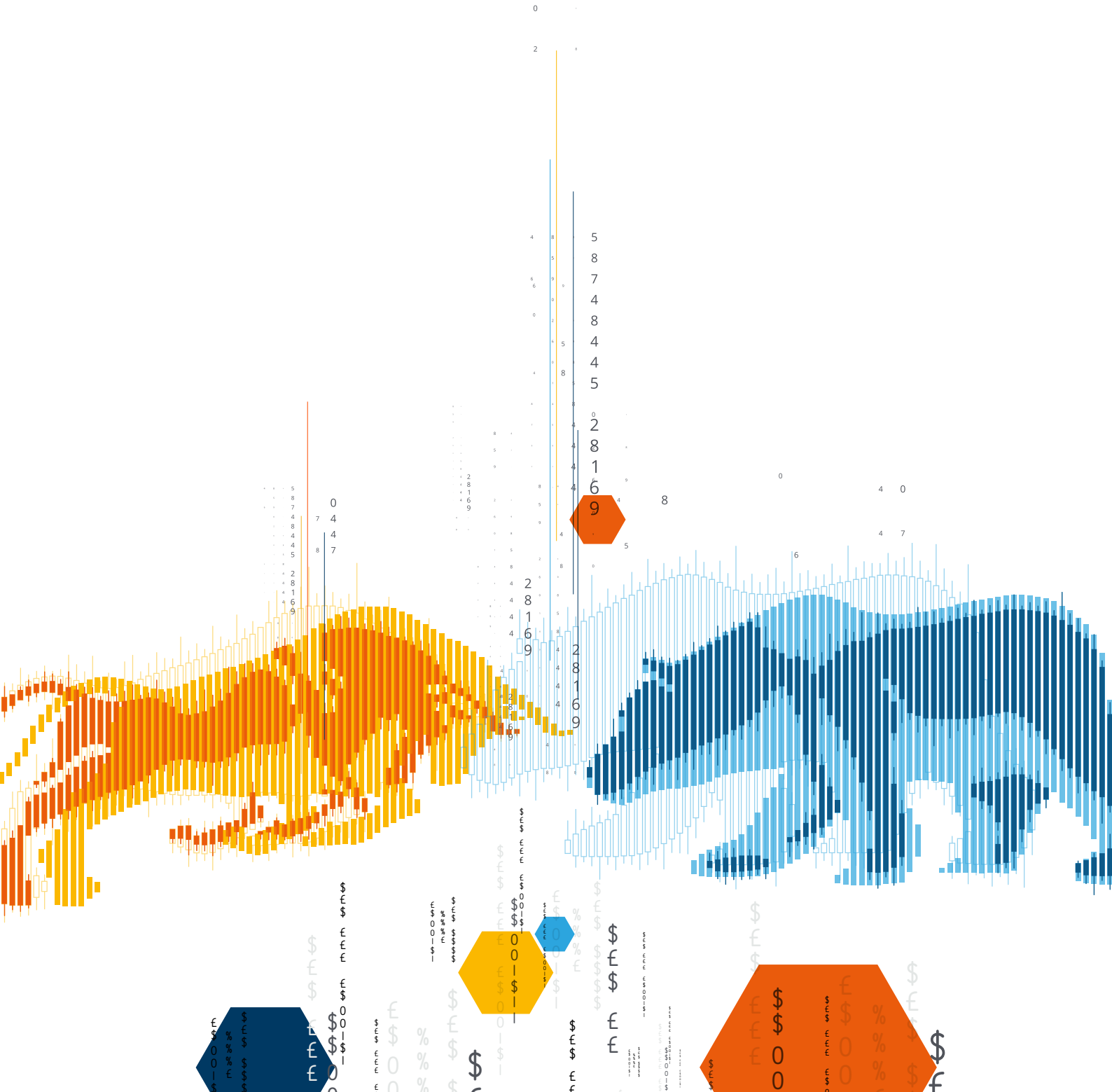
BAE SYSTEMS

Money Laundering in Financial Markets



Investment banks face a multitude of risks – not least countering the threat from money launderers. Gary Kalish examines how regulators, policymakers and financial institutions can together deliver a strong digital defence.

