Meet Fourthline, the company on a mission to create a safer global financial system

As part of our quickfire questions series – or QFQs – we spoke to Krik Gunning, cofounder and CEO of digital identity specialists Fourthline about the growth in financial crime during the pandemic and keeping up with the threat of financial fraudsters.

Temps de lecture : minute

2 December 2021

What was the catalyst for launching Fourthline?

We initially began our business as a deposit platform. The catalyst for launching Fourthline came when we were looking for a great client onboarding solution for our own business as a regulated payment institution. We started looking for parties who could help us out, but we found nothing in the market that would meet our high-quality standards. So, we thought, why don't we build this ourselves? After launching our deposit platform, several banks asked us whether they could use our Know Your Customer (KYC) functionality on a standalone basis.

At the end of 2017 we shipped the first version of our digital identity and verification product. Soon afterwards we signed N26, the largest digital bank in continental Europe, and a few other fast moving fintechs. Today, we have over 250 employees in Amsterdam and Barcelona helping us in our mission to fight financial crime.

Tell me about Fourthline’s technology – how does it work and how do customers use it?

Every year, $1 trillion is laundered. The problem is vast and unfortunately, financial crime is becoming increasingly sophisticated. To stay one step ahead of financial fraudsters, our technology identifies emerging financial crime patterns across borders.

We offer a bank-grade technology stack and have internationally recognised fraud experts in our ranks to authenticate and verify the identities of thousands of new customers every day by performing hundreds of checks and matching people against government issued ID documents.

Our biometric and geolocation analysis combined with checks against worldwide sanctions lists catches 60 percent more fraud than the rest of the market with 99.98 percent accuracy

How has the business evolved since its launch?

We have always focused on combating financial crime to create a safer financial ecosystem. What has changed is banks' unique responses and perceptions of the magnitude of the challenge.

Although KYC was not on most banks' radars five years ago, it is now a top priority. Anti-money laundering failures cost money, reputation, and customers. It’s no longer enough for financial institutions to improve financial crime checks on new clients. Regulators across Europe require them to also revalidate existing clients through large-scale remediation. This requires a very diligent, high-quality process under strict timelines.

Banks want to ensure they get it right the first time, exceeding regulatory requirements from a quality perspective, while also meeting the deadline to avoid forced account closures. They typically hire large teams of people to try to solve the problem. This is both costly and inefficient. We are committed to making this easier for all parties.

The type of fraud committed has also changed over the years. Where we commonly saw document fraud (hiding one's identity by means of a counterfeit ID document), in recent years we've seen social engineering become more prevalent. To combat this, financial institutions not only need to conduct holistic data checking beyond document verification at account opening, but also monitor customer identities throughout the customer lifecycle. Money mules, for example, appear to be perfectly legitimate people at onboarding, but transfer access to the account to money launderers after the account is opened.

Catching these individuals at KYC onboarding is extremely challenging but essential in the fight against financial crime. Banks and other financial institutions must adopt technology that can confirm the account user is the account holder throughout various points in the customer lifecycle.

Have you noticed any emerging trends in financial fraud that banks and financial institutions should look out for?

The pandemic has led to an increase in financial crime. To avoid detection, fraudsters are growing more skilled, using deepfakes, social engineering techniques, and creating synthetic online identities.

This year, 47% of detected financial fraud attempts in Europe involved social engineering or manipulation. In fact, we found a 37% increase of these attempts between June 2020 and June 2021 after analysing millions

of bank account openings. It is simply not enough for banks to have core identity checks and balances in place to protect against fraud. Specialist KYC technology is essential to stay one step ahead of increasingly inventive criminals.

What has been your biggest business challenge?

Applying AI to KYC is extremely challenging as it requires in-depth knowledge of regulatory requirements. It also requires data on specific markets and on both fraudulent and authentic ID documents.

We have set the bar high and only automate an identity check if we can objectively prove it leads to a higher quality outcome. This rigorous focus on quality made it a daunting task to apply AI at scale, but last year alone we shipped six new AI models and our proprietary Optical Character Recognition (OCR) models outperformed those of Google Vision (which in layman's terms, means they're really good!).

What's in store for the future?

Looking ahead, we expect to see the rise of portable digital identities in the form of eIDs, as well as more focus on continuous KYC processes. The latter will allow regulated institutions to continuously monitor customer identities throughout the customer lifecycle, after the initial KYC onboarding. This ties into the wider trend of account takeovers via social engineering techniques. We are focused on combatting account takeovers by re-verifying that the account user and the account holder are one and the same.

We expect to see an increase in fraud detection tools to combat the continued evolution of fraud techniques such as deepfakes. It's also likely that we'll see further digitisation of financial services and with that,

increasingly stricter AML regulations and enforcement.

Article by Maddyness UK