



Successful Transaction Monitoring: Overcoming Challenges Through Collaboration

A COLLABORATION BETWEEN

LYSIS
OPERATIONS

Lysis Operations,
AML & CLM Processing by Professionals

AND

NAPIER

Napier,
AI Powered AML Platform.

Contents

Introduction	3
Chapter 1: The cardinal numbers	5
Increasing numbers of compliance specialists	5
Increasing volumes of transactions and payments	5
Finding the needle in the haystack	6
The scale of the problem	7
Chapter 2: The challenges in getting it right	8
Chapter 3: Overcoming challenges	9
The role of effective technology	9
How artificial intelligence enhances transaction monitoring	11
A road map to successful implementation of artificial intelligence for transaction monitoring	12
Chapter 4: The operational gap	16
The importance of high-performing teams	16
Building sustainable & high-performing teams	17
Transaction monitoring managed service: The game changer	18
Emerging markets and lack of financial crime expertise	19
Conclusion	21
About the authors	22
Tom Griffiths, Associate Director, Lysis Operations	22
Nick Portalski, Chief Operating Officer, Napier	22
Luca Primerano, Chief AI Officer, Napier	22
About Lysis	23
About Napier	24

Introduction

Transaction monitoring is a key part in the defence against money laundering and financial crime. It is the process of identifying and reviewing anomalous activity and transactions before deciding to report any suspicious activity to law enforcement.

A successful process should monitor transactions against pre-defined rules and thresholds, anticipated activity; and should rely on a strong partnership between technology and operational expertise.

However, many institutions struggle with implementing adequate transaction monitoring systems and processes which puts them at risk of regulatory and legal intervention.

The Commerzbank case is a good example of such regulatory intervention: in early 2020 the bank was fined for AML failures, including long-standing weaknesses in its automated tool for monitoring money laundering risk on transactions for clients¹.

Also in 2020, the U.S. Treasury issued a nearly half a million-dollar penalty against a top compliance official for failures in underlying

anti-money laundering program tied to capping transaction monitoring alert volumes at U.S. Bank National Association (U.S. Bank)².

But if the risk of reputational damage and the risk of incurring hard-hitting penalties is so high, why do firms continue to struggle with transaction monitoring?

In this paper we take a closer look at some of the numbers relating to payments, transactions and the world of compliance to help explain why some of the current transaction monitoring technology and operational controls struggle to identify illicit activity. We then look at the role of technology, and what future developments will bring to transaction monitoring.

Finally, we argue the case for utilizing a managed service for transaction monitoring, and how approaching compliance in this way results in a more effective and efficient process. The combination of technology and expert personnel who are focused solely on the requirements and the outcomes, ensures illicit activity is identified and reported whatever the industry and associated risks may be.

1 <https://www.fca.org.uk/news/press-releases/fca-fines-commerzbank-london-37805400-over-anti-money-laundering-failures>

2 <https://www.acfcs.org/fincen-issues-rare-penalty-nearly-half-a-million-dollars-against-top-risk-officer-for-longstanding-aml-failures-alert-caps/>

Chapter 1: The cardinal numbers

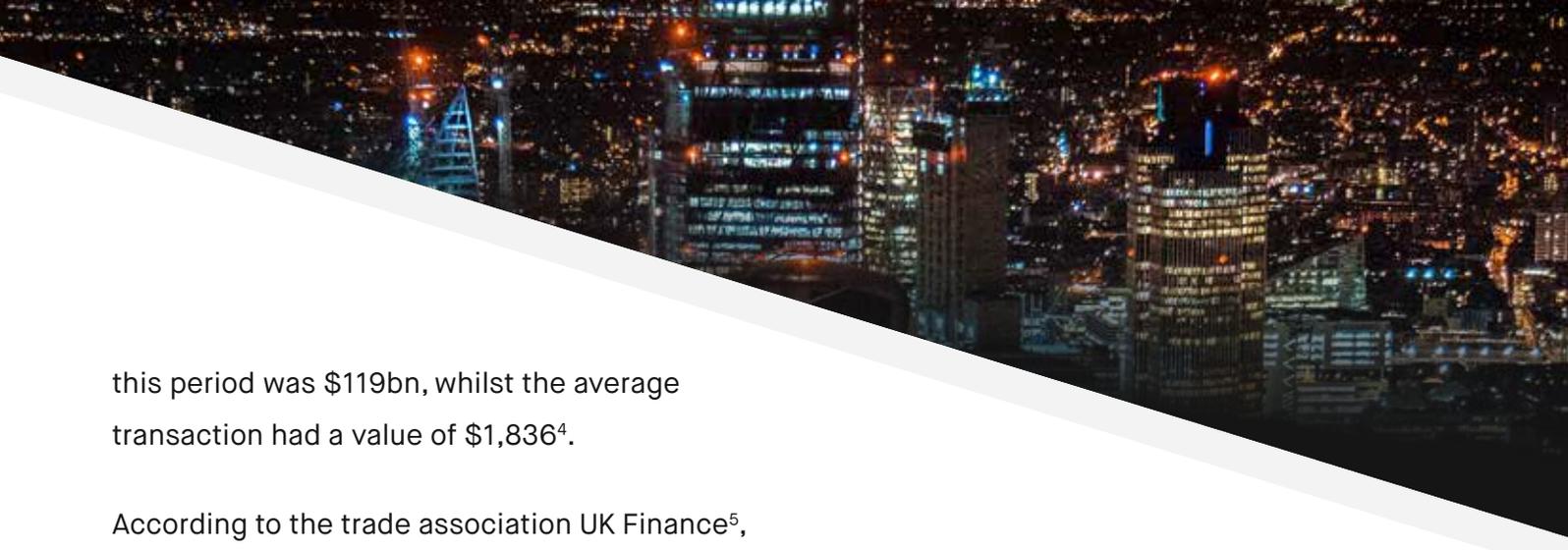
Increasing numbers of compliance specialists

