EBOOK: FINANCIAL CRIME

How AI can improve the detection of evolving typologies driving financial crime

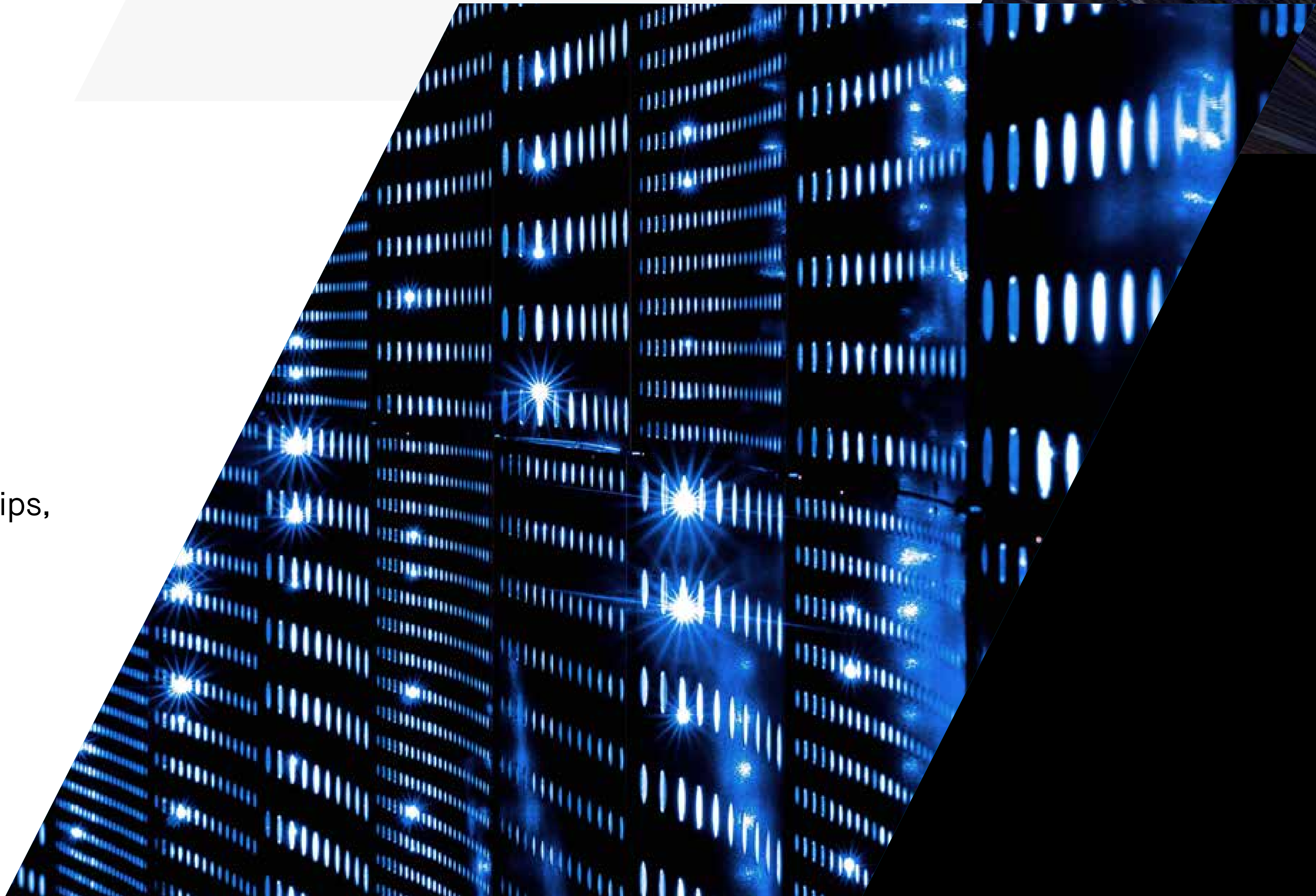
AUTHOR:

Dr Janet Bastiman
Chief Data Scientist,
Napier

CONTRIBUTOR:

Emma Miller
Global Head of Strategic Partnerships,
Data & Analytics,
London Stock Exchange Group

NAPIER



Contents

Anti-money laundering frameworks powered by AI can be more effective than rules-based systems in the fight against financial crime because they surface more valuable insights, detect anomalies and tune out the white noise.

