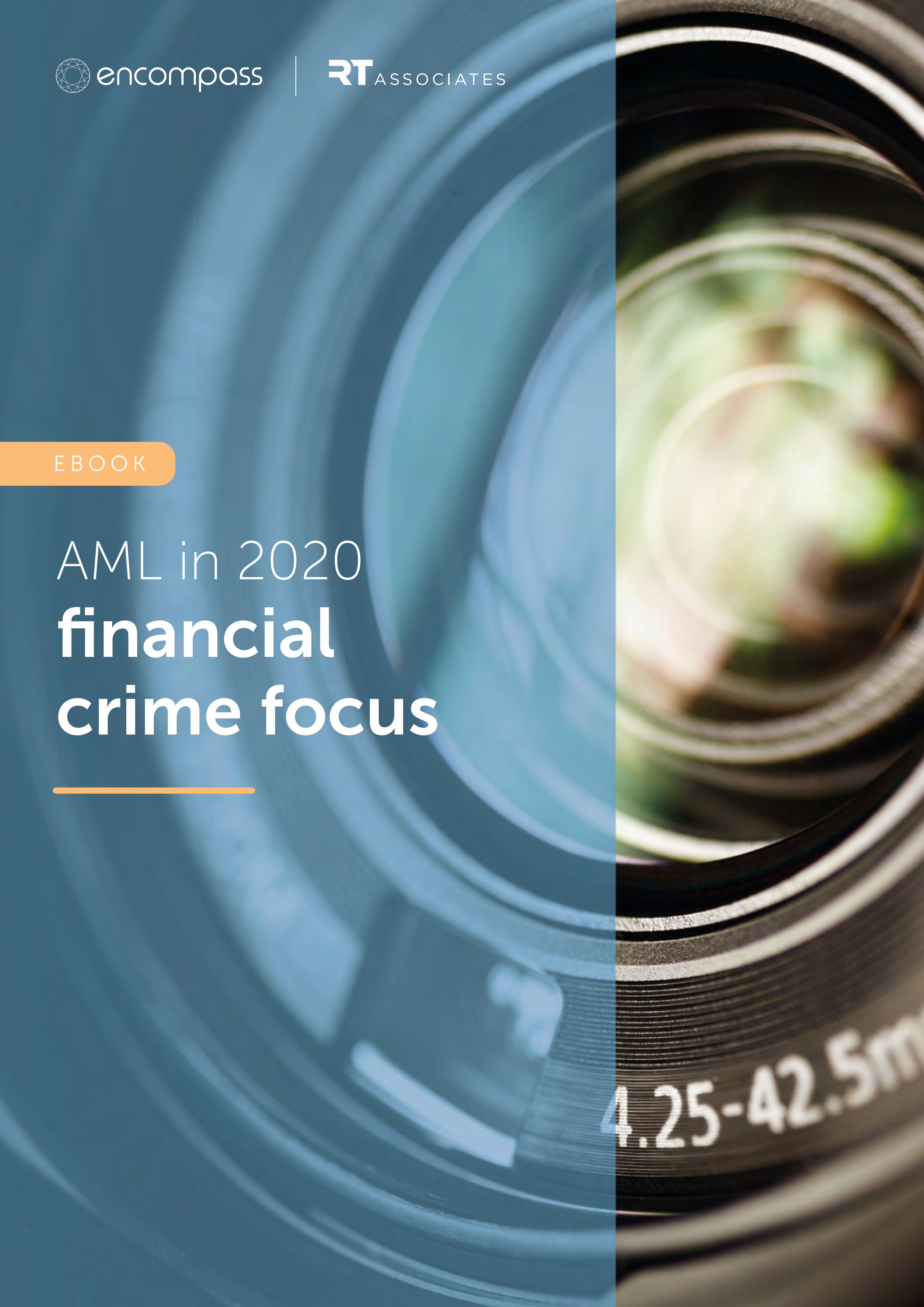
EBOOK

AML in 2020 financial crime focus



about **Dr Sian Lewin**

Co-Founder and Head of Client Delivery Director at RegTech Associates

At RegTech Associates, Sian works with technology clients to help them refine, grow and scale their RegTech products and companies and with regulated firms to ensure they select the solutions that meet their regulatory needs. She leads the research and content generation activities. Sian is a recognised expert and influencer in RegTech and financial regulation and was featured on the Innovate Finance Women in FinTech Powerlist of 2018.