Increasing headcount in compliance departments is a common kneejerk reaction to waves of financial crime allegations in the banking sector and the fear of not having adequate monitoring systems to avoid regulatory penalties. The Nordic bank Nordea recently hired 1500 additional personnel to deal with a backlog of transactions. But that only served to balloon compliance costs dramatically, forcing the bank to announce only months later that these roles would be terminated in favour of improving automation³.

Increasing volumes of transactions and payments

There is no doubt that banks and financial institutions are under enormous pressure as the volumes of payments and transactions in today's world are at their highest ever. The US Federal Reserve processed 4 billion financial transactions every day in the fourth quarter (October to end December) of 2019. The daily total average value of payments during

³ <https://www.businesstimes.com.sg/banking-finance/nordea-warns-of-compliance-job-cuts-reversing-hiring-boom>



this period was \$119bn, whilst the average transaction had a value of \$1,836⁴.

According to the trade association UK Finance⁵, there were 34.9 billion consumer payments made in the UK during 2019; with 85% of these payments being spontaneous. During the same period, there were 4.4 billion business-to-business and business-to-individual payments made in the UK.

Monitoring even a portion of these successfully will be difficult without adequate skilled resources and technology, especially as the technology and the methods criminals use to launder money are constantly evolving.

Finding the needle in the haystack

Finding the proverbial needle in the haystack – the anomalies that point to suspicious activity is still proving to be challenging. In the UK, the National Crime Agency received only 478,437 Suspicious Activity Reports (SARs) between April 2018 and March 2019 (a 3.13% increase on 2017-18 [463,938])⁶. It is implausible to make a direct comparison, but at a glance this number, when compared with the billions of transactions that flow through the banks daily, raises concerns that volumes of SARs is too low, indicating that large numbers of suspicious transactions are going undetected. While it is impossible and inaccurate to compare the total amount of payments versus the number of SARs based on numbers alone – they still simply do not tally.

4 https://www.federalreserve.gov/paymentsystems/files/fedach_quarterlycomm.txt

5 <https://www.ukfinance.org.uk/sites/default/files/uploads/pdf/UK-Finance-UK-Payment-Markets-Report-2019-SUMMARY.pdf>

6 <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019/file>

The scale of the problem

The volume of illicit funds being laundered through the global financial system is very difficult to estimate. The European Union Agency for Law Enforcement Cooperation (Europol) considers it to be “significant” and the United Nations Office on Drugs and Crime (UNODC) estimates that between 2% and 5% of global Gross Domestic Product (GDP) is laundered each year. This amounts to between €715 billion and €1.87 trillion of illegally obtained money being laundered by criminals through the global financial system each year.

While the number of SARs (or Suspicious Transaction Reports (STRs)) being recorded may amount to hundreds of thousands versus billions of transactions within most countries, and with up to 5% of a country’s GDP reported to being laundered each year, the role of transaction monitoring control clearly needs to do more to “find the **many** needles within the **many** haystacks”.

The amount of money being laundered through the financial service industry is immense but the sheer number of transactions are colossal – having the confidence that systems as controls are adequate to protect against this issue is challenging to say the least.

Risks of getting it wrong

In recent years, regulatory penalties for AML failings have been eye-wateringly high, with the likes of Standard Chartered being fined \$1.1billion, and Westpac AUS\$900 million. More damaging though is the hit to an institution’s reputation which can affect business and the bottom line for years after.



Chapter 2: The challenges in getting it right

The challenges in implementing effective transaction monitoring systems will differ considerably depending on the nature of an organisation's customers, the markets they service, and the maturity of their business.

Legacy technology

Larger, more established institutions may have a better understanding of the risks they face as they have had longer to monitor and identify patterns. However, they often struggle with the inefficiency of legacy technology and systems that produce too many false positives and have inflexible rulesets.

Most firms accept it would be would make business sense to implement new technology to overcome these challenges. But the reality

is that for big institutions this is too often a largescale project that takes a lot of time and resource to implement. Furthermore, the process can be very expensive if not managed correctly.

Compliance not a priority

In contrast, FinTechs, such as Payment Service Providers (PSPs), and challenger banks may find it easier to introduce new technology. These firms are often driven primarily by technological development and innovation, with compliance as a secondary consideration. The downside is that they may be less aware of the financial crime risks and compliance responsibilities because of the relative infancy of their business.

