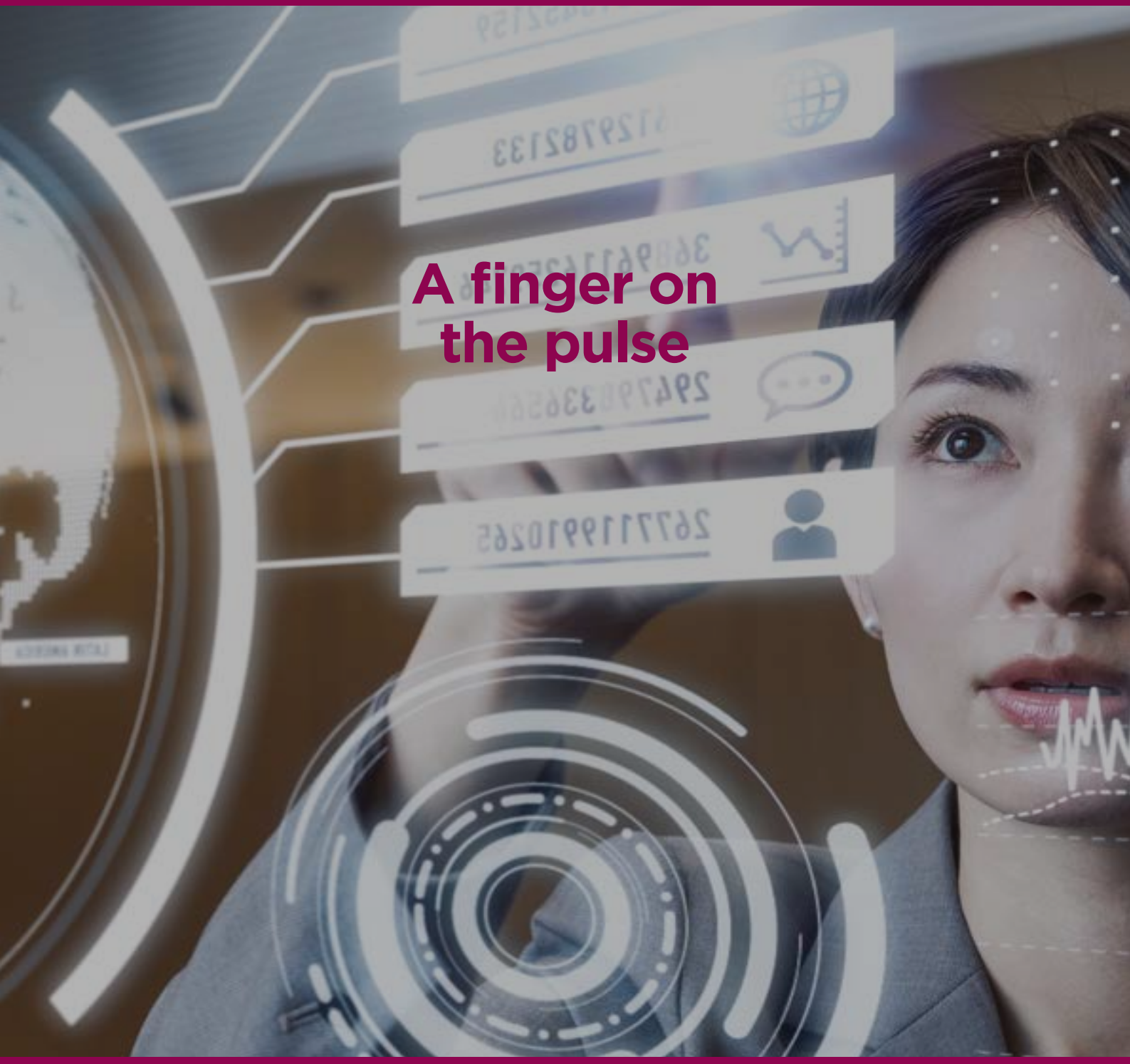
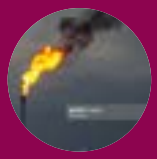
ISSUE 54

inCOMPLIANCE®

YOUR MAGAZINE FROM THE INTERNATIONAL COMPLIANCE ASSOCIATION



A finger on the pulse



p.13

Time to wake up

p.16

In the frame

p.24

At the leading edge

Celebrating 20 years
ICA
INTERNATIONAL COMPLIANCE ASSOCIATION

£4.95 where sold separately

A finger on the pulse

Joby Carpenter highlights the importance of adopting an intelligence-led approach to financial crime compliance

For nearly 20 years I worked for various public sector agencies helping others to better understand the nature of financial crime threats to the UK, its institutions and citizens. Working closely with law enforcement, security agencies, international regulators and prosecutors, we highlighted the threats posed by criminals, nation states and malicious actors who repeatedly tested our resilience by adopting innovative methods and schemes.