Introduction

Collectively, the ecosystem for preventing financial crime is under-performing, as evidenced by the familiar statistic that as little as 1% of all illicit transactions in Europe are recovered, and it's likely the actual figure could be even lower.

The upshot is that many terrible crimes are going unpunished, and criminals are not being brought to justice. Bad actors intent on abusing the global financial system are not unlike the mythical hydra: for every money laundering opportunity that is thwarted, they find another two.

Encouragingly, there is a desire and willingness from financial institutions, law enforcement, policy-makers and technology vendors to work together to improve this situation and fight financial crime more effectively.

We are seeing more examples of collaboration in information and intelligence sharing, as well as emerging partnerships between public and private actors to address these problems.

Examples of private sector collaborations include TMNL in the Netherlands and Invidem in the Nordic region.

Technology and innovation are also making a critical contribution, with the latest advances in artificial intelligence (AI) bringing new dynamism and flexibility to the fight against increasingly agile criminal elements.

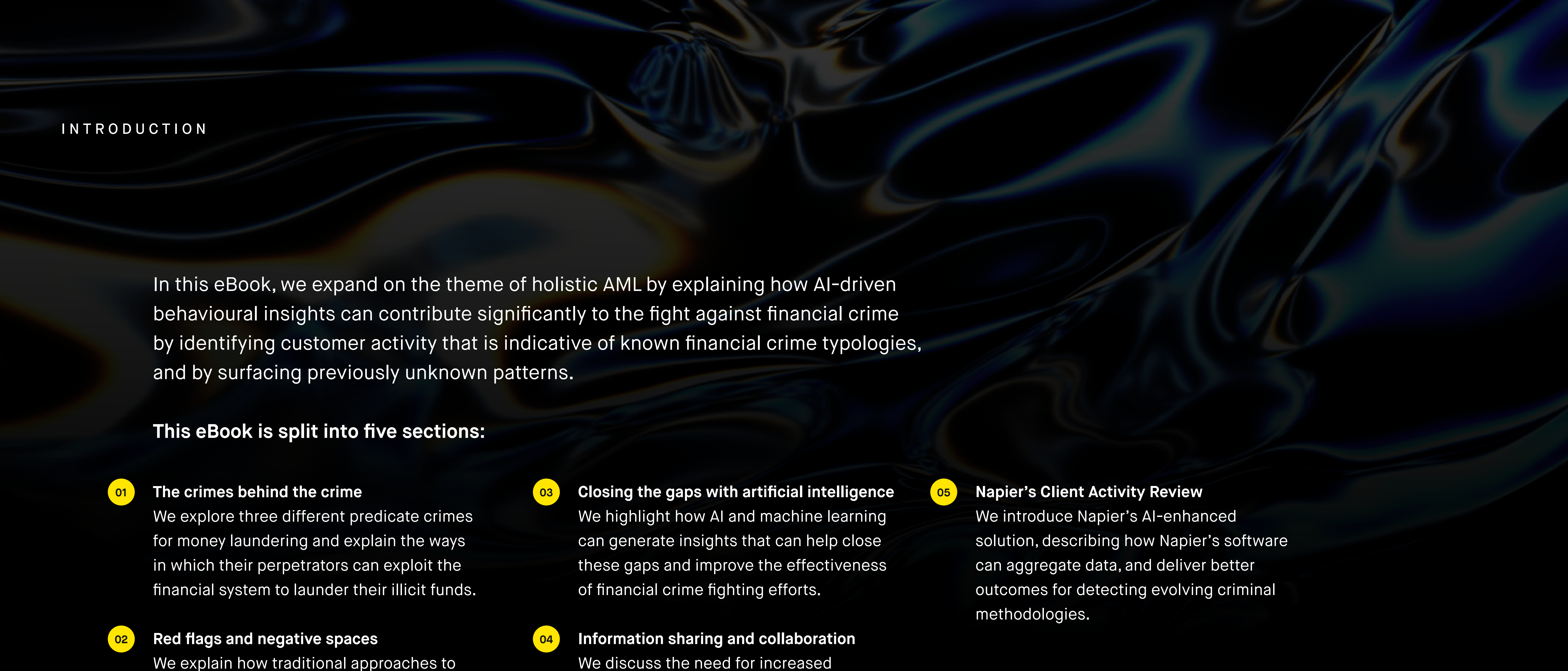
When faced with the day-to-day complexities of navigating financial crime compliance regulations and processes, it can be easy to lose sight of the human suffering and harm associated with money laundering and its predicate crimes.

