial neural networks. As a result, human supervision, while still necessary, becomes less intensive.

The design and use of a machine learning algorithm involves three stages:

/ **Data collection and analysis**: this data can either be **internal** (technical connection data, behavioral data, corporate data, etc.) and come via one or more channels; or it can be **external** (data collected from social networks, informational websites, business partners, financial institutions, etc.).

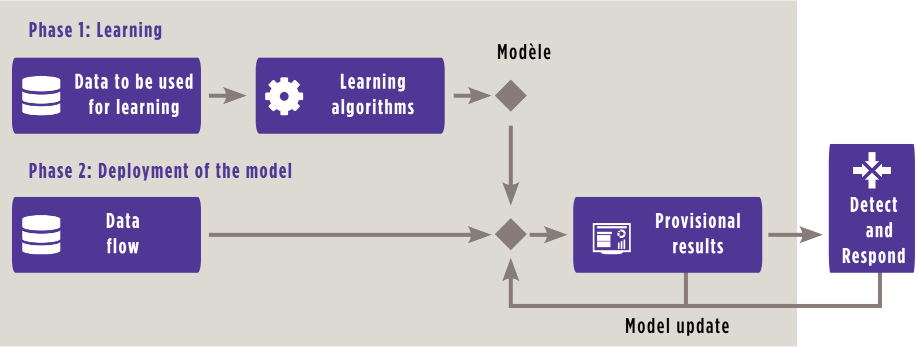
/ **Learning**: when learning, the mathematical model uses the collected data (to a greater or lesser extent under its own initiative) to make statistical comparisons, establish the rules for decision-making and the specific settings required to improve the precision of the level of detection. In practical terms, this learning process often involves the creation of customer profiles. As well as there being a wealth of data on offer, machine learning solutions do not require an absolutely reliable or comprehensive database; instead they operate using statistical principles, which means that an error or a one-off gap will have no significant impact on the results of the learning. However, for very specific applications, where data is less readily available, representative data becomes essential if machine-learning algorithms are to make accurate

/ **The prediction**: The prediction is the final operational phase of self-developed intelligence. Incoming data is exploited in real time by the model previously developed, and the target to be predicted; in the context of the fight against fraud, this is often in the form of a risk score: 0 if the transaction is safe; 100 if it is definitely a fraud.

> Detect and response rapidly to fraud while continuing to offer a satisfying customer experience

To illustrate these concepts, machine learning in the context of online banking often amounts to **create customer profiles based on historical information collected during online banking** (terminals used, usual time and place of connection, connection and activity journeys, etc.) then **predicte the degree of fraudulence of the current operation**, by comparing the current behavior of the customer with their profile.

Machine-learning approach



The fraud detection market

Whether in France or internationally, **the market for fraud detection within the online payments arena** - the first to be affected by such fraud - **is mature**. Many innovative solutions are being employed in this area, particularly those based on behavioral analysis and machine learning techniques.

Meanwhile, the broader area of **online banking is still moving toward maturity**. More and more approaches are emerging and, as a result, more and more market players have started to position themselves in the market.

Overall, the market comprises:

/ Players who integrate a behavioral analysis aspect into an existing authentication solution;

/ Tools to be installed onto client terminals;

/ Rule engines that can be integrated directly into transactional sites;

/ SIEM solutions (event correlation) designed for fraud detection;

/ Machine learning solutions.

Some players offer solutions combining several of these aspects. However, these solutions are often specialized according to area, such as payment, online banking, branch transactions, and so on. There are **few overarching solutions that can collect and analyze data originating from these different areas**, and, therefore, offer an overall strategy for the fight against fraud.

Regulatory and ethical framework

The algorithms based on machine learning have significantly higher performance results in fraud detection when they are fed by large volumes of relevant data and information, mainly of a personal nature. Against this backdrop, several concepts are being discussed in the context of French data protection legislation (LIL) and the EU's General Data Protection Regulation (GDPR), **to limit the use of personal data and artificial intelligence**. It should be noted that biometric data (keystrokes, mouse movements, etc.) is considered to be personal data, but its use in the specific area of fraud prevention and detection is still a matter of debate.

Moreover, from an ethical point of view, what would be the reaction of a customer who learned that his bank had built up a detailed profile of their behavior and internet usage, without any prior discussion or consent?