My belief is that an intelligence-led approach can also be deployed by financial crime compliance (FCC) professionals, moving away from a 'tick-box' approach to compliance whilst helping to manage legal, regulatory and reputational risks, with some assistance from the authorities. Organisations are realising they don't only need to meet regulatory requirements, they also need to have a finger on the pulse of financial crime to satisfy the increasing demand for firms to adopt a proactive stance in the face of the exponential growth in financial crime.

Use of intelligence can enable financial institutions to demonstrate a better understanding of their risk assessment

What intelligence tells us

If you are implementing change in your organisation, it is crucial to maintain a diligent overview of risks and threats. Threat is best understood as being informed by intelligence, without which we cannot understand the severity of associated risks. Perceptive use of intelligence can enable financial institutions to demonstrate a better understanding of their risk assessment and better implement its findings. It is worth summarising what all-source intelligence tells us about financial crime:

- Correspondent banking and personal accounts (including those used by money mule networks) continue to be abused by criminals using innovative techniques
- Mirror trading schemes and laundromats involving the abuse of non-resident accounts demonstrate the scale at which wholesale markets are exploited by money laundering networks, and the variety of approaches used
- Our understanding of the extent to which smaller, regulated firms (e.g. brokerages, 'contracts for difference' firms, hedge funds and wealth managers) facilitate harmful forms of financial crime is improving, but investigations and prosecutions remain rare
- The payments and FinTech sectors risk being criminally abused on a vast scale without adequate control frameworks or supervision, although multiple red flags exist to identify illicit activity
- The money laundering risk posed by cryptoassets is decreasing in proportion to its uptake amongst legitimate users, but a new generation of cryptoassets with enhanced levels of security and anonymity is creating new risks
- Corporate structures and the service providers that create them remain a recurring feature in complex money laundering schemes, and recent legislative changes only partially mitigate this
- The regulated perimeter is deliberately targeted by criminals who target third parties and sectors to evade detection (e.g. trade finance instruments)
- COVID-19's biggest impact on financial crime has been to accelerate the digitalisation of money laundering methods, corresponding to the mass growth in technology such as third-party payments
- International financial centres and offshore jurisdictions sit at the centre of illicit financial flows from high-risk jurisdictions, despite established regulatory systems.

Making sense of the threat picture

Money laundering, terrorist financing and sanctions evasion generate significant illicit funds and cause great harm, and authorities increasingly expect financial institutions to act proactively against these threats. For decades threat intelligence has been the preserve of intelligence agencies and government policymakers. Whilst threat intelligence is produced and acted upon by law enforcement and (some) regulatory bodies, it has taken longer to bed into the private sector.

Unfortunately, intelligence sharing, above and beyond a small number of firms involved in public-private partnerships (PPP), remains limited. This is beginning to register as ►

revelations (often identified by whistleblowers and investigative journalists) have led some banks to conclude that they need to make sense of the threat picture. A small number of firms are acting as thought leaders in this regard and see the advantages of incorporating intelligence into their decision making through the practical application of typologies, red flags, horizon scanning and so forth.

With the focus of the 6th Anti-Money Laundering Directive (6AMLD) on predicate offences (e.g. international corruption, human trafficking and environmental crime etc), firms are being asked to consider their exposure to these threats and build findings into their risk assessments. This also fits with a stated desire from law enforcement to reduce harmful criminality through improved reporting of suspicion, which must start with understanding the threat. Some regulators, such as AUSTRAC (the Australian Transaction Reports and Analysis Centre), are leading the way in this regard, sharing intelligence regarding high-priority harms with regulated firms.

Building a map

Undertaking a mapping exercise to build a matrix of threats, vulnerabilities and intelligence gaps is a critical piece of this jigsaw. The strategic intelligence picture which emerges can inform critical processes such as transaction monitoring, customer due diligence/know your customer (CDD/KYC) and wider systems and controls. Benefits include:

- Scoring, evaluating and prioritising crime types and money laundering methods
- Identifying and analysing modus operandi of illicit actors
- Understanding the materiality of the threat
- Enhancing control frameworks to manage financial crime risks.