Chapter 3: Overcoming challenges

The role of effective technology

For transaction monitoring to be effective, the role of technology must be to aid the compliance specialist to detect truly suspicious activity, while at the same time increasing efficiency.

There are four ways technology can do this:

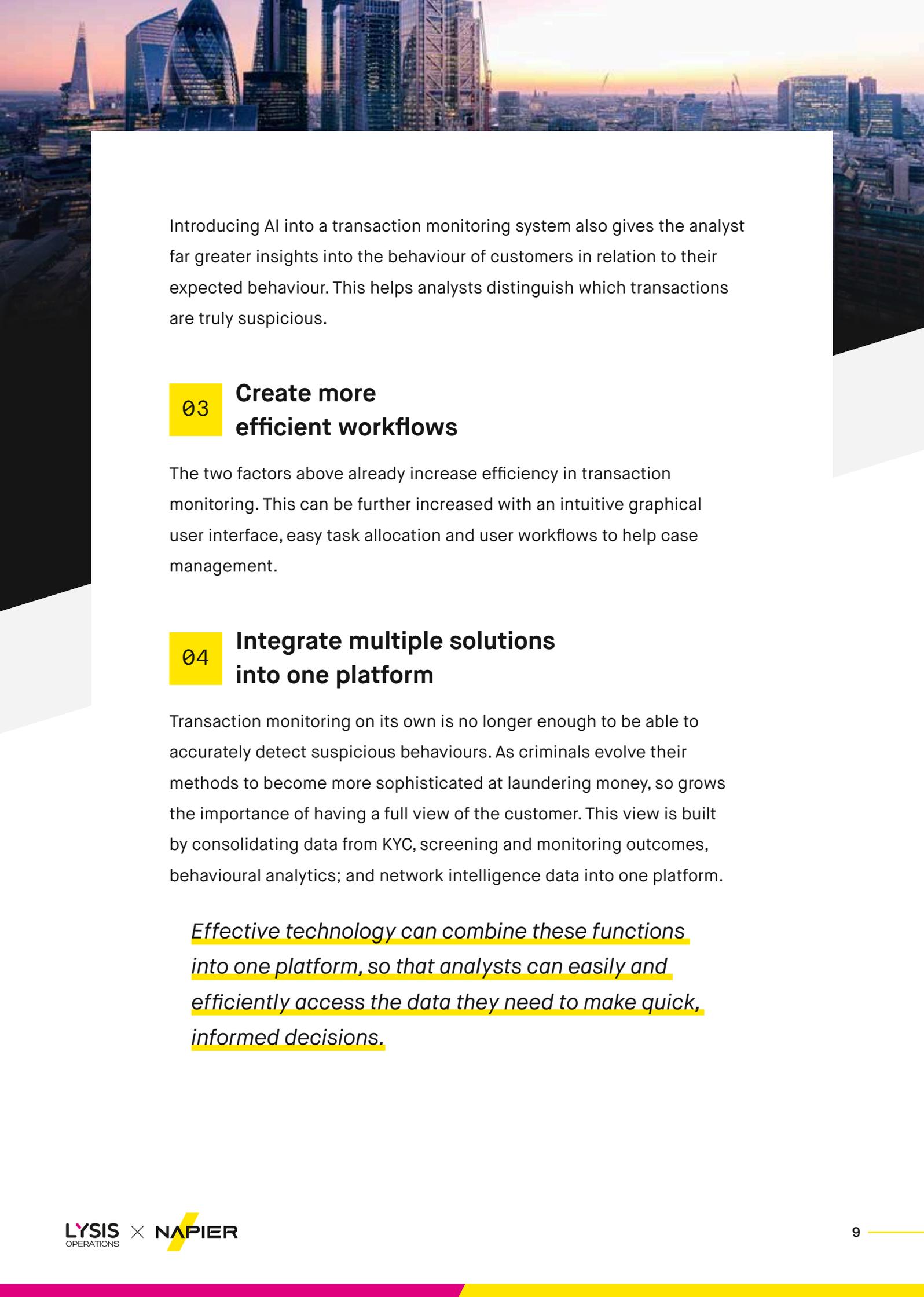
01 **Reduce the number of false positives significantly**

The biggest challenge faced by organisations using legacy technology, or technology that is not fit for purpose, is the high volumes of false positives produced when monitoring transactions. One of the issues in effectively reducing false positives, is to not negate the truly suspicious cases.

This is where modern technology can have a powerful effect, as it can decrease false positive volumes by using more accurate name matching algorithms, better rules and artificial intelligence (AI), yet continue to flag up transactions that do require investigation.

02 **Produce deeper insights**

Easier access to powerful analytics gives users the ability to drill down into each case and gain deeper insights into activities and transactions.



Introducing AI into a transaction monitoring system also gives the analyst far greater insights into the behaviour of customers in relation to their expected behaviour. This helps analysts distinguish which transactions are truly suspicious.