Human trafficking, corruption, wildlife smuggling and cybercrime are the specialty of organised criminal gangs, who will stop at nothing in the pursuit of profit and have no qualms in exploiting the financial system to legitimise the ill-gotten proceeds of their crimes.

> **It can be easy to lose sight of the human suffering and harm associated with money laundering and its predicate crimes.**

However, it is precisely by having a greater understanding of how these crimes manifest in patterns of money-laundering behaviour (also known as typologies) that will improve risk identification and investigative activities. Insights provided through the smart utilisation of AI can make a significant contribution to identifying customer activity that is indicative of known financial crime typologies and can also help to surface previously unknown patterns.

In a previous eBook, we proposed the need for a more holistic, customer-centric approach in the fight against financial crime, an approach which puts behaviour at the centre of triggering alerts and consequent investigations within financial institutions.



INTRODUCTION

In this eBook, we expand on the theme of holistic AML by explaining how AI-driven behavioural insights can contribute significantly to the fight against financial crime by identifying customer activity that is indicative of known financial crime typologies, and by surfacing previously unknown patterns.

This eBook is split into five sections:

01 **The crimes behind the crime**
We explore three different predicate crimes for money laundering and explain the ways in which their perpetrators can exploit the financial system to launder their illicit funds.

02 **Red flags and negative spaces**
We explain how traditional approaches to financial crime typologies, including the publication of red flags on a periodic basis, leave gaps that criminals take advantage of.

03 **Closing the gaps with artificial intelligence**
We highlight how AI and machine learning can generate insights that can help close these gaps and improve the effectiveness of financial crime fighting efforts.

04 **Information sharing and collaboration**
We discuss the need for increased collaboration and data sharing of these critical criminal typologies.

05 **Napier's Client Activity Review**
We introduce Napier's AI-enhanced solution, describing how Napier's software can aggregate data, and deliver better outcomes for detecting evolving criminal methodologies.

01 The crimes behind the crime

$23 billion

Estimated annual proceeds of the illegal wildlife trade.

$1 trillion

Paid in bribes each year worldwide

40.3 million

People estimated to be victims of modern slavery

Predicate offences are defined as any offence which results in proceeds being generated that may become the subject of an offence as defined this UNDOC convention, in article 6 which addresses the criminalisation of the laundering of proceeds of crime.

Criminals that commit predicate offences are highly motivated to maximise profits, hence, the premise behind anti-money laundering (AML) measures is to detect these criminals through analysis of their financial behaviour and interactions with the legitimate economy – namely financial institutions.

Detection of criminals attempting to launder money can provide law enforcement with the intelligence to combat financial crime and unearth the bad actors perpetrating the predicate crimes.

According to the Financial Action Task Force (FATF), the definition of what constitutes a predicate offence is the responsibility of individual countries to specify.

In some jurisdictions, such as the UK, predicate offences are defined on an 'all crimes' basis, which means that money laundering offences are not restricted to a list of defined predicate crimes. Elsewhere, in jurisdictions such as the European Union and the US, prescribe predicate crimes in law.

For example: the EU's Sixth Anti-Money Laundering Directive lists 22 predicate offences including human trafficking and migrant smuggling, environmental crime, tax crime, cybercrime, fraud, corruption, participating in organised crime groups, and racketeering.

Overleaf, we take a closer look at three of these offences - human trafficking, illegal wildlife trading, and corruption - to explore how the financial system is used to launder the proceeds of these crimes.

Each has a different but equally devastating societal impact.