A focus on joining the dots between intelligence, emerging threats, and vulnerabilities helps to ensure this information is built into FCC frameworks. Meanwhile, closer collaboration between lines of defence ensures that risk management and policy making are better aligned ►

and inform a firm's risk appetite statement. How so?

- The first line of defence (1LOD) and/or second line (2LOD) identify requirements
- Policy (generally compliance) considers risk and requirements, passed to 1LOD to implement (as part of broader CDD controls)
- Both lines work together to ensure risks are dealt with effectively (including implementing risk-based controls, escalations and suspicious activity reports)
- Where a three lines of defence model is in place, the 2LOD provides oversight to the 1LOD to ensure effective implementation whilst the third line (audit; 3LOD) provides assurance to the management board on effective implementation
- Freed up resources 'connect the dots' to support effective implementation of systems and controls.

A total stakeholder perspective

Designing and implementing a risk management framework requires a total stakeholder perspective, including views from frontline staff, product experts, policy, audit, risk and compliance. Each stakeholder can inform the likelihood of an adverse impact to the organisation and be a powerful force for mitigating risk. Threat intelligence can be a frame of reference to enable follow-up activity, including account monitoring and suspicious activity reporting, helping to meet regulatory and law enforcement expectations.

A variety of proprietary information, subscription services, advanced analytics, publicly-available data sources, media reporting, academic papers, regulatory notices, law enforcement press releases and court proceedings can assist MLROs to present findings to the management board. Open-source intelligence drives knowledge of real-time developments (aligned to business risk), relevant to implementing an effective control framework from the C-Suite down.

Ensuring intelligence assessments have a firm 'terms of reference' allows them to provide what MLROs require (i.e. to inform safeguards to enhance an AML framework). Approaching an issue from a strategic perspective can challenge deeply-held assumptions (i.e. inherent risk factors). An inclusive approach to intelligence development is not just a 'nice to have' but helps identify opportunities to reduce residual risk (e.g. leading to productive cooperation with law enforcement or a PPP). Any concern about the cost of implementing such an approach misses the potential for a more effective, efficient and intelligence-led deployment of resources.

MLROs can commission new research to fill gaps allowing them to focus on business as usual. Updating threat assessments on a rolling basis enables higher quality financial crime reporting and improved awareness at 1LOD and Board level through training and briefings. This approach questions conventional assumptions and allows a deeper understanding of the threat picture, helping to put in place more resilient mitigations.

A more dynamic approach

The private sector has more in common with its public sector intelligence counterparts than we commonly think but, despite steps forward, such as PPP, there remains little direct sharing of threat intelligence that would allow firms to pivot effectively to tackle evolving threats. However, solutions can be employed to deliver a range of benefits, including:

- Understanding new and evolving financial crime threats and money laundering methods (as per 6AMLD requirements)
- Informing business-wide risk identification and priority setting
- Factoring intelligence into systems and controls
- Highlighting follow-up activity, including reporting suspicion
- Identifying emerging criminal threats for ongoing monitoring
- Supplementing groupwide intelligence gaps to tackle regulatory concerns
- Enhancing liaison, ensuring that risk management and policy making are better aligned.

To date these benefits are largely restricted to a small group of banks. However, with support from policymakers, such as the Financial Action Task Force (FATF), and local supervisors working together with industry, an intelligence-led approach could drive a more dynamic approach to CDD and transaction monitoring. My view is that, with a degree of consideration, firms can commission bespoke pieces of analysis that will help move away from a 'tick-box' culture and address multiple risks in a way familiar to regulators and intelligence agencies. By instigating such a culture firms show that they wish to be financial crime subject matter experts in the same way they are compliance experts – working like intelligence professionals to understand the threat, whilst potentially avoiding regulatory scrutiny and financial punishment.

Joby Carpenter is a Senior Manager with Plenitude Consulting with over 18 years of experience and expertise in policy making, critical thinking and threat and risk analysis across the Government, intelligence and regulatory community

1. See the recent speech 'Imperatives for the New Decade' by John Cusack, Chair of the Global Coalition to Fight Financial Crime, which highlights the link between effective FCC and reducing harm https://www.gcffc.org/wp-content/uploads/2021/06/Speech-Imperatives-for-the-New-Decade.pdf
2. Such as the Joint Money Laundering Intelligence Taskforce (JMLIT) in the UK or FINTEL Alliance in Australia.
3. Examples of breaking news being quickly and effectively incorporated into a firm's risk assessment and systems and controls include Panama Papers, the FinCen files, laundromat exposés and revelations around new technology.