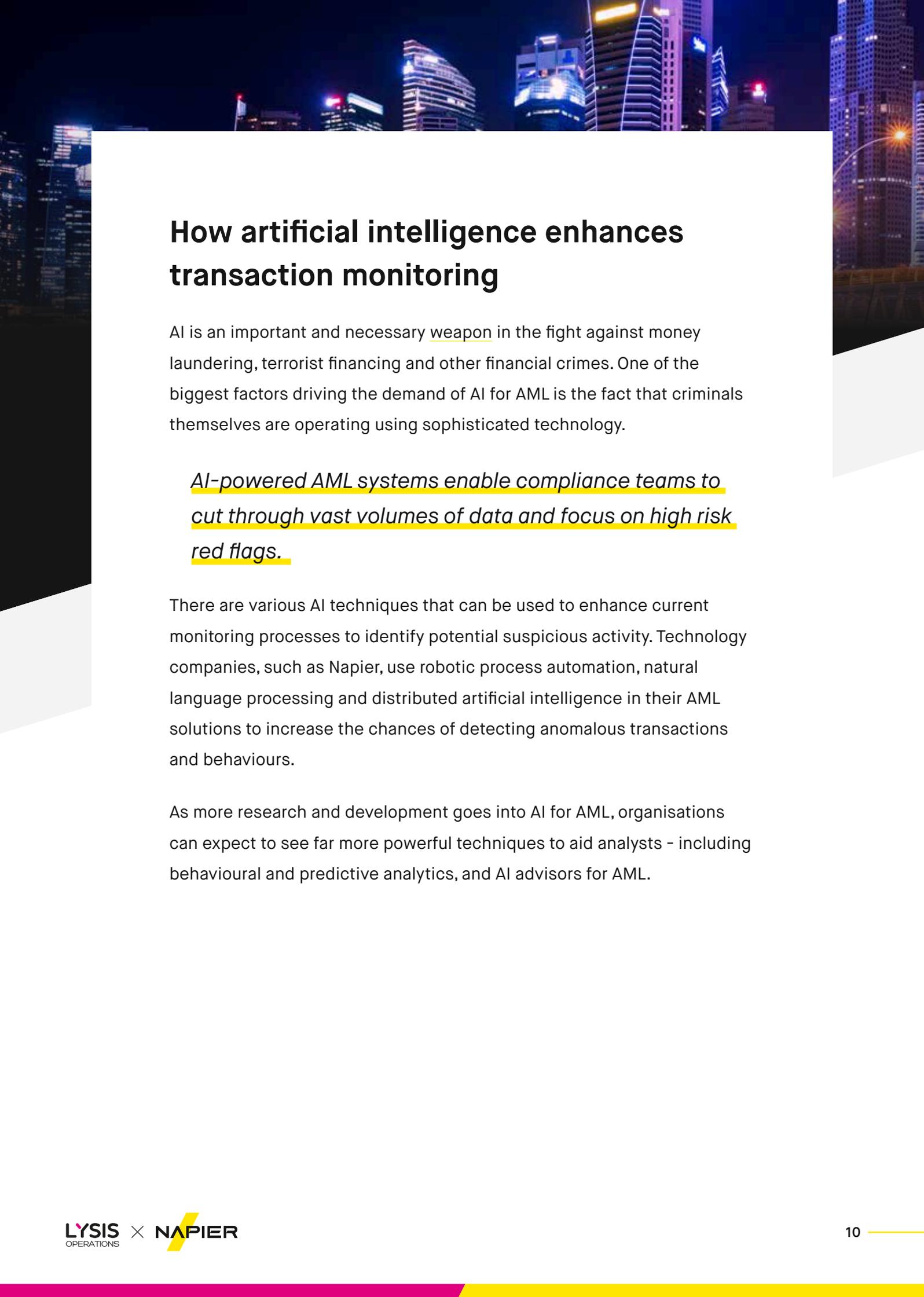
03 **Create more efficient workflows**

The two factors above already increase efficiency in transaction monitoring. This can be further increased with an intuitive graphical user interface, easy task allocation and user workflows to help case management.

04 **Integrate multiple solutions into one platform**

Transaction monitoring on its own is no longer enough to be able to accurately detect suspicious behaviours. As criminals evolve their methods to become more sophisticated at laundering money, so grows the importance of having a full view of the customer. This view is built by consolidating data from KYC, screening and monitoring outcomes, behavioural analytics; and network intelligence data into one platform.

Effective technology can combine these functions into one platform, so that analysts can easily and efficiently access the data they need to make quick, informed decisions.



How artificial intelligence enhances transaction monitoring

AI is an important and necessary weapon in the fight against money laundering, terrorist financing and other financial crimes. One of the biggest factors driving the demand of AI for AML is the fact that criminals themselves are operating using sophisticated technology.

AI-powered AML systems enable compliance teams to cut through vast volumes of data and focus on high risk red flags.

There are various AI techniques that can be used to enhance current monitoring processes to identify potential suspicious activity. Technology companies, such as Napier, use robotic process automation, natural language processing and distributed artificial intelligence in their AML solutions to increase the chances of detecting anomalous transactions and behaviours.

As more research and development goes into AI for AML, organisations can expect to see far more powerful techniques to aid analysts - including behavioural and predictive analytics, and AI advisors for AML.

A road map to successful implementation of artificial intelligence for transaction monitoring

While the purpose of AI is to enhance and simplify manual processing relating to transaction monitoring, successful implementation requires detailed planning and understanding of the specific requirements of an institution's risks and AML maturity.

