Think before you print!

Anti-Financial Crime: Looking Beyond Staffing

VISMA

Defining a Future-Proof Strategy for Anti-Financial Crime: Looking Beyond Staffing

The world of financial crime is murky and moves at high speed. Staying compliant is difficult in this environment. Banks face increasingly large fines and threats to their reputation. Attacks are becoming more sophisticated and complex. There has never been a more important time to create a solid compliance strategy for anti-financial crime.

So far, most banks have focused on hiring more people to tackle the problem. Many are still relying on older systems to execute compliance tasks. This may work in the short term. But with the world's leading economies going cashless and new regulations like Instant Payments and PSD2 coming into effect, this approach will soon be difficult to support. How can banks best perform their gatekeeper function? Let's explore the current landscape and how financial institutions can prepare for the future.

A Hiring Frenzy Takes Over the Industry

Do you have research skills worthy of joining the FBI? Looking to make up to €45,000 per year + benefits? Investigate and report suspicious behavior by day; watch the news at night and see criminals arrested thanks to your work.

This is just a taste of the job descriptions and salaries banks are using to attract Customer Due Diligence analysts. The number of job openings at compliance departments has increased substantially in the last two years. Hundreds of positions go unfilled in the Netherlands alone. NOS reports that ABN Amro increased its compliance staff by 550 people in 2018. ING grew its global compliance departments by 3,000 jobs in 2018, and still has vacancies to fill. People with law and business degrees are the most sought after. Criminologists and historians are also in demand.
What's driving this hiring spree? The answer is tougher regulation around Anti-money laundering (AML) and Know-Your-Customer (KYC) compliance.

Comply or Pay up

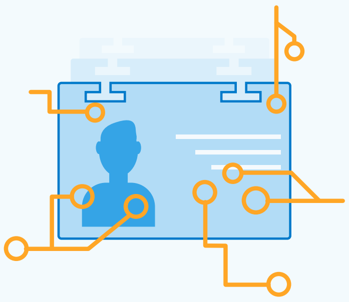
In the past 20 years, banks have faced increasing scrutiny from regulatory authorities. The decade following the 2008 financial crisis was particularly turbulent, as governments heightened their fight against fraud, money laundering and terrorist financing. Banks that fail to meet KYC, sanctions and AML requirements face hefty fines. In July 2018, Dutch authorities strengthened AML legislation by enabling regulators to impose a turnover-related administrative fine of 20% for significant AML breaches. This same law also broadened the publication powers of supervisory bodies.

The United States levied 91% of all global AML, KYC and sanctions-related fines between 2008 and 2018, totaling $23.52 billion. The highest enforcement action issued worldwide, in this time period, was an $8.9 billion penalty against a Tier 1 French bank in 2015.

In Europe, regulators issued $1.7 billion in fines between 2008 and 2018. The Dutch government stands out as the highest issuer. One of the leading Dutch banks, ING, had to pay a fine of €775 million in 2018 for failing to prevent money laundering. This included a payment to the state of €100 million, which was the alleged amount the bank saved for skimping on compliance staff for a number of years.

The Burden of Compliance

Fines are not the only problem when it comes to compliance. There's a big gap in the market for compliance staff. Experienced people are especially hard to find. Most compliance roles are also not as rewarding as some of the sexy job descriptions claim. They are excessively manual: ticking boxes, requesting identification from customers, and typing information in text fields. Do banks actually need people to fill these roles? What is the cost of compliance?



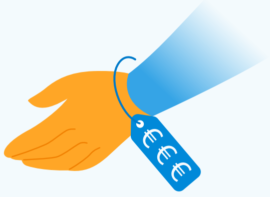
By implementing new technology to improve KYC processes, banks can save a significant amount in operating costs and avoid fines.

At the moment, most banks have multiple functions and departments involved in anti-financial crime, covering detection, investigation, and reporting. A recent Ovum survey shows that operational expenditure on financial crime activities increased by 9.3% between 2015 and 2019. That increase may seem low, but by some estimates, banks spend around $270 billion per year on compliance and the growth in costs has been sustained. By implementing new technology to improve KYC processes, banks can save a significant amount in operating costs and avoid fines.

