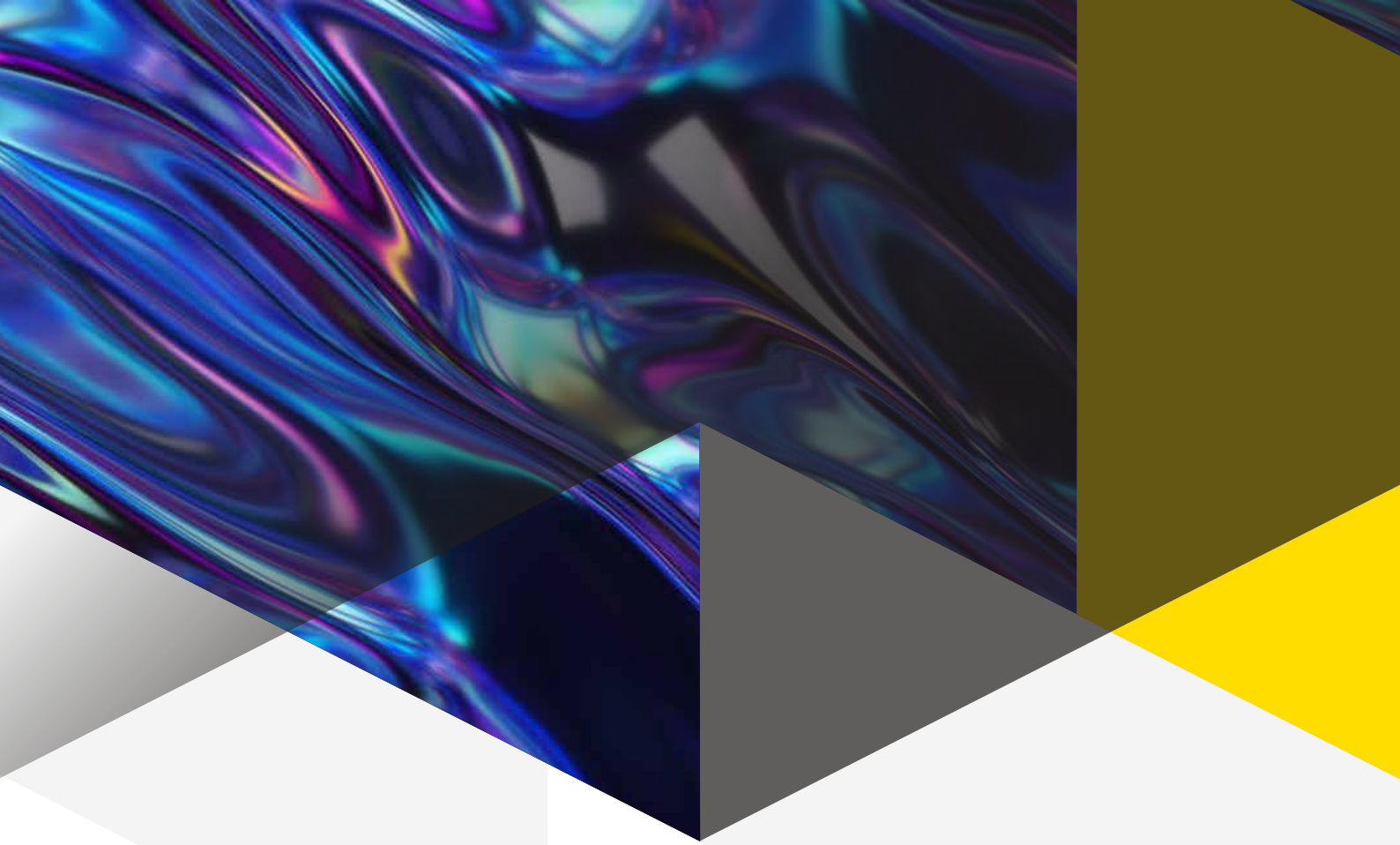


EBOOK: FINANCIAL CRIME

Understand your customer:

The importance of a holistic view of client activity in AML

By Julian Dixon
CEO, Napier

NAPIER

About the author

Julian Dixon

CEO, Napier

Julian founded Napier in 2015 when he recognised that there was a need to replace existing slow and inefficient compliance systems with advanced technology that combines big data with AI to increase efficiency and combat financial crime.