The automation of compliance activities is expected to be the biggest change for compliance in the next 10 years, so it is prudent to acknowledge hurdles you're likely to encounter along the way.

When you invest in AI, be prepared for results to take time and effort. Implementing AI is as much a cultural commitment from the top down as it is a financial investment. It is important to put the right governance and processes in place, and to clearly define target outcomes before embarking on any machine learning project.

The capability gap

Financial institutions must identify what they wish to achieve by introducing AI into the transaction monitoring system.

There is always going to be a gap between what the organisation wants to achieve through automation and what can be achieved from an internal, and often legacy, perspective as well as a regulatory perspective.

The Money Laundering Reporting Officer may wish to reduce the level of automation if they do not fully understand, or feel comfortable with the technology.

There is an increased need for compliance specialists to develop technological ability and understanding in relation to AI, analytics and regulatory controls.

Gradually introduce artificial intelligence

One way to introduce AI and machine learning is to run an existing rules-based transaction monitoring system alongside a new AI-powered system.

Doing this allows the old system to assist in training the new. It also enables financial institutions to challenge the traditional system, and simultaneously improve the performance of both.

Before a system that uses machine-learning can be fully deployed, it will need human input to fine-tune its initial 'self-taught' learning. The biggest challenge is that learning is not a 'tick and forget' exercise. Criminals are constantly changing their tactics in an attempt to remain under the radar.

For these reasons, most of a machine's learning will occur when the system is live, as a result of humans reviewing the alerts generated by the system. When analysts feedback their knowledge into the machine, the machine is able to improve the accuracy and relevance of its alerts to reduce false positives and help avoid false negatives.

Getting the basics right

If there is one theme that keeps cropping up, it is the need to get the basics right before implementing AI. This process can take a significant amount of time and effort – but it will ensure the benefits of machine learning are maximised and in turn, provide a difficult to replicate competitive advantage.

Aside from organising data and training staff on how to use the system, much of the preparation for AI and machine learning rests in laying a solid foundation with transaction monitoring rules. It is really important to get the rules right as AI should initially complement rather than replace traditional systems.

Giving compliance specialists superpowers

Analytics

With the introduction of AI, the nature of a compliance specialist's role will increasingly change from mundane data processing to highly investigative work as the AI automates the repetitive tasks involved in previously manual processes.

The introduction of AI-enhanced analytics will also give compliance specialists far deeper insights into customer behaviour and transactions. These analytics give the compliance specialist a view of the past, present and predicted behaviour of a customer, allowing the analyst to more easily identify unusual and suspicious activity. Having this intelligence available in easy-to-view graphics reduces the risk of illicit activity going undetected and simultaneously offers the compliance specialist even more control.

Network Analytics

The introduction of network analytics into transaction monitoring systems will help compliance specialists map a customer's network producing a global view of their relationships including immediate and extended networks.

This will provide the compliance specialist with the ability to identify relationships and



jurisdictions which may be prohibited or require further investigation in a way that legacy technology is unable to do.

Risk profiles

Determining a customer risk profile has been a long-established requirement by the regulators. However, a generic approach by definition is not effective in transaction monitoring as money launderers very quickly change their behaviours and activity once onboarded.

An AI-enhanced transaction monitoring system can produce dynamic customer risk profiles which are automatically adjusted based on the customer's behaviour, transactions, and other intelligence.

