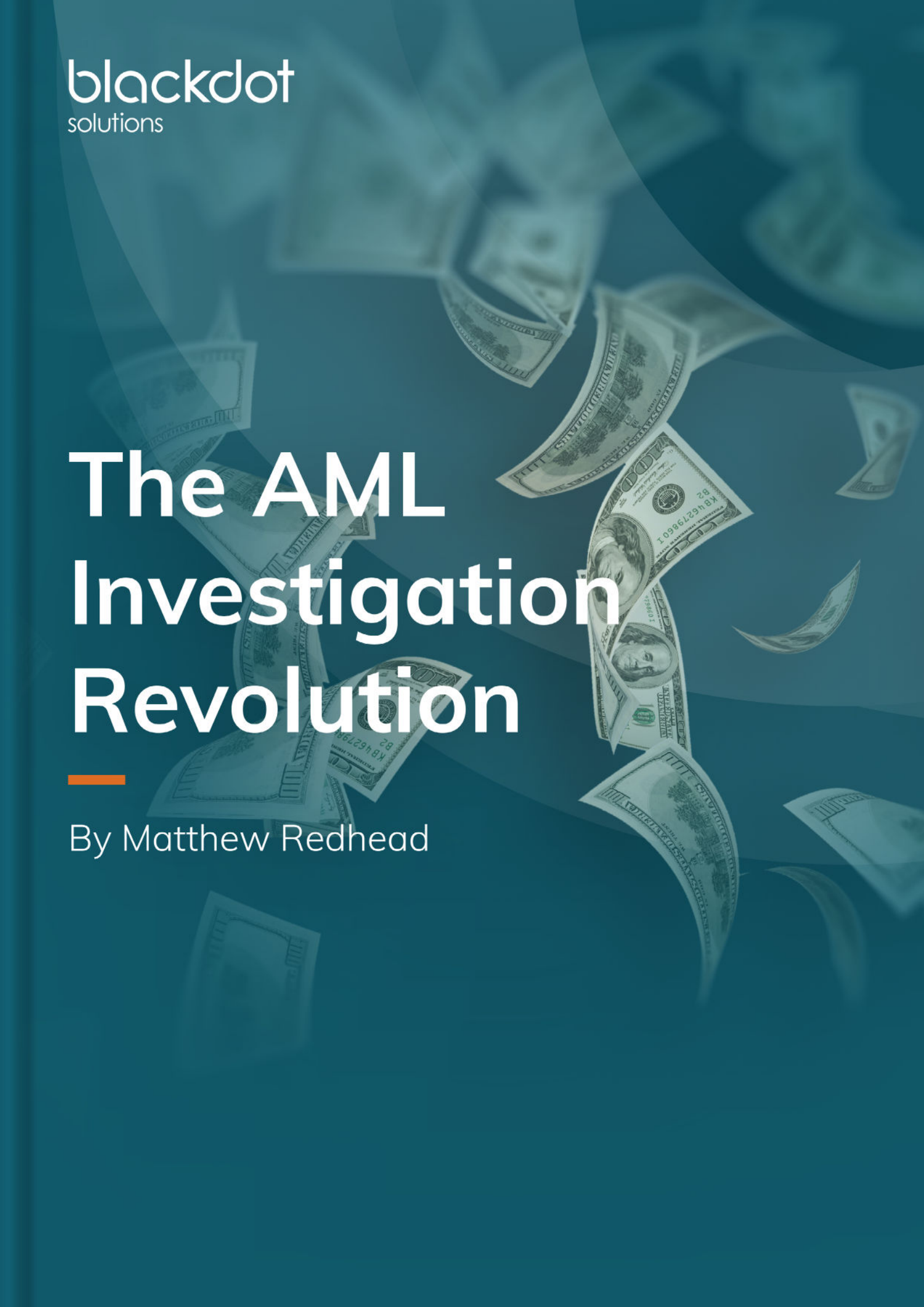
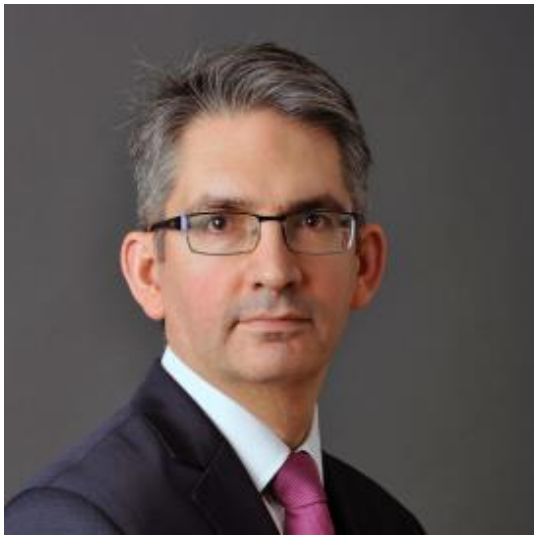
blackdot
solutions



