



## Open Banking, Open Risk?

Changing dynamics in financial services demand a new approach to financial crime risk management.

There is growing consensus that the current global framework for fighting financial crime is not as effective as it could be, and that more needs to be done at the international, regional and national levels to help identify and stem the flow of illicit finance – an activity which supports some of the worst problems confronting society today, including terrorism, sexual exploitation, modern slavery, wildlife poaching and drug smuggling.

The financial services industry is changing rapidly with the move towards open banking and challenger banks. New financial crime risks are arising from the products and services, technologies and new business models required to service a new generation of tech enabled consumers.

New ways of banking are of course followed closely by the sophisticated criminal and their ill-gotten gains. Fresh approaches are required by all stakeholders to address these risks.

### Emerging risks clearing the path for criminals.

The significant increase in players and products in the banking space means that previously closed down or managed risks are back and they are more aggressive than before. Examples of emerging risk we are seeing enabling criminals today are very much grounded in the risk areas that traditional banks faced 10 years ago.

- Market changes mean that customer on boarding controls are increasingly unfit for purpose. On-boarding controls are the first line of defence for financial institutions, ensuring you are who you say you are. This increased use of specialist service providers means that customers are being on boarded more frequently, and in an environment where customer experience is increasingly important. The use of new methods of electronic identification and verification including selfie images, videos and data from third party information providers is becoming commonplace. But as the number of players and methods of verification proliferate, levels of inefficiency and inconsistency have also increased. Inefficiency and inconsistency means opportunity for criminals to use fake documentation to get access to coshure banking facilities.

- With the number of players providing financial services in the market growing, the number of transactions being processed by any individual bank has reduced. An increasing amount of activity now takes place out of sight, for example through pre-paid cards or niche foreign exchange services.

As a result individual banks now have only a narrow view of the overall activities of their customers, making it harder to monitor and identify suspicious behaviour. Holistic transaction monitoring is the second line of defence for financial institutions. Ineffective monitoring equals a criminal's dream landscape.

### How do we fight this evolution of new money laundering risk?

Financial crime is a US\$3.5 Trillion-dollar threat to businesses and global economies. This is in the form of both financial losses due to illicit activities and financial fines and penalties imposed for non-compliance with global regulations. For example since 2008, \$36bn USD in fines have been levied on companies across the globe for fines relating to Anti-Money Laundering (AML) fines.

Two ways in which we at Deloitte Financial Crime are advocating for change in addressing international financial crime prevention are:

- A Public-Private Partnership model – Many of the structural inadequacies of today's financial crime risk management framework arise from the silos in which banks and FinTechs operate. By collaborating and sharing intelligence, learnings and data across stakeholder, we will be better able to identify the financial crime activities that are endemic in the system. Pooling transactional data would allow for a more holistic view of the typologies of financial crime. Enabling this sort of collaboration will require the regulatory support necessary to overcome the many data privacy issues, however just because there are challenges, that does not mean we should not try.
- Increasing and improving the use of technology to combat illicit finance. The governments of the G20 and the broader international community should encourage the process of innovation in financial regulatory technology that assists in compliance with financial crime regulations and improves risk management overall. One way technology can help is the SmartID concept. Banks and alternative provider would no longer have the burden of individually collecting customer information, and instead be able to use the verified attributes contained in a Blockchain enabled digital identity for identification and verification purposes.

## Contact



### Deirdre Carwood

Partner | Head of Forensic

Dublin

D: +353 (0) 1 490 7051

dcarwood@deloitte.ie