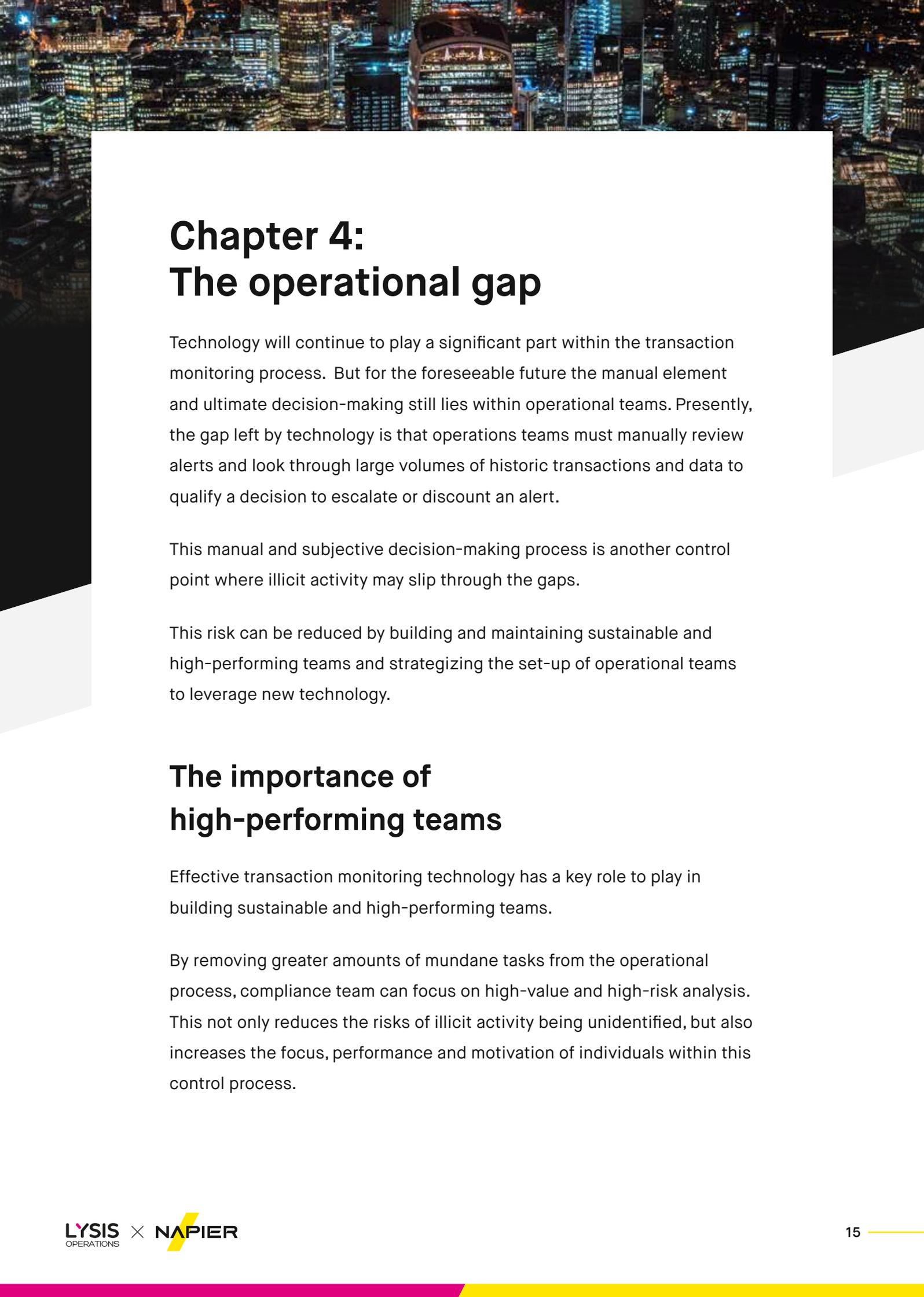
Leveraging third party intelligence

Good intelligence plays an increasing role in effective transaction monitoring systems. By introducing intelligence data from third parties, analysts have access to a wealth of contextual intelligence to help make rapid decisions about changes in customer behaviour to identify suspicious activity.

AI Advisor

As technology becomes more sophisticated, compliance specialists will have an AI Advisor by their side that continuously analyses patterns and learns to indicate unusual or complex insights and recommends areas of focus or action.

AI will evolve the role of the compliance specialist from mundane manual analysis into a deeper and more focused investigative role.



Chapter 4: The operational gap

Technology will continue to play a significant part within the transaction monitoring process. But for the foreseeable future the manual element and ultimate decision-making still lies within operational teams. Presently, the gap left by technology is that operations teams must manually review alerts and look through large volumes of historic transactions and data to qualify a decision to escalate or discount an alert.

This manual and subjective decision-making process is another control point where illicit activity may slip through the gaps.

This risk can be reduced by building and maintaining sustainable and high-performing teams and strategizing the set-up of operational teams to leverage new technology.

The importance of high-performing teams

Effective transaction monitoring technology has a key role to play in building sustainable and high-performing teams.

By removing greater amounts of mundane tasks from the operational process, compliance team can focus on high-value and high-risk analysis. This not only reduces the risks of illicit activity being unidentified, but also increases the focus, performance and motivation of individuals within this control process.

If a financial institution does not embrace technology to reduce the manual burden, the risk of an underperforming team will increase, as will the risk of illicit activity being undetected.

However, operations teams can be high performing without relying solely on technology. Here's how.

Building sustainable & high-performing teams

It is often difficult to keep people focused especially when their role is to review large volumes of data to identify the needle in the haystack. Achieving high-energy levels is very important to generate sustainable focus. It is vital to set achievable but challenging goals to motivate individuals within this control setting. These goals should be measurable and specific.

Highly productive teams are those who are entirely focused on outcomes and results.

Organising teams into cells or pods is more efficient and effective. Building autonomous small teams of cells/pods can create high-impact and dynamic sub-teams within the main structure. The cells or pods should be cross-functional and self-managing.

This is a subtle change which can strengthen support networks, promote collaboration and drive accountability. It is also important to have a Quality Assurance presence in each pod/cell to provide review and subject

matter expertise, to increase the effectiveness and overall control of the transaction monitoring process.

Transaction monitoring managed service: The game changer

Bringing effective technology and high performing teams together is a “game changer” in developing a successful transaction monitoring programme.

An effective transaction monitoring managed service can enhance transaction monitoring controls if operated by experienced personnel who have a single focus rather than additional internal responsibilities.

Having specialist compliance analysts and subject matter experts with the experience of working with technologists supports technology implementation and the continual performance of the controls.



Benefits of collaboration:

- ✓ Focused expert personnel dealing with the transaction monitoring controls
- ✓ AI-driven processes reduce the time spent reviewing false alerts
- ✓ Dynamic and evolving platform not constrained by legacy system challenges and data
- ✓ Cross-industry partnerships underpinned by proven systems and services

Using a managed service gives nominated officers and board members the comfort that transaction monitoring controls are undertaken by specialists in a transparent manner. A managed service also reduces the cost of technology and drives operational efficiencies and regulatory controls, which in time, reduces the cost of operational processing.