The AML Investigation Revolution

By Matthew Redhead

ABOUT MATTHEW REDHEAD



Matthew Redhead is an independent risk consultant to the FinTech and RegTech sectors, and an Associate Fellow at the Royal United Services Institute. He is also a regular contributor to Jane's Intelligence Review on serious organised crime, financial crime, terrorism and intelligence. He has extensive experience in financial services, having trained as a 'front office' banker and worked in various senior roles in financial crime risk functions. He has previously served as a government official at the MoD, and on secondment at the Office of Security and Counter-Terrorism (OSCT) at the Home Office.

EXECUTIVE SUMMARY

- *Financial Services and AML.* Under global Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) rules, the obligation to identify suspicious activity sits firmly with the private sector, and primarily with financial institutions (FIs).

- *The Problem with Compliance.* For three decades, the AML model has been compliance-based, with automated processes producing alerts that undergo mostly cursory investigative checks. But AML practitioners are beginning to recognise the inadequacy of this approach.

- *Emerging Alternatives.* FIs are leading the way, taking 'intelligence' and 'investigator-led' models from national security and policing, and augmenting their old AML frameworks into a more risk-focused model.

- *The Investigation-Led Model.* The trend in AML is running strongly away from compliance-based processes, towards a more reflexive, responsive and agile approach. Over time, the use of sophisticated investigation techniques is likely to become dominant in AML/CFT.

- *Inadequate Legacy Methods.* FIs need to be prepared for this, but in many cases are not. Common current tools of investigation are often simplistic and fragmented. The use of crude keyword searches on the internet or internal systems are still common.

- *Deploying Technology with Intelligence.* Fortunately, better ways are available. Social network analytics enriched with curated data can create integrated intelligence platforms, in which investigators can collate, analyse and assess data all in one place.

- *'One-Stop Shops' for Investigation.* The most advanced of these platforms allow FIs to combine their own internal data streams with carefully curated open source materials in secure and accessible environments.

- *Better Outcomes and Business Benefits.* For those FIs that have already begun their own 'AML Investigator Revolution', the benefits - better investigative outcomes, with increased speed and reduced costs - are already apparent.

INTRODUCTION

In September 2020, a consortia of media outlets released thousands of US Suspicious Activity Reports (SARs) into the public domain. These reports revealed secret financial crime leads sent by US Financial Institutions (FIs) to the Financial Crimes Enforcement Network (FinCEN), the US national Financial Intelligence Unit (FIU). Known in the media as the 'FinCEN Files', they show a global Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) framework struggling to tackle financial crime.

As many AML compliance practitioners admit, the vast majority of SARs produced remain of relatively low-quality, and have little impact on the scale or impact of money laundering, or other financial and economic crimes. While such crimes are typically fluid and complex phenomena, with criminals regularly mixing and matching modus operandi to avoid detection, the private sector has approached the problem in a wholly ineffective way, worried more about failing to meet the requirements of regulatory compliance, or controlling costs, than disrupting criminality. Approaches to AML/CFT have therefore invariably been slow and bureaucratic, with crude, automated monitoring and scanning systems as the centrepiece of many FIs' frameworks.

Over the last five years or so, however, an alternative approach to AML/CFT has begun to emerge within the industry, encouraged by an influx of skills from those parts of the public sector - the military, intelligence and law enforcement - focused on taking a proactive approach against opponents. This change in culture has encouraged a greater focus on underlying criminal risks and threats, the collation and exploitation of financial intelligence, and the integration of analysis and assessment in key functions. What we are seeing, slowly but surely, is the emergence of a risk management rather than compliance-led AML/CFT model.