Illegal wildlife trading

Environmental crime, which includes the offence of illegal wildlife trading (IWT) has come to the fore as a significant predicate crime for money laundering in recent years.

Like drug trafficking, the trade in protected species of flora and fauna is the remit of organised criminal gangs, however it is seen by criminals as offering larger profits and lower penalties than other, more established types of criminal activity.

The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) defines wildlife crime as 'the taking, trading (supplying, selling or trafficking) importing, exporting, processing, possessing, obtaining and consumption of wild flora and fauna…in contravention of national or international law'.

Over 37,000 species of wildlife are covered by CITES, including those threatened with extinction and others that are at risk of overexploitation.

Estimates of the proceeds of IWT are difficult to arrive at, but a recent report by the World Bank places it somewhere in the region of $7-23bn per year.

In 2020, FATF issued a report entitled 'Money Laundering and the Illegal Wildlife Trade,' its first global report on IWT, which it considers to be a 'major transnational organised crime that fuels corruption, threatens biodiversity and can have significant public health impacts'.

The latter impact mentioned highlights the spread of zoonotic diseases, which are those which pass from animals to humans, including the likes of Ebola, MERs, SARs. The most recent and high-profile instance of zoonotic disease is the COVID-19 virus, though no definitive link has been established between IWT and the global Coronavirus pandemic as of yet.

> **Proceeds of IWT are difficult to quantify, but the World Bank estimated that it is as much as $23bn per year.**

In 2021, the UN adopted a resolution to combat IWT, Resolution 73/343 which requires Member States to treat IWT as a predicate crime under domestic money laundering offences.

Along with the UN and FATF, the Egmont Group (a united body of 167 financial intelligence units, or FIUs) has also emphasised the importance of 'following the money' when it comes to IWT for three key reasons.

01 It can lead to the identification of the wider networks of organised criminals and therefore reduce the profitability of wildlife trafficking as these criminals are typically implicated in associated offences such as corruption and complex fraud.

02 The penalties for money laundering are generally more severe than the punishments for illegal wildlife crime, which may serve as a greater deterrent.

03 Tracing illicit financial flows relating to IWT is an important investigative tool when it comes to preventing IWT.

Illegal wildlife trading - continued

Similarly to legitimate businesses, illegal wildlife traffickers make use of well-defined supply chains that can span several jurisdictions and comprise source, transit, and destination countries. Source countries are those where the wildlife originates, and it may be poached, killed, or procured from these countries.

For example, Kenya and South Africa are both significant sources countries for elephant ivory which is primarily destined for markets in Asia, with UNDOC estimating that Vietnam, China, and Cambodia together comprising 88% of the destination market for ivory tusks.

Understanding these supply chains, which can vary species by species, and the types of actors involved in the process, is key in identifying the financial activities and behaviours that are indicative of IWT.

According to FATF, laundering of proceeds occurs at multiple points in the chain, and like other predicate crimes, multiple methods are used to clean the money.

These include:

01 Placing and layering of funds in the legitimate financial sector

02 Use of shell companies to conceal payments and co-mingle lawful and illicit funds

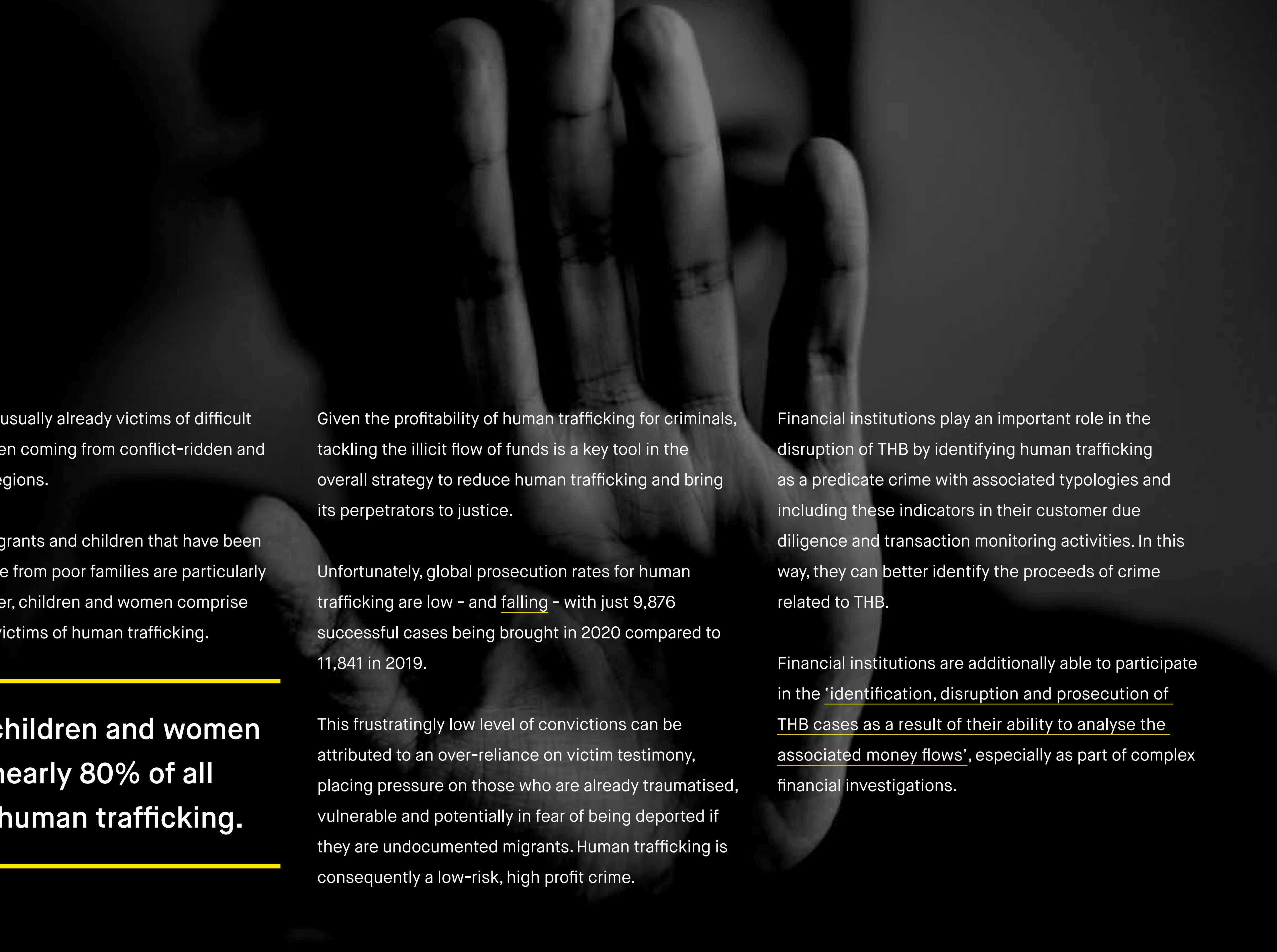
03 Purchasing high value goods, including real estate and other luxury items

04 Money value transfer systems, such as Hawala

For financial institutions, the illegal wildlife traffickers' use of the formal financial system is where they can most easily take action and where their regulatory obligations reside.

Many financial institutions are now including IWT as a specific financial crime risk, but there are challenges associated with being able to distinguish behaviour that is related to IWT from that which may be indicative of other types of crime.

Human trafficking



The most recent estimate cites 40.3 million victims of modern slavery - men, women and children trafficked for forced labour, including sexual exploitation and forced marriage.

In 2018, UNODC estimated that 50% of victims were trafficked for sexual exploitation, 38% for forced labour and the remainder for other forms of exploitation.

With the profits from this horrendous crime averaging $150bn per year, organised gangs are expanding their portfolio of activities to include trafficking in human beings (THB) by taking advantage of global dislocation, making it one of the fastest growing global crime categories.

As well as being a violation of human rights, FATF describes human trafficking as 'also one of the most significant generators of criminal proceeds in the world'.

Victims of THB are usually already victims of difficult circumstances, often coming from conflict-ridden and poverty-stricken regions.

Undocumented migrants and children that have been abandoned or come from poor families are particularly vulnerable. Together, children and women comprise nearly 80% of all victims of human trafficking.

