REPRINT

R&C risk & compliance

TACKLING KYC AND AML WITH DIGITAL IDENTITY

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

APR-JUN 2021 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

FOURTHLINE

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

ONE-ON-ONE INTERVIEW

TACKLING KYC AND AML WITH DIGITAL IDENTITY

Krik Gunning
Co-founder and Chief Executive Officer
Fourthline
E: k.gunning@fourthline.com

Krik Gunning started his career as an M&A banker at ABN Amro. He then co-founded advisory boutique IvyRoads before joining Safened as chief commercial officer in 2015. In 2017, he co-founded Fourthline and now serves as chief executive officer.

R&C: How would you characterise the prevalence of money laundering across the globe at present? What kinds of risks and threats does it present?

Gunning: According to Deloitte, financial crime costs an approximated $2.1bn a year globally. Money laundering – which is largely facilitated by fraudulent account openings – soared to record highs in 2020, according to most experts and industry analysts. While we do not track money laundering itself, our internal data showed identity fraud attempts surging by 15 percent during the year – much of it driven by new opportunities arising during the pandemic and subsequent lockdowns. Our proprietary data also found that social engineering surpassed counterfeit documentation as criminals' preferred form of identity fraud in 2020, which confirms the criticality of holistic data checking as opposed to simple document verifications. As financial crime becomes more sophisticated, comprehensive data verifications with checks across identity, liveliness, documentation, biometric data, device metadata, watchlists, and so on, becomes increasingly crucial to security. Beyond the obvious costs that money laundering imposes on society as a whole, banks face great risk of sanctions and reputational damage by allowing money launderers access to their services. Particularly insidious is the use of money mules, who are legitimate ID holders, who open accounts and then transfer access to money launderers or perform activities on behalf of them. Catching these individuals before they open an account is a challenging but essential task for banks – one that requires unified data in an organisation and collaboration across the industry as a whole.

R&C: Could you explain how digital identity tools are being leveraged to augment know your customer (KYC) and other anti-money laundering (AML) processes?

Gunning: Digital identity tools tackle error-prone and costly legacy processes that regulated institutions rely on to remain compliant. By reducing inefficiencies and inaccuracies associated with existing back-office work, digital identity management tools streamline know your customer (KYC) and anti-money laundering (AML) processes and ensure that those processes detect fraud at the highest levels while also providing a simple and convenient way for account openers to authenticate their identity. Consumers will no longer tolerate being forced to visit a bank branch to submit documents or prove their identity. The new standard expected by consumers is an entirely digital process that results in access to their new account in a matter of minutes. To fulfil this expectation, banks must adopt technology that can use mobile or web interfaces to authenticate documents, confirm

liveness, and verify that the ID holder is the same as the account opener.

R&C: What factors are driving the growing interest and appetite to utilise this technology? How much are AML regulatory developments contributing to investment in this area?

Gunning: Increasingly strict regulations are being implemented in the European Union and around the world, which is also driving banks to adopt new technology to maintain compliance without compromising customer experience. In order to provide competitive customer experiences, regulated institutions need technology that onboards customers quickly and seamlessly. Beyond a general trend toward digitalisation, there is tremendous pressure on banks to reduce costs right now. Operational costs at banks, and compliance costs in particular, have spiralled out of control in recent years, and shareholders are demanding that more efficient, less labour-intensive approaches be implemented.

R&C: What are the benefits of adopting digital identity technology? Are there any challenges or pitfalls that need to be properly managed?

Gunning: The benefits of adopting digital identity technology include detecting fraud and preventing money launderers accessing services, meeting customer expectations by elevating customer experience and security, improving account opening conversion rates and reducing the cost of customer acquisition, reducing an institution's total cost of compliance, and avoiding non-compliance and the fines and reputational risk that comes along with it. As far as challenges are concerned, these include overcoming bias toward legacy systems and internal processes, difficulties aggregating data across functions and processes, and inaccurately or incompletely evaluating the total cost of compliance across complex processes and cross-functional lines. Moreover, FinTechs are generally faster to adopt new technologies, whereas institutions have a

> **"In order to ensure quality in fraud detection, it is critical to be able to see the full picture."**
>
> *Krik Gunning, Fourthline*

hard time keeping pace because of the scale of their operational structures and processes.

R&C: In what ways has digital identity technology improved in recent months? What innovations are enhancing available KYC and AML solutions?

Gunning: Artificial intelligence (AI) advancements are driving a more seamless onboarding experience for end-users, improving the ability of the mobile/web interface to recognise text and populate fields accurately. AI advancements are also improving the ability to recognise counterfeit documents and documents that have been tampered with. Network analytics is improving the ability to use isolated data points that span across a customer profile – and an entire applicant database – to identify anomalies and inconsistencies that may indicate fraudulent behaviour. These techniques have been augmented by increasing cooperation from clients and government institutions. This support has helped many organisations to sharpen their proprietary fraud database, which leverages cross-pattern and cross-border detection while remaining fully General Data Protection Regulation (GDPR) compliant.

R&C: What steps should be taken when embedding a digital identity system? What considerations need to be made to ensure the system is efficient and effective?

Gunning: In order to ensure quality in fraud detection, it is critical to be able to see the full picture. Assessing data points across thousands of document types for countries throughout Europe provides a more complete understanding of identity fraud attempts, and therefore enables better detection. By examining more data, more patterns can be seen, which allows more fraud to be identified. When considering the cost of an implementation or a process, be sure to include all expense components, including labour costs for processes like reviews and investigations, among other things. Some vendors are able to both automate processes that are traditionally manual, and provide more highly skilled, cost-effective support for any manual processes that do remain. It is also beneficial to provide a model to clients for calculating their cost of compliance, which enables them to clearly define inefficiencies and construct smarter solutions.

R&C: What themes do you expect to shape digital identity in the years ahead? Will it be an essential tool for understanding customer profiles and reducing money laundering practices?

Gunning: In the years ahead, we expect to see durable, portable identities in the form of eIDs, as well as continuous KYC, enabled by eIDs, which allow regulated institutions to continuously monitor accounts throughout the customer lifetime after their initial KYC onboarding. This ties into prevention of account takeovers by re-verifying throughout the customer lifetime that the account holder and account user are one and the same. We also foresee increased innovation in fraud detection tools to combat the continued evolution of fraud techniques, such as deep fakes and high tech masks. Additionally, there is likely to be a continuation of the digitalisation of account opening and banking services, closely aligned with increasingly strict AML regulations and more aggressive enforcement of existing regulations. R&C