Sitting at the centre of this is the AML/CFT investigator, undertaking the whole range of intelligence collection and investigative tasks. At present, this currently entails using multiple separate platforms and data streams, open source and otherwise. Walking around Financial Crime Compliance and Financial Crime Risk Management (FCC/FCRM) functions in major FIs, it is not unusual to see investigators' desks cluttered with multiple standalone platforms and separate screens. AML investigation, while increasingly important to successful AML execution, continues to be impeded by a fragmented approach that allows unnecessary frictions to persist.

But there are solutions. Platforms based on the concept of 'Intelligent Automation', often already in deployment in national security and law enforcement agencies, create integrated environments which bring together not only sophisticated network analytics, but a range of carefully curated internal, proprietary and open sources. Unlike many investigatory frameworks in FIs, they reduce - and in some cases eliminate - the need to juggle between systems. They put the right material in front of the investigator, at the right time, leading to better casework, better decision-making and better outcomes. They are the obvious next step in the 'AML Investigation Revolution.'

THE PROBLEM WITH COMPLIANCE

The global AML/CFT system, created by the G7's International standard-setter, the Financial Action Task Force (FATF), is now thirty years old. Within that system, FIs and other obligated sectors are expected to undertake two essential roles, which have translated in practice into a multitude of internal policies, procedures and controls:

- *Preventing Financial Crime:* using Client Due Diligence (CDD) and Know Your Customer (KYC) provisions to prevent criminals getting 'through the door', and transaction monitoring and screening to identify their activities if they do.
- *Recording and Reporting Suspicious Activity:* maintaining client data for set period, and reviewing any instances of unusual or inconsistent client behaviour for indications of possible illicit activity to be reported to the authorities.

Investigation should play a key part in bridging these two responsibilities, with investigators acting as the connection between detecting risk and acting upon it:

- In **AML/CFT,** undertaking detailed investigation and making decisions on internal referrals about the future of the relationship, Enhanced Due Diligence (EDD) or issuing SARs.
- In **Sanctions**, clarifying whether there has been a 'true match', but also identifying potential wider network risks from counterpart relationships for external reporting and internal reviews of client relationship management.
- In **Fraud**, dealing with a range of alerts, making decisions on client refunds and the need for fraud-based SARs

However, as AML/CFT and financial crime structures have evolved since 1990, the position of investigators has become increasingly subordinate, with investigatory teams treated as support staff assigned to handle the output of automated systems, rather than key decision-makers in their own right. Much of this is driven by the low quality of alerts that investigators receive - around 90% according to be 'False Positives' according to most estimates - but investigators are also hindered by the low quality of investigatory tools to hand. Poor material and inadequate technology can in turn generate a 'throughput mentality' amongst investigators, where the focus is less on quality of investigation, but on ensuring that volume-based targets have been met.

Although these are not the only problems that the AML/CFT regime faces, they are amongst the major causes of the high proportion of low value SARs produced by FIs. This leads to a situation where FIs and their investigators are making a marginal difference in the fight against financial crime, with officials consistently reporting the majority of such reports to be of no immediate use to Law Enforcement Agencies (LEAs). In 2017, Europol, the EU's policing agency, suggested the proportion of unused reports by member states' agencies was an astonishing 90%.

THE INVESTIGATION REVOLUTION

In the face of these kinds of statistics, there has been an ongoing debate in the financial services industry about how best to respond - whether to stick with the familiar compliance-based approaches or switch to an alternative. For those who have faced significant regulatory censure and Deferred Prosecution Agreements (DPAs), change has been the only option. In response, some have opted to more heavily automate pre-existing controls in order to cut down costs. But even the more efficient legacy AML/CFT platforms – Transaction Monitoring (TM), Sanctions Screening and the like – although important, remain extremely crude ways to identify and develop financial crime risks or indicators of concern, however fast they work.