Together, children and women comprise nearly 80% of all victims of human trafficking.

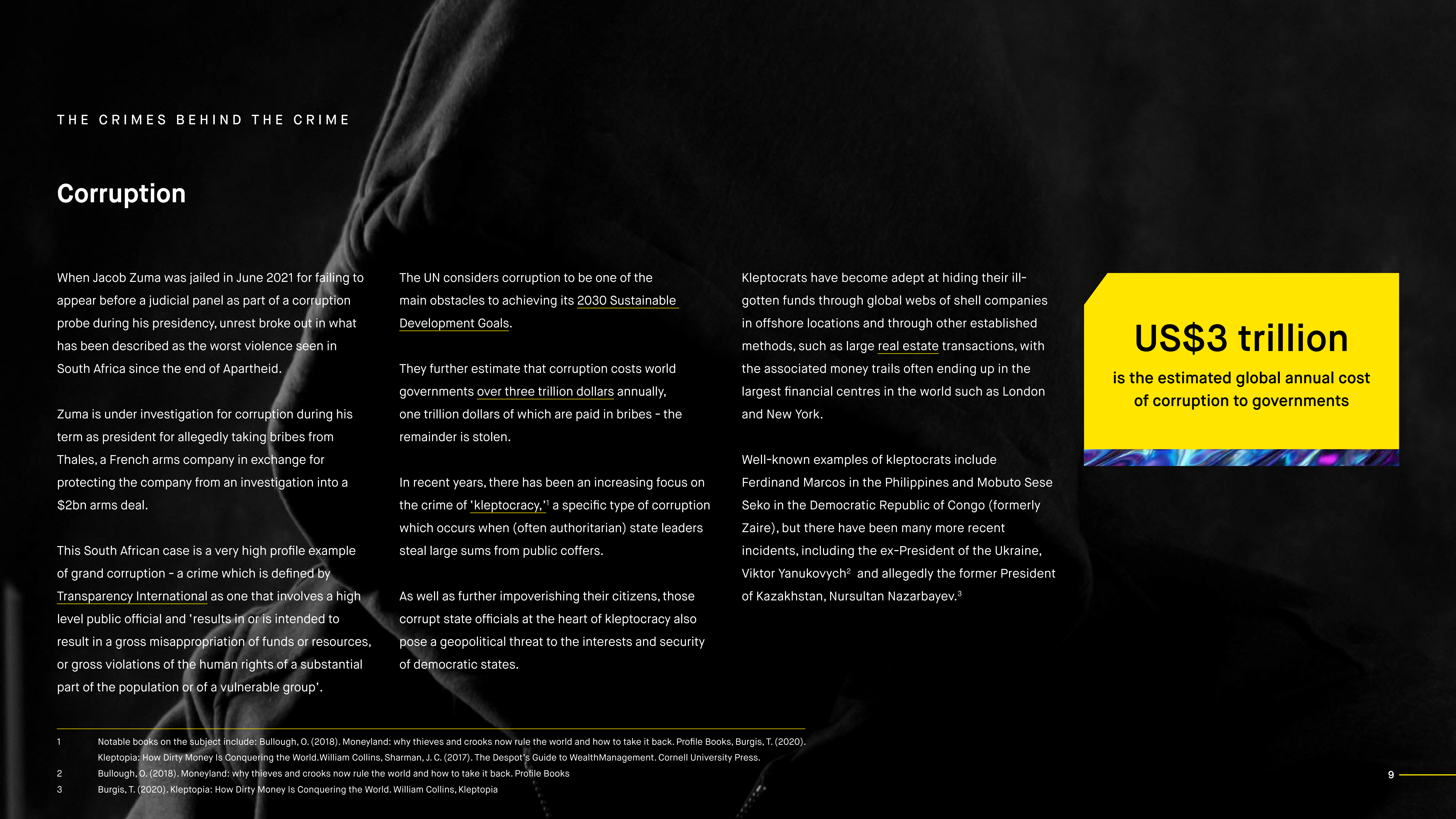
Given the profitability of human trafficking for criminals, tackling the illicit flow of funds is a key tool in the overall strategy to reduce human trafficking and bring its perpetrators to justice.