This cost reduction is driven by multiple institutions using the same evolving technology stack. This reduces the cost to licence as well as the cost of implementation and servicing without any impact on effectiveness.

An effective managed service is supported by industry leading expert consultants who provide constant knowledge, support and oversight of the service no matter how long or short the engagement.

Cross-industry collaboration is a high value asset which many institutions will struggle to replicate internally.

Emerging markets and lack of financial crime expertise

Recent legislation brought more industries into the scope of money laundering regulations across Europe. Estate agency businesses were brought into the scope within the EU by the 4th Money Laundering Directive in June 2017; and art dealers by the 5th Money Laundering directive in 2020.

Both industries must now ensure they have transaction monitoring programmes in place to identify illicit activity or face financial penalties for failing to do so.

Estate Agents and Art Dealers

It is difficult to expect estate agents and art dealers to be specialists in financial crime – but this is the expectation of the regulators. Some companies in these industries, owing to the nature and/or size of their business, do not have the capacity or need for a full-time compliance function. This is a key area where a transaction monitoring managed service would support this requirement.

Art dealers, including persons storing art, become “obliged entities” if they deal in one-off transactions worth more than €10,000 or where the value of a series of linked transactions amounts to €10,000 or more. To identify these types of transactions, a robust and effective transaction monitoring programme is required. Using an external service run by experts, and underpinned by sophisticated technology, will allow art dealers to ensure they are compliant with money laundering regulations.

Payment Service Providers

Payment Service Providers (PSP) have boomed in recent years – this growth, and increased regulatory scrutiny means these firms must have a robust transaction monitoring programme in place.

Given the nature of the business PSPs offer, transaction monitoring is a vital part of an effective AML framework, and it should be done in real time. Transaction monitoring systems should develop and evolve in line with the growth of the business, as well as in line with the industries they service. As industries evolve, so will the risks. It is important for transaction monitoring systems and capabilities to be responsive.

Conclusion

The sheer volume of transactions the global financial industry processes each day makes monitoring even a portion of these difficult, especially as the methods and technology criminals use to launder money is constantly evolving. AI-powered transaction monitoring systems enable compliance teams to cut through vast volumes of data and focus on high risk red flags.

The automation of compliance activities is expected to be the biggest change for compliance in the next 10 years, so it's prudent to acknowledge hurdles that are likely to be encountered along the way. The introduction of AI-enhanced analytics will also give compliance specialists far deeper insights into customer behaviour and transactions, ultimately giving control back to the compliance officer.

It is important to note that despite the advancement of technology, people continue to play a key part in successful transaction monitoring programmes. Highly productive teams are those who are entirely focused on outcomes and results. By having a focus on technology and operational expertise, the value of transaction monitoring can be enhanced.

Utilising a managed service for transaction monitoring results in a more effective, evolving and efficient process. The combination of technology and expert personnel who are focused solely on the requirements and the outcomes, ensures illicit activity is identified and reported whatever the industry and associated risks may be.

Bridging the gap with effective technology and expert personnel not only results in compliance specialists being given superpowers but also enable financial institutions to protect themselves and global financial system from being used for money laundering and other illicit activity.

An effective managed service underpinned by innovative technology will ensure those illicit needles within the colossal haystack of payments will not only be identified but analysed effectively and reported appropriately.

With the historic and on-going failures of financial institutions to adequately identify instances of financial crime through effective transaction monitoring controls resulting in ever increasing fines and scandals, now is the time to consider a new approach to transaction monitoring.

About the authors



Tom Griffiths,
Associate Director,
Lysis Operations

Tom Griffiths is an Associate Director at Lysis Operations. Tom has been working within regulatory change since 2003 and specialises in financial crime. Prior to joining Lysis, Tom held a breadth of roles covering change management, systems integration and advisory positions at a number of financial institutions including JP Morgan, Lloyds Banking Group, Standard Chartered and ABN Amro.

Since joining Lysis, Tom has carried out governance framework reviews and change management projects for several clients within regulatory operations and compliance departments. Tom has also held senior advisory roles within financial crime for several global financial institutions.