Money laundering and terrorist financing come at a high cost to society.

Easing the financial burden is not the only incentive to adopt new technology. Inefficient and cumbersome compliance processes also take a toll on customers. Mitek and Consult Hyperion state that banks can lose up to €10 million a year due to complex and burdensome compliance practices that turn customers away. The cumulative lost opportunity could surpass €150 million after five years. Inefficient onboarding has resulted in customer abandonment rates of 56%. Today's consumers don't expect to visit physical bank branches to identify themselves and start an account. They also want to experience the least amount of friction when banking. At the same time, nobody wants to become a victim of financial crime, and banks are well aware of the long-term damage an incident can cause to their brand's image. In fact, the 2019 Ovum survey we cited before, shows that protecting customers from being the victims of crime is the top overall concern for compliance execs.

Failing to perform the appropriate checks is thus, not an option. Not only because of the associated costs to banks, but because financial crime has a direct impact on human lives. Money laundering and terrorist financing come at a high cost to society.



Human trafficking generates roughly $150 billion a year for traffickers.

The Human Cost

A 2015 report by the Financial Action Task Force offers insight into how criminal and extremist groups exploit the sheer size and vulnerabilities of the financial sector to carry out their activities. The examples that follow are just a selection of the many offenses explored in the report.

Terrorist Financing offenses

Terrorist groups have multiple means of generating revenue. These include donations, extortion, kidnapping for ransom, the exploitation of natural resources, the use of “front” companies or NGOs, and sometimes legitimate enterprises. Even healthcare organisations and health insurance companies may be complicit in terrorist financing. To transfer funds, these criminal groups typically use banks, money value transfer systems, and cash - or a combination of these. A stark example from Belgium illustrates this.

Over a three-day period, three individuals declared around € 90,000 in cash to customs officials at Brussels' airport. The three couriers were all Belgian nationals who had been living in Belgium for a long time. The funds they declared were said to originate from a German non-profit that provides humanitarian aid in African countries. According to the German Financial Intelligence Unit, the non-profit was linked to another NGO that had been banned in Germany for allegedly supporting a terrorist organisation.

Each of the couriers had a bank account which had received funds from a radical Islamic organisation. Nearly €20,000 had been withdrawn in cash from their accounts. A sum of €10,000 was transferred to Turkey. Belgian authorities suspect that at least part of the funds described above could have been used to support terrorist activities. But extremist groups, such as these, are not the only source of concern. Human trafficking is another.

Human trafficking offences

Human trafficking generates roughly $150 billion a year for traffickers, according to a 2014 report from the International Labor Organization. Besides sex trafficking, which sees an estimated $99 billion per year, billions are made in industries like manufacturing, agriculture, mining and other industries due to forced labor. These illicit activities also exploit vulnerabilities in the financial sector.

A recent example from the UK serves as a cautionary tale. Two brothers trafficked 18 men from Poland to the United Kingdom to work in a major sports clothing warehouse. The traffickers paid for the tickets to the UK and once the men arrived at their destination, they were forced to hand in their passports to a representative of a local employment agency. They lived in terrible conditions. The offenders helped the men open bank accounts and then took control of their bank cards, using physical and verbal threats to coerce them. The offenders took the majority of the victims' £265 weekly wage, leaving each victim with just £90 a week. The offenders reportedly made £35,000 throughout the exploitation period. Close cooperation between the offenders' bank and the police revealed further suspicious activity. A high percentage of the men's income was withdrawn quickly after it reached their accounts. Analysis of ATM activity for these customers showed that their ATM usage often occurred at the same machine at the same time, suggesting that a third party was indeed in control of their cards. The offenders were eventually sentenced to serve six years in prison, as the Financial Action Task Force reports.

A Delicate Balance

The consequences of financial crime are grave, as illustrated in the above case studies. Society expects that banks (along with governments and other financial institutions) act as gatekeepers to the financial system. Consequently, they should take this seriously. The question is, how can banks avoid fines while reducing the burden of compliance and executing their duties efficiently? As we hinted at before, new technologies are coming to the rescue.