Determined to create a world-leading technology solution to help compliance officers fight financial crime in an efficient way, Julian has grown Napier from a start-up to a global company, with clients including Tier 1 banks, payment services companies, and blue chip corporates.

With over 20 years of financial services experience gained at major investment banks including Deutsche Bank, JP Morgan and Commerzbank, Julian has extensive knowledge of financial services processes and technology.

Julian is a valuable contributor in panel discussions, and co-author of the PayTech book. He is invited regularly to share his views on how RegTech is well placed to solve the industry's challenges relating to financial crime.

in Connect with Julian on Linkedin

Contents

The importance of a holistic view of client activity in an AML solution

Thinking about anti-money laundering (AML) holistically is not a new concept by any means. But creating practical, pragmatic solutions that allow financial firms to move to an integrated approach to tackling financial crime is.

In this eBook, we explore why holistic AML approaches are critical to successful financial crime-fighting, why they are so hard to implement and how Napier's Client Activity Review is the fundamental first step in a client-centric view of financial crime risk across your whole firm.

What do we mean by holistic AML?

GLOBAL LEVEL

At a global level, it is the international co-operation between law enforcement, policy-makers and supervisors, enabling the sharing of data and intelligence to investigate and catch criminals who are unconstrained by national borders.

INDUSTRY

At an industry level, it is the collaboration between financial firms to share data on bad actors or suspicious activity, or even pooling (non-private) data for the purposes of Know Your Customer (KYC), such as in the KYC utility model.

INDIVIDUAL

At the individual firm level, holistic approaches to AML overcome operational, business, system and data silos, allowing a co-ordinated view of customers and activity across the enterprise - lines of business, products, regions, state and national borders.

Holistic AML - why is it important?

The United States must continue to stay ahead of emerging illicit finance challenges and position itself to be a model for AML/CFT for years to come. To do this, the U.S. government must holistically approach strengthening the U.S. AML/CFT regime to make it more effective, efficient, and responsive to an evolving threat environment[1]

Holistic approaches to AML are paramount because of the nature of the money-laundering problem itself - in terms of how the modern criminal economy works and also how the responses to that criminal economy are shaped in policy, law enforcement and supervisory frameworks.

1 US Treasury (2020) National Strategy for Combating Terrorist and Other Illicit Financing

The Criminals

Obviously criminals do not publish their own performance statistics so it is difficult to get an accurate picture of the scale of the money laundering problem, but experts[2] agree that between 2% and 5% of global output per year can be attributed to the proceeds of crime.

Based on 2019 global output figures, that indicates somewhere between $1.7 and $4.3 trillion is illicitly obtained in any given year. To put that into perspective, only the US and China produce economic output greater than the entirety of the global criminal economy.

Increasing globalisation, the massive shift to digital channels for finance and gambling, the emergence of crypto assets as well as peer-to-peer platforms provide criminals with a whole range of new ways to launder their illicit gains, as well as the more traditional methods such as cash smuggling and trade-based money laundering.

Huge amounts of money are being laundered each year, by increasingly sophisticated and complex methods employed by savvy criminals making the most of new and innovative technologies.

2 The United Nations Office on Drugs and Crime (UNODC) study to determine the magnitude of illicit funds generated by drug trafficking and organised crimes estimated that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered.
In 1998, the IMF stated in 1998 that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's gross domestic product

The Financial Crime Fighters

Based on the number of illicit funds that are being retrieved or frozen, these bad actors seem to be getting away almost scot-free - Europol estimates that less than 2% of criminal assets are recovered[3]. This is not for a lack of trying.