Prior to joining RegTech Associates, she was awarded a PhD from the London School of Economics. Her systematic research explored the challenges faced by banks in dealing with the volume and speed of regulatory change following the 2008 financial crisis. She has more than 20 years of experience in helping large financial institutions such as JP Morgan, UBS and RBS build their regulatory strength in response to regulatory requirements.

Fighting financial crime will continue to be a key focus for the global financial industry in 2020.

Regulators show no sign of easing up on their expectations with respect to Anti-Money Laundering (AML) compliance, especially given the findings of the EU's post-mortem report on recent money laundering cases involving EU banks, the high profile compliance failings in Australia, and the publication of the UK Government's Economic Crime Plan for 2019-22. For regulated firms, improving the efficiency and effectiveness of their AML and Counter-Terrorist Financing (CTF) will continue to be a high priority, assisted by the continuing adoption of innovative regulatory technologies (RegTech).

Based on RegTech Associates' research, insight and knowledge of the industry, we bring you our 2020 financial crime predictions with the hope that, by coming true, the fight against financial crime will be strengthened and the real harm caused to society will be reduced. Predictions include:

- **Continual changes in AML and CTF regulation** will drive regulated firms to seek more efficient and flexible CDD and EDD technology solutions.
- **Widening the regulator perimeter of AML and CTF regulation to crypto-assets** will promote the adoption of crypto-specific AML solutions.
- There will be **a rise in demand for education** about how artificial intelligence (AI) and machine learning (ML) can improve the effectiveness of financial crime (and fraud) detection.
- **Pragmatic approaches** such as layering innovative AI and ML technology over existing rule-based systems and providing greater interoperability will be key to the success of financial crime RegTech vendors in 2020.
- **Moving from data management to risk management** is key to tackling financial crime and in 2020, we will begin to see greater integration of data sets for KYC and transaction monitoring to gain greater insights over the lifecycle of a customer.
- **Industry collaboration on data sharing** will progress and industry utilities will continue to emerge and we will also see increased focus on the sharing of financial crime typologies using technology.
- Forward looking financial firms will be **exploring more holistic management of financial crime** across both AML and fraud, driven by similarities in the available technologies available for improved detection, such as ML.

regulatory and policy changes and their impacts

2020 is likely to see no respite from changes to the regulatory framework surrounding AML and CTF.

Continual regulatory change...

In the EU, the Fifth Anti-Money Laundering Directive (5MLD) came into force in January 2020, and will be closely followed by the Sixth (6MLD), which is set to be transposed into law in Member States by the end of the year and in force in the EU in June 2021.

For regulated firms, the 5MLD introduces changes to Enhanced Due Diligence (EDD) processes which involve high risk third-party countries and introduces some more prescriptive measures for Customer Due Diligence (CDD), specifically relating to corporate customers and greater transparency around Ultimate Beneficial Ownership (UBO). Member States are required to maintain public UBO registers and firms now have a responsibility to report any discrepancies they find between their records and those in the registry, adding to their regulatory reporting requirements.

Continual regulatory change is challenging for well-intentioned firms working hard to embed robust AML and CFT compliance frameworks. We anticipate that firms will strengthen their efforts in seeking technological solutions to ensure their EDD and CDD processes are more sustainable and adaptable to ongoing changes in the regulatory rules.

Focus on crypto-assets

In Europe, 5MLD extends the scope of the AML regulations to providers of exchange services between crypto-assets and fiat currencies and also to providers of custodian wallets. This will require these providers to conduct CDD monitor transactions and file suspicious activity reports where appropriate.

In Singapore, the Association of Cryptocurrency Enterprises and Start-Ups (ACCESS), facilitated by the Monetary Authority of Singapore (MAS), has developed a Code of Practice which aims to standardise the approach to tackling AML and Counter Financing of Terrorism, Know-Your-Customer (KYC) best practices for the crypto industry.

Both of these initiatives demonstrate the need for crypto firms to implement AML compliance frameworks and without the problem of legacy technology, we envisage that adoption of RegTech by these firms will accelerate as a result.

managing the **risks** of **innovative technology**

From our close collaboration with both the financial industry and technology vendors, we know there is a high level of enthusiasm about the promise of innovative technologies in helping to solve the problems of financial crime but also a level of confusion and risk aversion inhibiting their adoption.

Pragmatism and interoperability will be important for vendors.

