REPRINT

R&C risk & compliance

MANAGING FINANCIAL CRIME RISK AND AML PROCESSES WITH TECHNOLOGY

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2018 ISSUE

www.riskandcompliancemagazine.com

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

C6
An Acuris company

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

ONE-ON-ONE INTERVIEW

MANAGING FINANCIAL CRIME RISK AND AML PROCESSES WITH TECHNOLOGY

Nick Parfitt
Product Director
C6 Intelligence
T: +44 (0)20 3741 1200
E: info@c6-intelligence.com

Nick Parfitt has 18 years' experience in project and programme management, business process change and implementation of technology and business solutions in leading global financial services, telecommunications and public sector organisations. He also has seven years' experience in financial crime compliance consulting and industry experience supporting Tier 1 financial institutions in assessing their anti-money laundering (AML) and Know Your Customer (KYC) sanctions operations.

R&C: To what extent are financial crimes growing in frequency and complexity? How would you summarise recent trends in this area?

Parfitt: The development of technologies has been the biggest driver for change in financial crime; fraud has now become the most commonly experienced offence. According to the Crime Survey for England and Wales, an estimated 3.6 million cases of fraud were recorded in 2016 alone. Financial fraud losses across payment cards, remote banking and cheques totalled £768.8m in 2016. In particular, we are seeing increased levels of crime-as-a-service, use of ransomware, criminal use of data – not only for direct financial gain, but also ransom, extortion and complex fraud, payment fraud and virtual currencies, such as cryptocurrencies or Bitcoin becoming the standard for extortion and payment for illegal products and services.

R&C: Could you outline some of the key legal and regulatory developments affecting anti-money laundering (AML) and other financial crimes in recent times? Do companies need to accept that they now operate under heightened scrutiny, and react accordingly?

Parfitt: Newly established organisations include the Panama Taskforce, which provides investigative and asset denial opportunities, and is also identifying new tax evasion structures and the Joint Financial Analysis Centre (JFAC), which investigates offshore companies with concealed UK ownership, as well as doors to commit economic crime and many others. The National Crime Agency (NCA) is working on an arrangement for UK law enforcement to receive Ultimate Beneficial Owner (UBO) information from overseas territories and Crown Dependencies within 24 hours of the request. Such a step would answer the growing demand for fast and transparent access to UBO information, which was also outlined as highly recommended by a number of authorities. On a regional level, the implementation of the 4th EU Money Laundering Directive is the most important upgrade to the EU legislative measures

"The development of technologies has been the biggest driver for change in financial crime; fraud has now become the most commonly experienced offence."

Nick Parfitt, C6 Intelligence

to tackle money laundering and terrorism financing. Another key piece of legislation is the EU General Data Protection Regulation (GDPR) which will be enforceable from 25 May 2018. Companies need to understand the changes and complexity in the regulatory environment. Sources of information and profiles are growing proportionately. In order for companies to operate under heightened scrutiny, they need to consider due diligence and compliance procedures as part of their normal analytics cycle. Ultimately, prevention works better than investigating crime after it has happened.

R&C: What steps should companies take to ensure adequate processes, and other programmes and policies, are in place to address financial crime? How important is the role of senior executives in driving such initiatives forward?

Parfitt: This is very much a board-affecting issue. We only need to look back as far as the Habib Bank settlement of $225m expecting to negatively impact earnings per share by 67 percent for failure to have adequate anti-money laundering infrastructure, to highlight the impact of failure to appropriately develop and apply processes and policies. These shareholder-impacting consequences, which are a familiar feature of mainstream news, not only adversely affect the balance sheet in the short term but, long term, affect the reputation of the organisation. This is a combination of organisations strengthening their existing defences, in addition to the broadening of regulated industries; virtual currencies, pre-paid cards, online gaming services and money remitters.

R&C: In what ways can companies utilise technology to help manage risks arising from financial crime? How would you characterise the attitude companies generally have toward their exposure to financial crime and the technology they utilise to manage it?

Parfitt: Effective and efficient compliance should be delivered through a combination of technology and human intelligence, the task is simply too vast for a people-based solution alone, but current technology is not yet sophisticated enough for the nuances of adverse media searches to be relied upon in their entirety. There is not yet a 'unicorn' technology platform that cures all compliance's ills, so a multi-layered approach is the most effective defence.

R&C: When utilising programmes as part of an anti-financial crime strategy, what benefits might companies derive from a combination of in-house and outsourced resources to manage the risks?

Parfitt: There are a number of clear benefits of using a combination of in-house and outsourced resources, including the availability of resources to help to manage workloads through peaks and troughs, reducing costs by outsourcing specific tasks that require a level of specialist expertise, sharing of best practices and access to third-party data providers through partners.

R&C: What overall advice would you give to organisations in terms of marrying technology with protocols so as to enhance the efficiency of their anti-financial crime capabilities and allow them to detect unusual behaviour and identify red flags?

Parfitt: Prevention is better than a cure. Developing a robust and consistent 'know your client' process that can be replicated and repeated frequently with minimal operational resource is key. This allows organisations to focus on specific changed activity, rather than arbitrary interval-based checks which are inefficient and ineffective.

R&C: Going forward, do you expect the risks posed by financial crime to increase over time? Do companies need to ensure they are prepared to deal with existing and emerging threats?

Parfitt: Regulation and control always follow the crime event; therefore, we will always be behind the curve. The trick is in not falling too far behind. Emerging payment methods, such as Bitcoin, which may facilitate financial crime, are on the rise. The importance of data privacy and the impact this has on the ability to collect and process data is crucial to avoiding financial cyber crime. With the fragmentation of geopolitical environments, the uncertainty of the EU and the UK post-Brexit where member states may be motivated to ease trade controls to support their economy, these are challenging times; organisations need to be set for continual change and evolution. R&C