Recent research by LexisNexis[4] suggests that the total annual cost of financial crime compliance across all financial institutions globally is $180.9bn.

Why are these financial crime compliance efforts so seemingly ineffective? Matthew Redhead, Associate Fellow at RUSI explains:

"Firstly, the AML framework that has developed over the last three decades is relatively static but financial criminality develops and grows like an organism, constantly testing the boundaries and coming up with new ideas. Secondly, the framework is fragmented - in financial institutions, AML departments have grown, becoming increasingly specialised to meet the growing detailed requirements of regulatory demand. As they become more specialised, they become delinked and decoupled from each other. They exist in their own stovepipes, not in the complex web of interaction that we see in the criminal world."

Financial firms must, therefore, transform from this fragmented approach - which creates gaps for criminals to exploit - to a more integrated, comprehensive view of all their financial crime risks, supported by the latest technology.

"In the fight against financial crime, fragmentation is our greatest enemy."[5]

- Christopher Woolard, Executive Director of Strategy and Competition at the FCA

3 https://www.europol.europa.eu/newsroom/news/does-crime-still-pay

4 https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report

5 https://www.fca.org.uk/news/speeches/technology-and-global-ties-turning-tide-financial-crime

Obstacles to overcome

As the saying goes, 'if it were easy, everyone would be doing it' and creating a more unified way of addressing money laundering is definitely not easy with several common challenges facing financial firms. Whilst it is tempting to blame complex and ever-changing regulation for some of these difficulties - and they certainly are a contributory factor - most of the barriers to achieving holistic AML are internal to firms.

No appetite for 'rip and replace'

Incumbent technology stacks used for AML purposes are often based on older technologies, which tend to be more inflexible and have problems coping with the exponential increases in transaction volumes experienced over the last few years. Also, multiple systems exist and are typically segregated by line of business and/or product, usually as a result of organic growth or through mergers and acquisitions. Despite these obvious drawbacks, there is little appetite to engage in large scale 'rip and replace' projects due to the multi-year timescale, the cost and ultimately, the risk involved.

Process-driven approach

AML is typically managed using a set of linear processes with few feedback loops between each discrete process step. Not only does this exacerbate the silo-effect, but it acts as a barrier to considering AML from either a data-driven or customer-centric perspective.

Process-driven approaches are followed for the onboarding and ongoing monitoring of customers for KYC purposes. Customer risk reviews most typically occur on a periodic basis, depending on the level of risk attributed to the customer at the point of onboarding. Low-risk customers may not receive a file refresh for up to five

years, allowing money mules, for example, to slip through the net. At the point of onboarding, money mules pass as low-risk customers but their ongoing behaviour is clearly not that of a normal customer and won't be identified for five years in this instance.

Some firms are moving to more trigger-based reviews but research from 2017[6] showed that nearly 90% of financial institutions were still performing ongoing KYC checks on a periodic basis.

Transaction monitoring too is largely process-driven. Rule-based systems generate alerts (a large proportion of which are false positives) which are investigated by analysts and either escalated, reported as Suspicious Activity Reports (SARS) or resolved. Rarely are the results of these investigations fed back into the customer monitoring process to trigger a risk review.