Fighting crime with new technology

Financial crime is becoming increasingly sophisticated and institutions face attacks on multiple fronts. Understandably, the associated workload is daunting. Operational challenges are often made worse due to the lack of technological capabilities. Platform performance is a key technology challenge for anti-financial crime. This is reported across the board, by compliance, fraud and security, and related technology functions. Specifically, these departments are struggling to enhance “detection effectiveness,” and deal with the volume of information. Managing high levels of high positives is particularly difficult. So is responding and adapting in an agile way to threats, especially as criminals find new ways to go about their business as soon as banks become effective at tackling common attacks.

Platform performance is a key technology challenge for anti-financial crime.

To deal with these challenges, many banks are betting on Artificial Intelligence (AI) and Machine Learning (ML). As Ovum explains, “the long-term goal is for detection capabilities to automatically learn, respond, and optimize to tackle evolving trends, with the use of AI techniques allowing new data sources (e.g., through natural language processing) and ML allowing models to be developed and optimized by platforms themselves.” Nearly 85% of compliance executives and over 90% of fraud executives in Ovum’s 2019 report stated that their institution is “using or actively planning to use machine learning to tackle fraud.”

AI takes center stage

The use of AI is not unheard of when it comes to combating fraud in the financial sector. What's new, is expanding the use of AI to analyze and detect a wider breadth of illicit activities. FICO, the industry's leading vendor, can trace its Explainable AI reason reporter for fraud detection back to 1988. The software has since been enhanced with more advanced models, adaptive and predictive analytics. Now dubbed Falcon X, the software is used by 9,000 banks worldwide to detect all kinds of financial crime, including money laundering.

> The technology banks need to optimize compliance is already available, and many leading banks are already leveraging it to improve the effectiveness and efficiency of their compliance efforts.

What's particularly interesting about FICO's software is that it leverages ML techniques that were developed using data from the FICO Falcon Intelligence Network, "a global consortium of transactions that spans credit and debit cards, P2P transfers, suspicious activity reports (SARs), and real-time payments." In many ways, FICO's network aggregates the collective intelligence of the financial sector, helping users reduce false positives while prioritizing high-risk activities. The software also identifies unusual patterns in existing customers. It goes on to analyze prior alerts and outcomes to improve detection. In cases where there is no historical data from suspicious activity reports, the software identifies “subtle patterns” in existing data to develop customer archetypes which can be used to detect illicit activity if it were to develop.

In sum, the technology banks need to optimize compliance is already available, and many leading banks are already leveraging it to improve the effectiveness and efficiency of their compliance efforts. Still, there are many organizational puzzles to solve. Perhaps the largest one is the silos that commonly separate different departments, like fraud and financial crime. According to Ovum, only a quarter of retail banks have adopted an integrated approach to financial crime systems, despite collaboration between these functions being the norm.

An integrated approach

FICO’s research shows that up to 80% of the requirements of the fraud and AML compliance functions are the same. Yet, most banks keep those functions separate. Breaking down these silos can go a long way to reduce the cost of compliance and improve operational effectiveness, because employees can share their experiences and make more informed decisions collaboratively. A side-effect of this division is that departments tend to use multiple systems. Switching between systems across functions impacts staff productivity, and results in disjointed operational processes. It also drives up costs. Functionality is often duplicated and requires additional maintenance and integration work.

This also impedes adaptability, Ovum’s research explains, as large-scale changes require more testing. It also makes management reporting challenging, as data extraction is complex and there is a lack of standardization. Finally, the use of multiple systems increases staffing issues. Each system requires specific training and resource support, making it difficult to transfer skills within and across functions. This challenge is felt most by people on the fraud compliance front. A quarter of institutions consider that this drives user-experience challenges for fraud investigations staff, and is damaging to productivity.

The good news is, the industry is catching on. More than 70% of banks that are actively looking to integrate fraud and compliance seek to do so within the next three years. With the volume of transactions set to increase, prioritizing and streamlining case management with an integrated approach will become even more important.

More than 70% of banks that are actively looking to integrate fraud and compliance seek to do so within the next three years.

What the future holds: less cash and more payment speed

The amount of transactions that will have to be screened by banks will only grow in the future. For starters, societies are going cashless. China is leading the way here. By 2017, more than three-quarters of Chinese people were using digital payments instead of cash. In Sweden, "even children pay with debit cards," the government claims. About 80% of people in the country pay their purchases with cards. The British are heading in that direction too. The Telegraph reports that there were 11.5 billion fewer cash transactions in Britain in 2018 compared to 2008 – a decline of 51%.

Beyond increasing volumes, the drive towards digital payments will also increase the complexity of compliance, especially in Europe, where regulations like PSD2 and Instant Payments are entering the picture.

PSD2 will make the financial system in Europe more open and digital. Online retailers with a PSD2 license, for instance, will be able to fetch users' account data from their bank and automatically charge the account for purchases once the user approves. For banks, this opens up a Pandora's box when it comes to compliance. It's not just about making sure they are PSD2 ready, by opening up their banking ecosystem. More access also means more transactions and more parties to check.

Similarly, banks are bracing for Instant Payments, where transfers are done within seconds. By the end of 2019, 2,360 PSPs in Europe were reachable with Instant Payments. The implementation of instant payments will probably lead to more bank transfers, but the burden of compliance, and particularly fraud prevention, does not necessarily lie with the total amount of transactions. Rather, it has more to do with payments' speed.

Imagine a criminal who just stole €100,000 from an unsuspecting company by sending them a fake invoice. The first thing that the criminal will want to do is make the money untraceable. He will likely split it over multiple bank accounts that he owns (through a false name), or through money mules. After doing this several times, the money comes back together in one account with small enough transfers to stay unnoticed. This process is called smurfing.

Before instant payments, it could take hours or even days before money was deducted from one account and credited to another. There was more time to monitor all the bank accounts and more time for banks to communicate and trace the money. Instant payments will make criminals harder to catch.

Banks will need to be prepared. For one, sanction screening will need to be real-time and not batch based. However, the more effective solution is communication between multiple banks. Dutch banks are ahead of the curve in this regard. So far, five banks in the Netherlands have agreed to work together in order to fight money laundering and terrorist financing. With a central place to see patterns between multiple banks, the chance of catching criminal activity will increase substantially.

Conclusion

As we explain above, hiring more and more staff will simply not be enough to fulfill anti-financial crime obligations. Banks need to apply a more integrated approach to compliance, bringing AML and fraud prevention under one roof. They will need to rely more on technology to automate screening and get smarter at detection, especially with the introduction of instant payments and PSD2. Moreover, they will need to work together to face up to the growing complexity of crime.

Visma Connect offers a one-stop shop for financial institutions entering the new world of payments. We offer Critical Payments Services, including PSD2 and SWIFTNet connectivity, as well as KYC, real-time transaction screening and AML solutions powered by FICO technology - all under one roof. We offer a dashboard that connects and consolidates alerts and cases from different software modules, helping you integrate your data and processes for better compliance decisions. This centralised system supports investigative processes and workflows. Your entire team can use it to collaborate on cases and submit regulatory reports. Our services have built-in flexibility and convenience. Cost is based on volume, so you can scale as quickly and as often as you need. We handle the maintenance, so you don't have to worry about changing the system when regulations and business conditions change.

Would you like to know more?

For further information, go to www.vismaconnect.nl
or call +31 (0)88 - 11 61 800.

Click here for more information

About Visma Connect

Data is today's most valuable resource. With digitisation increasing around the world, it's becoming imperative for societies to have a safe, fast and verifiable means to share data for different purposes. Visma Connect is at the heart of this transformation. Just as energy companies provided the infrastructure to power the industrial revolution, Visma Connect is the utility company of the digital society.

Mission
Our mission is to empower citizens, companies and governments through secure, efficient and qualified digital information exchange worldwide. We do this by designing, building, connecting, analysing and managing information chains and data sharing ecosystems for the public, healthcare, logistics and financial sectors.

Vision
A digital society in which citizens, businesses and governments can interact, conduct business and share information in the certainty that their data arrives safely at the intended recipient and is only used and analysed according to the permissions that the owner of the data granted.

Written and edited by:
Gloria Quintanilla and Steven Schouten

www.vismaconnect.nl