In contrast, several global FIs have experimented with more radical strategies, looking to examples from other sectors with stronger track records in risk detection and management. An influx of talent from the worlds of national security, law enforcement and the military have thus brought different kinds of thinking into the AML/CFT space, challenging pre-existing assumptions, and placing intelligence and investigation more firmly at the centre of the private sector response. This shift has taken different forms:

- *Risk Focus:* Whereas legacy investigation approaches were largely undifferentiated and non-prioritised, investigations have become focused on key financial crime risk areas of societal concern, such as Human Trafficking.
- *Professionalisation:* Pre-existing AML/CFT investigation teams have developed more rigorous approaches to investigation practice and doctrine, supported by external training from consultancies and former law enforcement and intelligence officers.
- *Integration:* Teams looking at different types of financial crime risk - AML, fraud, sanctions, Anti-bribery and Corruption (ABC) - have integrated their investigatory capabilities to cross-fertilise knowledge and improve performance.
- *Feedback:* Investigatory teams have increasingly become key stakeholders in the process of platform optimisation - they are helping those who set the parameters on legacy controls refine what they are looking for, based on evolving casework.
- *Expansion:* New investigatory teams, such as internal Financial Intelligence Units (FIUs), have been created to mount longer-term monitoring and investigation of risks at strategic, operational and tactical levels - affecting decision-making from the FI's exposure to individual companies through to entire jurisdictions.

These developments have been supported and further encouraged, moreover, by the growth of investigatory collaboration between the public and private sectors in Financial Intelligence Sharing Partnerships (FISPs). Projects such as the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) have brought together investigators from state agencies and FIs to share key leads and strategic intelligence, and the effects – though modest so far – have been encouraging. Between February 2015 and June 2020, for example, JMLIT supported 750 cases, with a result that £56 million of previously undetected illicit assets were seized or restrained. The pandemic has driven this agenda further forward, with the development of co-located investigatory 'fusion cells' between law enforcement and FIs to fight COVID-19-related fraud together. The perceived success of these projects suggests that investigative collaboration between the sectors will only grow over time, making investigation an ever more important aspect of the AML/CFT effort. This will gain further impetus, moreover, as countries look to expand the legal grounds for sharing AML investigatory material within the private sector prior to suspicious activity reporting, with the introduction of legal 'safe harbours', such as the US's PATRIOT Act Section 314 (b), to allow and promote investigative collaboration between FIs in order to identify and mitigate AML/CFT risks. Taken together, these trends demonstrate that investigations, as the foundations of

AML collaboration, are moving toward centre-stage in the world of financial crime, and there is every reason to think this will continue, as the benefits grow.

FINANCIAL SERVICES ARE NOT READY

This year, over 570,000 SARs have been received by the authorities in the UK alone, suggesting that thousands, and possibly tens of thousands, of AML/CFT or other financial crime investigations happen every single month within FIs. As noted above, their quality can vary widely, in many instances because FIs are not working with optimal tools or intelligence sources. It is not unknown for FIs to still be using common word processing and spreadsheets applications to collate, store and analyse customer behaviour, or first-generation Social Network Analysis (SNA) platforms to try and identify key transactional relationships. Investigators are also expected to work their way through a range of different and disconnected sources, both internal and external, to collate material for their casework. These sources typically include:

- *Customer Relationship Management (CRM)* systems: to collate detailed CDD/KYC data.
- *Case Management Systems (CMS):* to collate relevant case notes from other investigatory teams.
- *Internal SAR Databases:* to collate past risk reporting on a current case.
- *Vendor Databases:* to collate information stored in sanctions, adverse media and other vendor tools used by other teams during due diligence processes.
- *The Internet:* to collate information Open-Source Intelligence (OSINT) to enrich and expand upon internally available material.

Access to the different sources can vary between and within FIs, with investigators even within the same institution having uneven access to such sources, due to internal permissions management and licensing agreements with outside vendors. But there are also the significant challenges with ensuring that investigators are getting the right kind of contextual intelligence, delivered in a way designed to support robust investigatory outcomes. A common set of problems for investigators in FIs include:

- *Quantity of Intelligence:* This is a matter of either feast or famine, especially with regard to OSINT.
- *Quality of Intelligence:* The provenance and reliability of material is often hard to assess, and leads to extended and often fruitless efforts to corroborate information.
- *Consistency of Intelligence:* Open-source searches on the Internet, for example, will often produce results that vary depending on location and past user history, or on what online vendors might be seeking to sell.It is worth remembering that the internet is not designed to help investigators find information.
- *Security of Investigations:* Some investigations can also leave potentially glaring online footprints on more sensitive sites such as social media platforms.