The silo effect

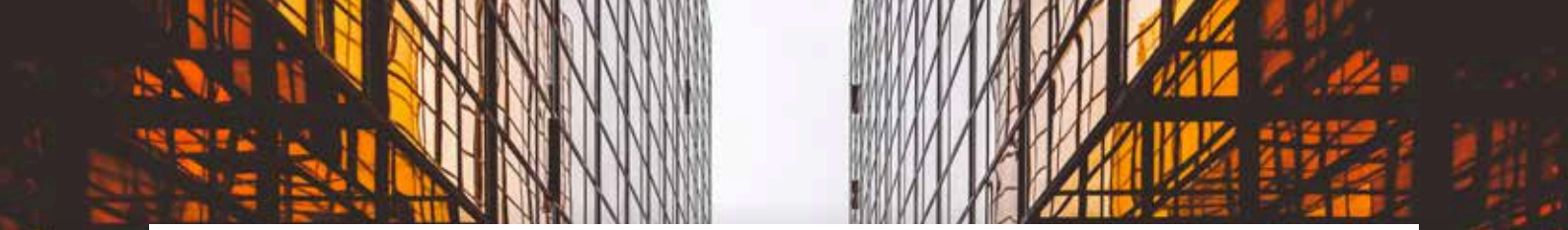
As Matthew Redhead described above, financial institutions tackle financial crime compliance in a very siloed manner. Operating models for AML typically follow the contours of the business - with separate teams and processes for different lines of business such as retail banking, wealth management, capital markets and commercial banking. Data is siloed according to type - customers, accounts, transactions and separate teams are using the data for different purposes.

6 https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/kyc-compliance-the-rising-challenge-for-financial-institutions-special-report.pdf

"Silos can sometimes cause damage...isolated departments, or teams of experts, may fail to communicate, and thus overlook dangerous and costly risks. Fragmentation can create information bottlenecks and stifle innovation...silos can create tunnel vision or mental blindness."[7]

Breaking down silos is hard in AML because there is a tension between the need for specialist expertise on the one hand and a joined-up vision of financial crime risks on the other. It is possible though, and the best place to start is to move to a client-centric view of the world.

7 Gillian Tett (2015) The Silo Effect Little Brown



Customer-centricity is key. So is understanding customer behaviour

A firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means scrutinising transactions to ensure that they are consistent with what the firm knows about the customer, and taking steps to ensure that the firm's knowledge about the business relationship remains current.[8]

Regulatory supervisors, such as the UK's Financial Conduct Authority (FCA), mandate the need for the ongoing review of customers to assess all clients' activities and behaviours over time. Fundamental to this is the ability to bring together disparate sets of customer-related data so that there is a 'single view of the customer' - not just at a snapshot in time but across the entire customer lifecycle.

Consolidating fragmented customer data sets to obtain a complete record of a customer's accounts across lines of business, geographies, and products then allows regulated firms to use that data more productively.

8 FCA (August 2020) Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)

Customer behavioural analytics is an increasingly important tool in fighting financial crime. As we saw earlier, financial criminality is constantly changing and using rule-based transaction monitoring alone, without a full view of the customer behaviour, is unlikely to be as effective in identifying new patterns of suspicious activity

Rule-based systems are typically based on red flags - thresholds developed from patterns of activity that indicate known financial crime typologies. These are then applied to transaction data. Two problems arise here:

- The first is that transaction data alone gives a relatively small number of data attributes to work with, which are often either not populated or incorrect due to data quality issues.
- The second problem is that using only red flags and rules on these data sets makes it hard to distinguish between what is legitimate and what is not from a behavioural perspective.

For example, in the US, the last hour of trading on the New York Stock Exchange on the third Friday in the months of March, June, September and December is known as the 'triple witching hour' - the quarterly expiration data of stock market index futures and options and stock options. Obviously, there is a spike in trading volumes and therefore payment activity.

For financial criminals, this is the ideal opportunity to hide criminal activity in plain sight because there is so much cash in the market. However, rules-based systems may not be able to detect this as the payment activity may appear to be legitimate - they are unable to factor in how humans might behave in response to certain events.