Therefore, the nature of the data handled by machine learning algorithms requires a high level of vigilance and transparency in order to guarantee that data remains confidential, meets regulations, and that there is no risk to corporate or brand reputation.

ALERTS AND COUNTERMEASURES

The implementation of automated fraud detection tools requires analysis of the feedback from any associated alerts and countermeasures. The challenge for companies is twofold: first, to **react quickly** when faced with a suspicion of fraud, and, second, **to be able to block the fraudulent transaction before it becomes effective**.

Automation of counter-measures

The automation of countermeasures allows instant action to be taken against suspected fraud, but it also **risks irritating customers if it is done in error**. Current solutions, even those based on «simple» rules or on machine-learning algorithms may generate a significant number of false positives, and, hence, errors. Therefore, the **degree of confidence** in the detection systems is the **main criterion when considering automation**.

Target architecture

Some detection solutions offer an **alert management functionnalities**, but they are often limited and an additional module is typically required. The additional module can be put in place by:

/ Using a solution available on the market, particularly incident-management or alert-investigation solutions;

/ Using existing in-house solutions, in particular notification and communication management solutions;

/ Developing an in-house solution based on existing components.

Furthermore, the integration of automatic countermeasures may result in some **major architectural changes** within the company's information system (the blocking or cancellation of operations, strong authentication being required to complete operations, etc.). These impacts must be identified at the outset of the projects.

Adaptation of business processes

Beyond the identification of the areas that must be included within the management of alerts and responses, it is essential to **work in partnership with the relevant business functions** and **help them move toward a more automated model**. It will also be necessary to identify where the alert stops within the company: With the analyst teams? With advisors? Directly with the customers?

The challenges faced by institutions manipulating banking data to prevent fraud have a significant impact on customer confidence and on the battle to reduce losses. Real-time analysis of customer data by machine learning-based tools may be the perfect recipe for proactive detection of fraud, without neglecting the importance of the response that will ultimately block fraudulent transactions. The arrival of new payment methods, such as instant payment, reinforces the need for real-time detection and automated response, while respecting the regulatory framework which increasingly governs these practices.

INTERVIEW: FRÉDÉRIC GERMAIN

PROGRAM DIRECTOR OF IS SECURITY FOR SOCIETE GENERALE RETAIL BANKING

What are the threats which must be confronted in the fight against fraud today?

For several years now, the information systems of banks have increasingly opened up to customers and the outside world, leaving them exposed and vulnerable to increasingly diverse and serious threats. This ranges from phishing to identity theft, from a «simple» password theft to social engineering and massive theft of sensitive information.

This threat context strongly encourages us to strengthen our capabilities in fraud protection and detection and add value to the client through the innovative solution of machine learning.

Why use machine learning to combat these threats?

To respond to increasingly sophisticated threats, we want to use machine learning to shift from a reactive approach of detecting known frauds to a proactive approach of detecting unknown frauds. Ultimately, we also foresee the use of behavioural biometrics.

This is why the Retail Banking IS Security Program, launched by Societe Generale in 2015, as well as strengthened information leakage prevention measures, have enabled the implementation of innovative devices capable of self-learning and detecting «fraudulent» events before any negative impact reaches the bank and its customers.

What have been the main difficulties with detection and alerting projects?

Beyond the challenges of technical development and project methodology posed by these relatively new technologies, one of the key success factors will depend on providing and connecting large sets of data hosted within a Big Data platform.

In order to combat fraud, the objective is to be able to build a profile of our customers' habits and to estimate, in real time, the level of risk associated with each navigation activity and transaction in full compliance with CNIL[1] regulation.

The impact of such "difficulties" has been eased thanks in particular to close collaboration with teams in charge of the Big Data and customer departments.

Another key success factor depends on the adoption of a «new» recruitment policy geared towards quickly locating and attracting the profiles of Data Scientists (currently still an uncommon job occupation) and highlighting the value that Data Scientists can provide.

What are your challenges for 2017/2018?

Our main challenges for 2017/2018 will be to extend the scope of our work to all client markets. This is in order to meet the needs of our various marketing and sales departments and to strengthen the capability of our machine learning solutions, whilst also remaining attentive to the maturity of market solutions and how such solutions could meet our expectations.

[1] The Commission nationale de l'informatique et des libertés (CNIL) is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data.

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France)

Wavestone's mission is to enlighten and guide their clients in the most critical decisions, drawing on functional, sectoral and technological expertise.