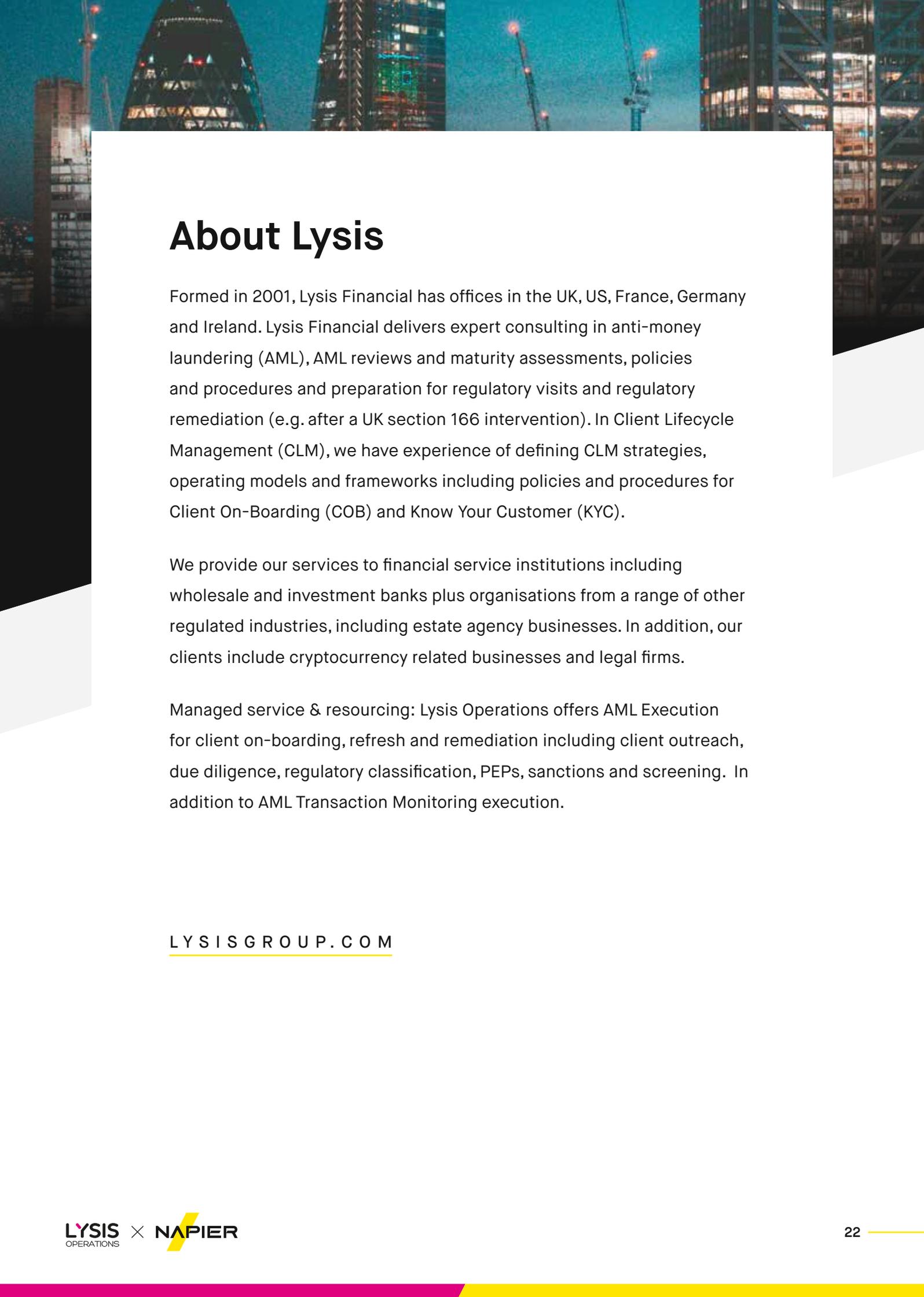
Nick Portalski,
Chief Operating
Officer, Napier

Nick has extensive leadership experience in designing and delivering enterprise products using multiple technologies. Having worked in successful FinTech start-ups and enjoyed global responsibilities with IBM, his expertise lies in taking concepts from embryonic vision through to advanced end products.



Luca Primerano,
Chief AI Officer,
Napier

Luca is the Chief AI Officer at Napier, where he focuses on running artificial intelligence programmes partnering with tier-1 universities and clients. Luca has extensive experience in decision automation and digital transformation that he gained at Goldman Sachs, Deutsche Bank and Deloitte and has an MS in engineering from Politecnico di Milano specialising in anomaly detection, data correlation and pattern identification.



About Lysis

Formed in 2001, Lysis Financial has offices in the UK, US, France, Germany and Ireland. Lysis Financial delivers expert consulting in anti-money laundering (AML), AML reviews and maturity assessments, policies and procedures and preparation for regulatory visits and regulatory remediation (e.g. after a UK section 166 intervention). In Client Lifecycle Management (CLM), we have experience of defining CLM strategies, operating models and frameworks including policies and procedures for Client On-Boarding (COB) and Know Your Customer (KYC).

We provide our services to financial service institutions including wholesale and investment banks plus organisations from a range of other regulated industries, including estate agency businesses. In addition, our clients include cryptocurrency related businesses and legal firms.

Managed service & resourcing: Lysis Operations offers AML Execution for client on-boarding, refresh and remediation including client outreach, due diligence, regulatory classification, PEPs, sanctions and screening. In addition to AML Transaction Monitoring execution.

[LYSISGROUP.COM](https://www.lysisgroup.com)

About Napier

Napier is a new breed of AML and trade compliance tech provider. Our Intelligent Compliance Platform is transforming compliance from legal obligation to competitive edge. All Napier products are built on our ICP third generation compliance platform which can be delivered via public cloud, private cloud or on premise. Our tools dramatically reduce both false positives and false negatives and empower compliance teams to make validated decisions with unprecedented speed and accuracy.

Find out more./

Our expert team is ready to answer your questions. Get more information or book a demo today.

napier.ai | info@napier.ai



A COLLABORATION BETWEEN