Customer behaviour analytics, however, does provide these sorts of insights - and can help to more accurately identify suspicious activity. It works like this:

01 Create a 360-degree view by bringing together customer identities, associations, transaction patterns and behaviours across the organisation

02 Use that data to compare the customer's current behaviour with that over their entire relationship with the organisation

03 Compare that customer's behaviour to other similar customers (segmented according to similar profiles e.g. similar industries for corporate customers or similar age ranges for individuals)

04 Compare that customer's behaviour to all other customers

Steps 2-4 allow anomalous behaviour to be identified and investigated further, even if rules-based alerts have not been triggered. Many different types of behaviour can be identified in this manner - unusual times of the day for transactions, unusual counterparties, use of atypical currencies etc. none of which may be caught by existing red flags. As well as the increased likelihood of detecting suspicious activity, the other key benefit of customer behavioural analytics is that it is much harder for financial criminals to evade. Well known red flags and the rules used to trigger them are easy to game - detection of anomalous behaviour, much less so.

Introducing Napier's Client Activity Review

Client Activity Review (CAR) provides regulated firms with that customer-centric view of their data in a way that doesn't require the complete re-architecting of a firm's data infrastructure. Customer behavioural analytics are layered over the top to enable you to truly Understand Your Customer, rather than just Know Your Customer.

CAR combines all customer data, including transactions, payments and screening results (such as underlying changes in beneficial ownership and KYC data), into one automated control centre which allows you to triage all anomalies and behavioural changes in light of a full view of the customer.

Key Features

DATA INTEGRATION

CAR can integrate data from your existing KYC and transaction monitoring systems without the need to replace them - immediately providing you with a full transaction history complete with any alerts that have been triggered for that customer over a specific time period.

AUTOMATIC REVIEWS

Client reviews are automatically scheduled according to the required frequency - this can be based on any characteristic of a customer, not just the risk score. For example, if customer information changes because they move house or perhaps become a director of a company in a high-risk country, a view can be triggered.

REAL TIME GRAPHICAL ANALYSIS

CAR presents a real-time graphical analysis of a customer's behaviour over a dynamically selected period of time, highlighting any anomalies in comparison to other similar customers. Comparisons of behaviour against the previous time period can also be presented, allowing deep investigations into the likelihood of suspicious activity without having to switch between different views or applications.

COMPLEMENTS RULES-BASED MONITORING

Customer behavioural analytics also allows the use of rules to determine whether the observed behaviour is out of line with expectations based on the results of the KYC performed at on-boarding e.g. if the customer was on-boarded as low risk but is exhibiting behaviour more suggestive of nefarious activity.

ENHANCES RISK ASSESSMENT

CAR significantly enhances the assessment of customer risk. By unleashing the power of machine learning, traditional rule-based deterministic scores can be augmented with machine learning generated scores based on multiple data points and aggregations.

Key Benefits

No matter the size of the financial institution, Napier's Client Activity Review will provide benefits.

For financial crime compliance teams in large Tier 1 banks, overheads can be reduced significantly by aligning teams and systems to handle AML more effectively. There is a holistic view of each client - and a holistic approach throughout the bank. Relationship Managers can benefit from this also - ongoing reviews provide a means to manage the relationship effectively and even identify opportunities to up- and cross-sell products to existing customers.

For smaller banks with small compliance teams that are having to do everything, relying on manual processes and making use of spreadsheets, CAR can automate all of that, providing one single system for managing AML.

For all organisations, Napier's CAR allows you to:

01 Take action when it really matters because the system is triggered, in almost real-time, by data that is at odds with the customer's unique expected behaviour

02 Automate the review of client activity on an ongoing basis, allowing you to move towards dynamic risk-scoring and perpetual KYC