Anti-money laundering measures remain a key priority for regulators, governments and financial institutions worldwide. In 2019, G20 leaders used their meeting in Osaka, for example, to formally agree the adoption of new cryptocurrency guidelines[1] and the UK's Financial Conduct Authority (FCA) has also recently published their thematic review on money laundering in capital markets.[2]

The trouble is, mitigating the risk of financial crime is easier said than done – particularly in the digital age. Although technology has propelled customer innovations such as online banking and faster payments, it has also carved out new opportunities for those with more nefarious ambitions.

This is a particular challenge for banks operating in the financial markets space. Their vulnerability to money laundering is rooted in the array of large and complex financial transactions they oversee, which – while potentially lucrative – also opens up a myriad of risks. Under local regulation and legislation in the UK, firms have a legal requirement to ensure their systems and controls can counter the threat of financial crime. But are such systems fit for purpose?

Fighting financial crime

Let's take a look at how capital markets organisations seek to prevent financial crime – in theory at least, it starts from the top. Leadership needs to ensure that compliance is a core aspect of their organisation's DNA and that colleagues are aware of all the relevant policies and procedures.

Of equal importance is the need to stay pro-active – organisations must always be looking for new ways to mitigate the threats they face.

However, it's far from straightforward. Such is the scale and complexity of their operations, financial markets organisations may struggle to have visibility of exactly what is occurring, and the controls they have in place may only mitigate some of the risks they face. And even with the various controls that firms may have implemented, criminals are aware of this so will create structures and work through brokers in order to obfuscate the true source of their funds.

The operational complexity helps explain why financial markets organisations tend not to have a centralised unit focused on investigating suspicious activity – financial crime, market abuse or insider dealing – and instead have different teams operating often in isolation from each other. This is because they view market abuse and the threat from insider dealing through different regulatory lenses, rather than seeing it as the single phenomena of financial crime.

Can more be done to help bring them together?

Bridging the gap

A closer working environment would strengthen communication by allowing the sharing of knowledge, information and relevant system access. Combining teams facilitates a more holistic view, which can combat not just insider dealing and money laundering, but economic crime itself – similar to how some organisations are reviewing how they address the link between cyber, fraud and financial crime. This chimes with the points raised within the recent FCA thematic review,[3] as well as starting to align with the UK's Economic Crime Strategic Board's Economic Crime Plan.[4]

But it's not all down to the banks themselves. Government organisations, too, have a role to play. For example, they could consider a single utility to consolidate and analyse the relevant information submitted from market participants and organisations in order to identify all acts of economic crime, such as the reports of potential suspicion relating to money laundering and/ or market abuse and insider dealing. Moving further towards a more intelligence-led approach, one that takes into account the information available through the current AML teams and separately the teams investigating potential market abuse and insider dealing.

Time to team

Money laundering within financial markets isn't going away. But while its invidious presence will always haunt the global financial system, by working together, regulators, governments and financial institutions can all play a part in minimising the threat.

About the author

Gary Kalish is a Senior Financial Crime Prevention Consultant at BAE Systems Applied Intelligence

gary.kalish@baesystems.com

How we can help

Address the technological problem

Financial institutions must develop and maintain a comprehensive understanding of the monitoring and surveillance rules that various teams and parts of their organisations have in place, and where they may overlap. A thematic review, either in-house or with the help of our own consultants, can help. Also consider something along the lines of NetReveal® Rule Optimisation or Advanced Analytics Platform.

Bring together systems and processes

Understand how Suspicious Activity Reports are raised within your business, and how teams are able to make use of them. Conducting a case management review will show gaps in the system, and also build the case for a more holistic case management system that combines data and intelligence from across different parts of the business. Take a look at our Netreveal® Enterprise Case Management solution or talk to our consultants about how we can review and improve your teams' performance.

[1] https://www.zdnet.com/article/g20-supports-guidelines-to-make-cryptocurrency-exchanges-hand-over-user-data/

[2,3] https://www.fca.org.uk/publication/thematic-reviews/tr19-004.pdf

[4] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 85,800 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/financialmarkets

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai