Error terror

Traditional KYC processes are time-consuming, cumbersome and offer ample opportunities for human error. They also leave banks open to financial and reputational hardship. Yet as anti-money laundering regulations continue to tighten and banks are dragged kicking and screaming into the digital age, **Tom Loonen**, professor of financial law and integrity at the Vrije Universiteit Amsterdam, explains why the old modus operandi is no longer viable – and what we can expect from the future of KYC.

Financial criminals, says Tom Loonen, can be like moles. As the professor of financial law and integrity at the Vrije Universiteit Amsterdam says, they go about their business, making money transfers within an intricate, hidden network of underground tunnels. But now and again, they have to pop their heads up into the legitimate world to get some air. That's when financial institutions, law enforcement – or a combination of the two – can catch them.

Historically, explains Loonen, who also works as a special counsel at Amsterdam's Pinsent Masons international law firm, the problem has been that know-your-customer (KYC) processes have been too cumbersome to keep up with the moles' movements. Many opportunities to catch them are missed due to human error. In other cases, it just takes too long to get to the air holes. Yet as more banks implement digital processes, along the way partnering with their competitors and law

VikaSuh; Creativa Images; TA design/Shutterstock.com

Tom Loonen, professor of financial law and integrity, Vrije Universiteit Amsterdam

enforcement, those chances are becoming greater. It's a slow process, with many banks reluctant to embrace the digital age. Traditional KYC processes, after all, are not particularly efficient or effective. Important questions are often not asked. Information, if it was stored at all, has typically been scattered across various disconnected platforms. And when new IT systems are introduced, they're often stapled onto old ones. Connecting them is a challenge, and there certainly isn't one complete picture of each client stored anywhere.

Even though, for a long time, that's how things were done, it's simply not a viable way of running a financial institution. For one thing, anti-money laundering (AML) legislation is becoming stricter, with new EU measures approved by MEPs this year requiring financial institutions to verify their customers' identity, what they own and who controls the company. Even before that, some senior managers and board members were being prosecuted and fined for breaking the rules.

Banks, for their part, are realising that it is no longer sustainable to plough money into larger and larger KYC workforces, especially when technology can do part of that job much more effectively. As Loonen says: "The current modus operandi doesn't work. Banks have no choice but to change."

Investing in integration

For the past few years, we have seen banks investing huge amounts of money and time into new integrated KYC systems, which can communicate with the other IT systems at the institution. "Traditional processes were very time consuming, lots of errors were made and it also wasn't very client friendly," Loonen explains. "With new systems, they can very easily extract and send data in a proper way and make multi-related inventories about clients."

UK building society Nationwide, for example, has partnered with identity verification (IDV) platform Jumio to bolster its online account opening processes. Leveraging AI, biometrics, machine learning and automation, the platform's API provides end-to-end identity proofing, KYC and AM solutions. As a result of this integration, Nationwide claims that their KYC processes have become more streamlined and efficient and the time to open an account has been dramatically reduced.

Meanwhile, as part of its digital transformation, Santander has engaged Encompass, a firm that helps global banks and financial institutions fight financial crime and streamline their KYC processes to comply with AML requirements, providing a more efficient way of onboarding clients. Having one platform with all of the information gathered during the corporate discovery stage – and throughout further Customer Due Diligence (CDD) investigations, which are carried out to ensure compliance with AML and counter-terrorism regulations – has allowed the bank to make decisions much faster.

Centralising data

More than that, though, a growing number of large banks are working together on pilot projects to share their information in a central database. The idea is ultimately to enhance AML efforts collectively. In the Netherlands, for instance, a network of five banks shared CDD data for KYC checks during a 2019 pilot. Today, the resulting Transactie Monitoring Nederland (TMNL) network is focused primarily on transaction monitoring. Banks send anonymised transaction data to TMNL, which uses the information to identify meaningful connections between them, providing new insights into potential money laundering activities.

In the UK, meanwhile, Mastercard's payment technology arm, Vocalink, has formed a partnership with UK retail interbank payment systems operator Pay.UK to build the Mule Insights Tactical Solution (MITS). Six Nordic banks – among them Danske Bank and Nordea – have collaborated to launch Invidem, a platform that collects and verifies KYC information for corporate customers. Through Invidem, the founding banks have developed a common standard for KYC information, made available through its KYC services and platform, to ensure compliance with financial crime prevention requirements.