The proliferation of separate data sources and intelligence streams can add further friction to the investigative process, as investigators switch between multiple separate platforms to collate and analyse material. This not only slows down the process of investigation, but also creates the room for mistakes and potential missed connections that will undermine the value of the final assessment product produced by the investigator. This ‘multiple system’ approach also makes the process of investigation more difficult to record, manage and ultimately audit.

GETTING PREPARED

The presence of experienced and well-trained investigators can help mitigate some of these problems, but even the best investigator needs to be equipped with the right data and tools. The key - as already identified in national security and law enforcement agencies - is what has become known as 'Intelligent Automation' where investigators are placed at the centre of seamless and carefully-curated intelligence environments. These environments make the collation, analysis and assessment of material as frictionless as possible, by:

- *Creating a Panoramic View.* Rather than pursuing multiple strands of intelligence on diverse platforms, investigators can work through a primary platform that brings together the right kind of intelligence – internal and external – in a single space in the shortest time possible.
- *Taming the Intelligence Deluge*. Instead of chasing down myriad disparate sources from scratch, Augmented Intelligence allows an investigator to start from a robust foundation of carefully curated material.
- *Taking a Structured Approach*. It can be easy for investigators to become unstuck and unstructured in their investigations as they move across different sources. Having a clearly structured dashboard of options can encourage a more systematic approach.
- *Augmenting Thinking.* No investigator is infallible, and it is easy to miss helpful links. Increasingly, Augmented Intelligence environments are able to highlight potential connections that might not be immediately obvious to the human eye, leaving the investigator to make the decision on whether the link has significance.
- *Nurturing Real-time Analysis.* Collating and analysing intelligence can be a 'stop-go', process, result in disconnected thinking, especially in complex investigations. In contrast, integrated intelligence environments allow investigators to analyse material and record their judgements in a connected form as they go.

ASSESSING THE BENEFITS

As recent research has suggested, the use of Intelligent Automation is already paying investigative dividends in defence and security institutions. Such environments greatly improve investigations by streamlining the process, reducing blockages and preventing investigators from becoming overwhelmed by a torrent of irrelevant data. Translated to an AML/CFT environment, this has obvious positive implications in terms not only of effectiveness - that is to say better investigations and outcomes - but also increased efficiency. Integrated investigations are likely to be quicker than a more fragmented alternative, bringing better Value for Money, while also being much less likely to return the wrong investigative finding. They can also be excellent ways of demonstrating to regulators that an FI has taken a risk-based attitude, and exercised their obligations with an eye to necessity and proportionality - not words typically used for the performance of platforms in AML/CFT. They are a world away from the volume and process driven approach so familiar today.

CONCLUSION

The decisions made by AML/CFT investigators within FIs are extremely significant, and can have an impact on law enforcement decisions or the future of a customer relationship. If genuinely suspicious activity is missed due to poor investigative practice or inadequate tools, then a crime that might otherwise have been detected and disrupted will be allowed to proceed. Having the best investigative tools to hand enables businesses to make these kinds of risk-based decisions with confidence. At the same time, similar failings could lead to an innocent person being treated as a subject of concern, raising issues of fairness and having implications for financial inclusion. Whether the investigator gets it right or wrong will have a major effect. The outcome of every investigation can move the needle a little bit the right way – or the wrong way - and, in combination, can make a major difference to how well an FI tackles financial crime and protects its customers.

Despite the ubiquity of the compliance-led approach to AML/CFT, it has a poor record when it comes to delivering positive outcomes - disrupting financial crimes and reducing illicit flows. Investigator-led approaches, using augmented and integrated intelligence environments, have a better record of success against high profile risks, such as countering terrorism. Their deployment within the financial services sector for AML/CFT, though still nascent, are already beginning to show fruit, especially when allied with closer cooperation across firms and sectors. As AML/CFT practitioners focus-in increasingly on delivering genuine financial intelligence value, it seems obvious that empowering the investigator is the right way to go.