03 Complete more suspicious activity checks, more often because client activity reviews are fully automated

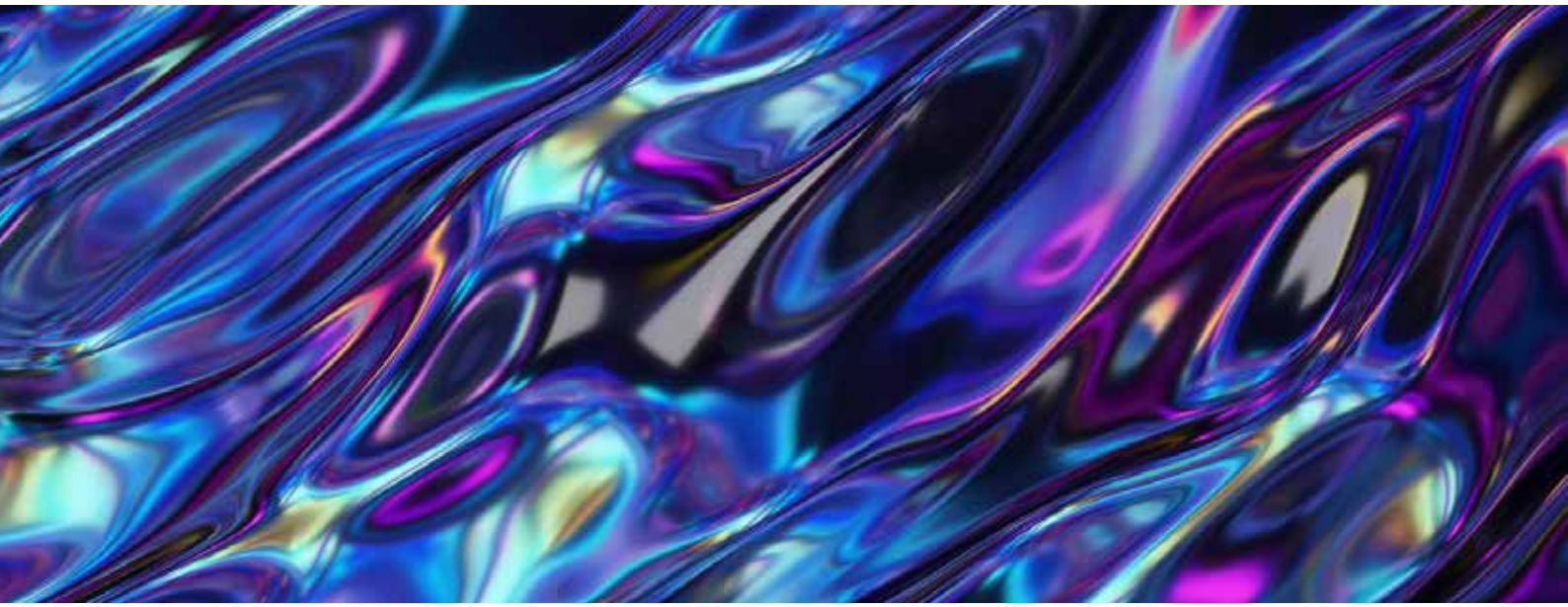
04 Focus on reviewing suspicious flagged activities to understand why they've occurred and determine the urgency of follow-up action rather than spending time on laborious tasks and wading through huge amounts of data

Napier's Client Activity Review is your first step towards holistic AML.

There is no need to replace existing systems - CAR adds that extra level of efficacy, control and customer-centric insight to improve your AML framework.

CAR solves the problem of siloed data - bringing KYC and transaction monitoring data together to provide a holistic picture of your clients' behaviour.

And finally, CAR integrates insights from transaction monitoring back into the ongoing KYC monitoring and review, allowing the dynamic management of customer risk that linear, process-driven systems are not able to achieve.



About Napier

Napier is a London-based specialist compliance technology company founded in 2015, with offices in Kiev, Singapore, Australia and Malaysia.

Trusted by the world's leading financial institutions, our next generation Intelligent Compliance Platform is transforming AML & Trade Compliance.