Loonen is also seeing banks developing their KYC departments to make room for more so-called 'financial detectives'. "These are people who are highly qualified and are specialists in making a full inquiry and detailed research into clients," he explains. "They can really look at what type of client this is, what his background is and advise what to do with this client or prospect."

At the same time, Loonen has noticed more openness among banking executives to cooperate with public offices and law enforcement. One such example is the Financial Intelligence Unit in the Netherlands, which is the central reporting point for banking entities to report unusual transactions. "Banks are more and more willing to share data with authorities but also with other banks, in order to make sure that the chances of getting hold of criminals are as high as possible," Loonen says. "Of course, this is also because in the Netherlands, the Public Attorney has been tough, and we have seen board members at several banks being investigated and potentially personally prosecuted for neglecting to follow AML laws."

Challenges ahead

Progress, in short, is happening apace – but Loonen is emphatic that there are still many challenges to overcome. In the Netherlands, for example, there are still significant concerns about data privacy within the TMNL network. "While the Dutch Central Bank and the Minister of Finance are very happy with the

$5.8bn

The amount the global AML market size is expected to grow to by 2027, up from $2.8bn in 2022, enjoying CAGR of 15.9%.

GlobeNewsWire

TA design/Shutterstock.com

Xxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxx

initiative, the Privacy Authority is not happy because they believe that personal privacy is at stake," Loonen explains. "I'm not so sure that's the case. I understand that people are anxious with regards to privacy, but I believe we always have to find a balance between what we want to achieve – a safe financial system that doesn't enable criminals and terrorists – and the price for that goal. In my view, with the assurances being given by the banks and the authorities being very vigilant, it's a fair investment."

As technology, including AI, becomes a more important part of KYC processes, there are also mindset shifts to be made. Traditionally, KYC workforces were made up of armies of people carrying out repetitive manual work, such as data entry. Increasingly, AI has the potential to take on many of those tasks, allowing specialists to focus on the exceptions. According to Loonen, banks must be flexible and willing to adapt to these new ways of working.

At present, the biggest banks have up to 8,000 people working on KYC every day, but Loonen believes that, over time, this number could be cut in half. "A lot of work has to be done first to obtain, analyse and store information in proper systems," he stresses. "But once this has been achieved and the right AI solutions have been introduced, I would not be surprised if banks could reduce their KYC workforces by 50 percent or more."

With all this activity in the background, Loonen is watching with interest at how the situation develops over the next few years. One thing he is certain of is that progress won't be flawless. "We will definitely have a lot of accidents happening in the near future when it comes to AI," he predicts. "Banks want to reduce their costs as soon as possible and maybe they will sometimes do that too quickly and use systems that are not 100% okay, built on AI that is a little bit shaky."

He is also certain that our knowledge of the underground banking network – and the movements of the moles within it – will increase. "When you have all of those institutions combining data, you are making that chance to catch a mole as big as possible," he says. "But it is very challenging. I'm not so sure we will win this war. But I'm sure that we will make very big steps and make great efforts to reduce the chances for these moles to pop up and use the financial system. However, of course it is much better to catch the moles themselves."

There is one final point on which Loonen is adamant: banks that do not accelerate their digital transformation and embrace digital KYC processes will be left behind. "The digital journey for clients today is so crucial," he stresses. "If you have 20 clients waiting to open an account with you and can only handle ten, the other ten will go to your competitor and you won't be able to grow commercially. At the same time, legislation will only become more severe. If banks don't have their data and their processes in order, they run the risk of losing their license." They are still pinpricks, in short, but there is more and more light filtering into the murky network inhabited by financial criminals – ultimately resulting in fewer places for those pesky moles to hide. ●

$800bn – $2trn

The estimated amount that is laundered each year across the world, representing 2-5% of global GDP

United Nations Office on Drugs and Crime

0.1%

The amount of money laundering funds that are recovered by AML activities

Taylor & Francis Online