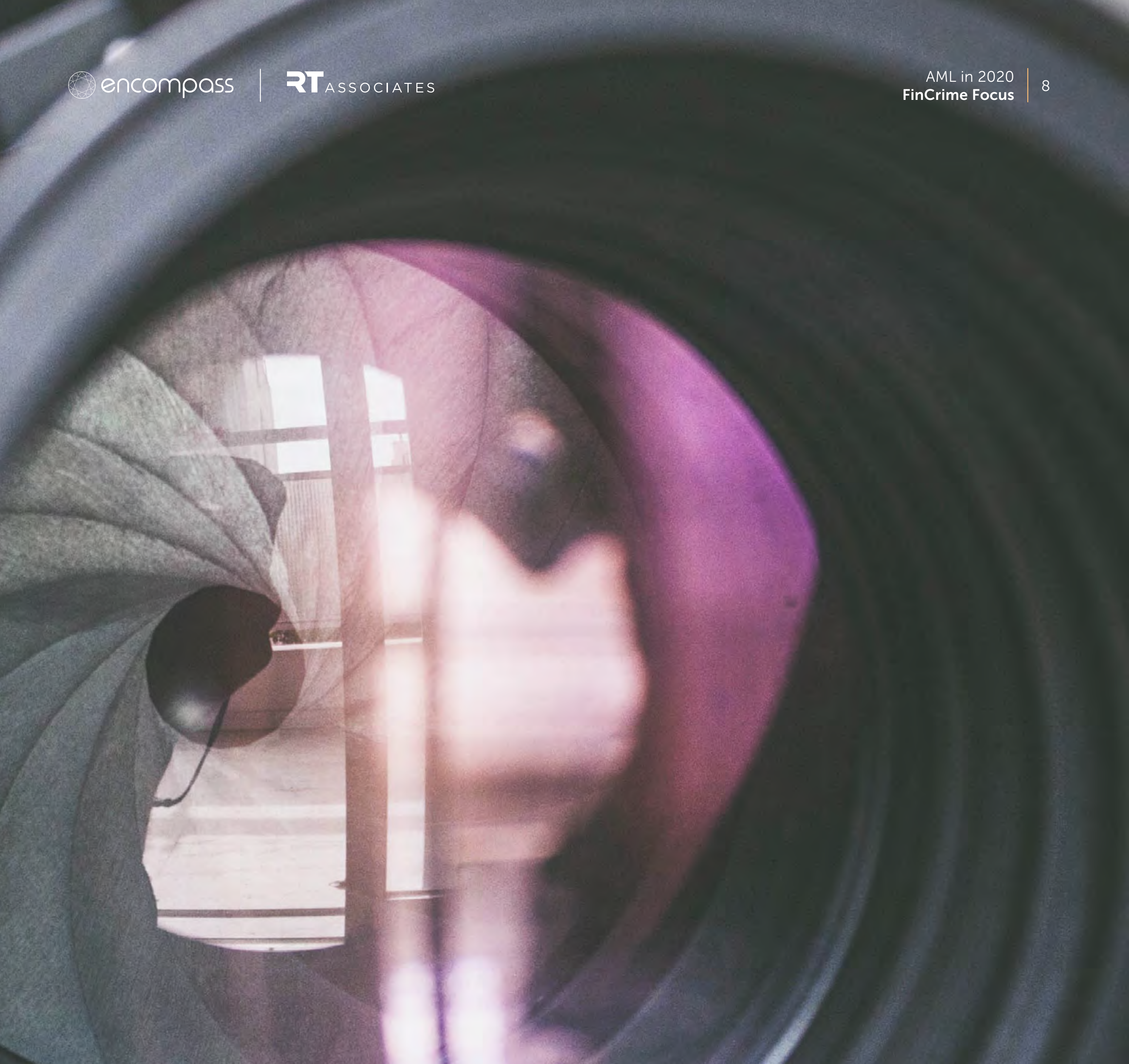
Given the level of regulatory scrutiny on financial crime, managing the risks associated with the adoption of new technology products is absolutely necessary. Vendors need to understand that it is unrealistic, at this point in time, for large financial institutions to completely rip out and replace the entire suite of legacy systems for KYC and transaction monitoring.

The level of risk is too high and such an approach would not be tolerated by many supervisors. Instead, we predict that successful vendors will focus on augmenting existing capabilities either by layering more effective AI-driven products on top of existing rule-based systems or providing specialist products with a high degree of interoperability to integrate with legacy technologies to solve specific problems.