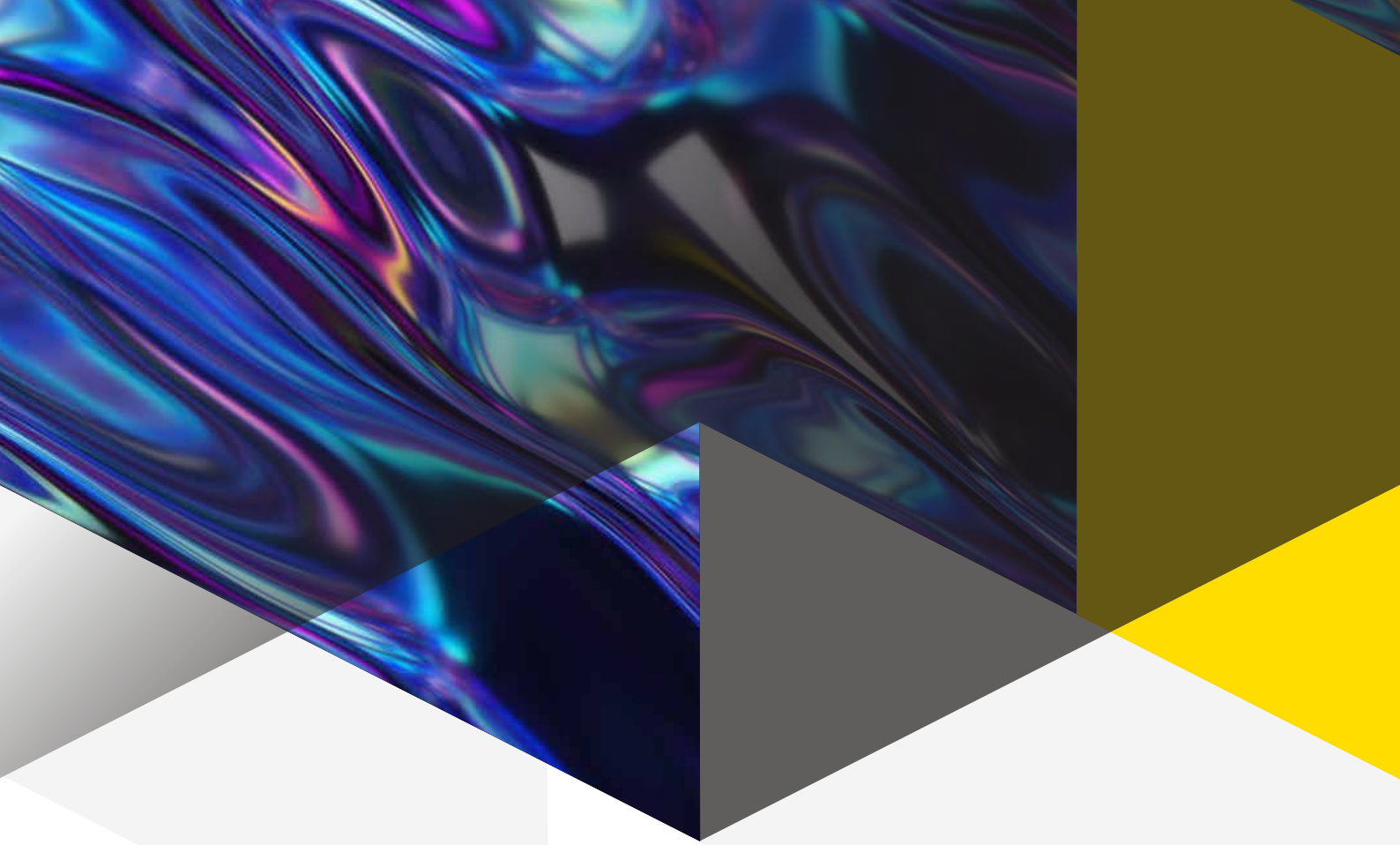
We design and build compliance technology to help companies in any sector comply with money laundering regulations, detect suspicious transactions, screen potential customer & business partners and help analysts predict customer behaviour.

Napier uses deep industry knowledge and cutting-edge technologies such as artificial intelligence and machine learning to help businesses detect suspicious behaviours and fight financial crime.

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



NAPIER

NAPIER.AI