More education around AI and Machine Learning in fighting financial crime.

Financial firms also have to manage the risks or tensions that exist between the need or desire to use more advanced and efficient technology such as Artificial Intelligence (AI) and Machine Learning (ML) and the need for those technologies to meet regulatory standards on explainability and broader model risk management and governance.

We suggest that, in 2020, we will see an increasing focus on vendors making this as easy as possible for their financial institution customers through the provision of detailed documentation and even training around AI governance standards. Finally, we believe we will see a rise in the demand for senior management education around the use of AI and ML for fighting financial crime and the benefits that it can deliver.



breaking down **silos**

Much of the research we conducted in 2019 confirmed what is now somewhat of a truism in the financial industry - that fighting financial crime is incredibly fragmented on a number of different levels.

Combining KYC and transaction monitoring data

Within many financial organisations, and for very good reasons, the data, systems, people and processes for conducting KYC are often very separate to those for monitoring transactions and reporting suspicious activity.

More effective AML can be achieved, however, by combining data from these two processes so that firms can monitor behaviour and customer activity through the customer lifecycle and then layering machine learning on top to identify anomalous patterns and potential suspicious activity.

We anticipate that firms with more sophisticated AML platforms will take this next step, enabling the move from data management to risk management.

Further collaboration on data sharing

Across the industry, each financial firm conducts its own KYC and due diligence on individuals and companies, many of whom are obviously also customers of other financial firms. Thus, KYC data is fragmented across the industry, resulting in costly inefficiencies. This also applies to typologies of financial crimes, identified bottom-up by individual firms and shared officially on a top-down level by authorities such as the Financial Action Task Force, often with a significant time lag between their identification and publication.

Our hope for 2020 is that industry collaboration around data sharing for AML will make significant progress, encouraged by the initiatives for KYC utilities in the Nordics, UAE and the Netherlands and also the FCA's 2019 techsprint. We also anticipate greater sharing of financial crime typologies, facilitated by vendors who are capturing typologies as part of the machine learning models for transaction monitoring.

Managing AML, CTF and fraud together

Financial crime risk in the form of AML and CTF is usually monitored and managed separately to dealing with fraud for two key reasons.

Firstly, fraud detection and monitoring ideally happens in real-time so that preventative action can be taken such as stopping payments. Transaction monitoring for AML purposes, however, tends to occur retrospectively because suspicious activity reporting is usually performed after the fact.

Secondly, the regulatory framework specifically mandates prescriptive regulatory compliance obligations for AML and CTF whereas managing fraud risks is considered by regulators such as the FCA as an obligation to protect consumers and for the sound management of a financial institution.

These two factors mean that often fraud and AML/CTF are managed very separately, even though the two crimes are often interrelated and fraud is a known predicate crime for money-laundering.

Greater holistic management of different types of financial crime is now possible from a technological point of view - many vendors with products designed to prevent fraud are now developing use cases for AML because both AML and fraud require the same also leverage the same transactional parameters, account and customer information, peer group definitions, watch lists, and detection models.

In 2020, we expect to see further development of integrated financial crime management from a technical perspective - but it may well be a few years before the operational frameworks to support this are implemented.

about **RegTech Associates**

RegTech Associates is an independent advisory company, positioned at the core of the RegTech market.

We work closely with CEOs and Founders of start-up and scale-up technology companies to help them grow their businesses. We partner with our clients throughout the product and company lifecycle, from design through to commercial strategy and sales.

We spend a lot of time with regulated firms in financial services to understand their regulatory problems and how technology can help solve them. We also collaborate with leading regulators to foster dialogue and industry collaborations across a number of regulatory issues.

Find out more at rtassociates.co.

about **Encompass**

Encompass automates information and news discovery for KYC requirements for client onboarding, event-driven refresh and remediation.

Driven by your internal policies and choice of reliable, independent sources, **Encompass** constructs corporate ownership, discovers beneficial owners, and comprehensively screens entities and persons for risk.

Our advanced intelligent process automation dynamically builds a comprehensive KYC profile from multiple sources, including corporate registries, company and regulatory data, adverse media and identity verification - enabling fast, confident decisions. Incorporating leading biometric and eIDV sources for individual KYC verification, **Encompass** delivers a single platform to manage every type of customer.

Find out more at **encompass**corporation.com.