Unfortunately, global prosecution rates for human trafficking are low - and falling - with just 9,876 successful cases being brought in 2020 compared to 11,841 in 2019.

This frustratingly low level of convictions can be attributed to an over-reliance on victim testimony, placing pressure on those who are already traumatised, vulnerable and potentially in fear of being deported if they are undocumented migrants. Human trafficking is consequently a low-risk, high profit crime.

Financial institutions play an important role in the disruption of THB by identifying human trafficking as a predicate crime with associated typologies and including these indicators in their customer due diligence and transaction monitoring activities. In this way, they can better identify the proceeds of crime related to THB.

Financial institutions are additionally able to participate in the 'identification, disruption and prosecution of THB cases as a result of their ability to analyse the associated money flows', especially as part of complex financial investigations.



Corruption

When Jacob Zuma was jailed in June 2021 for failing to appear before a judicial panel as part of a corruption probe during his presidency, unrest broke out in what has been described as the worst violence seen in South Africa since the end of Apartheid.

Zuma is under investigation for corruption during his term as president for allegedly taking bribes from Thales, a French arms company in exchange for protecting the company from an investigation into a $2bn arms deal.

This South African case is a very high profile example of grand corruption - a crime which is defined by Transparency International as one that involves a high level public official and 'results in or is intended to result in a gross misappropriation of funds or resources, or gross violations of the human rights of a substantial part of the population or of a vulnerable group'.

The UN considers corruption to be one of the main obstacles to achieving its 2030 Sustainable Development Goals.

They further estimate that corruption costs world governments over three trillion dollars annually, one trillion dollars of which are paid in bribes - the remainder is stolen.

In recent years, there has been an increasing focus on the crime of 'kleptocracy,'[1] a specific type of corruption which occurs when (often authoritarian) state leaders steal large sums from public coffers.

As well as further impoverishing their citizens, those corrupt state officials at the heart of kleptocracy also pose a geopolitical threat to the interests and security of democratic states.

Kleptocrats have become adept at hiding their ill-gotten funds through global webs of shell companies in offshore locations and through other established methods, such as large real estate transactions, with the associated money trails often ending up in the largest financial centres in the world such as London and New York.

Well-known examples of kleptocrats include Ferdinand Marcos in the Philippines and Mobuto Sese Seko in the Democratic Republic of Congo (formerly Zaire), but there have been many more recent incidents, including the ex-President of the Ukraine, Viktor Yanukovych[2] and allegedly the former President of Kazakhstan, Nursultan Nazarbayev.[3]

US$3 trillion

is the estimated global annual cost of corruption to governments

[1] Notable books on the subject include: Bullough, O. (2018). Moneyland: why thieves and crooks now rule the world and how to take it back. Profile Books, Burgis, T. (2020). Kleptopia: How Dirty Money Is Conquering the World.William Collins, Sharman, J. C. (2017). The Despot's Guide to WealthManagement. Cornell University Press.

[2] Bullough, O. (2018). Moneyland: why thieves and crooks now rule the world and how to take it back. Profile Books

[3] Burgis, T. (2020). Kleptopia: How Dirty Money Is Conquering the World. William Collins, Kleptopia

Corruption - continued

High-profile leaks such as the Panama Papers in 2016, the Paradise Papers in 2017, the FinCEN Files in 2020, and the Pandora Papers in 2021 have shed light on the scale and sophistication of methods used to hide dirty money, as well as some of the elaborate schemes used to avoid tax and work around international sanctions.

According to the International Consortium of Investigative Journalists, the Panama Papers held details of the offshore holdings of 140 politicians and public officials globally. All of these revelations point to a situation where more must be done to fight corruption.

In June 2021, the UN held a special General Assembly Session against corruption and introduced a political declaration outlining its commitments to tackling corruption.

In addition, AML legislative frameworks have been tightened up in recent years - partly in response to the leaks mentioned above - with stricter rules introduced around the identification of ultimate beneficial owners (UBOs), namely the 5th and 6th Anti-Money Laundering Directives in the EU and the 5AMLD, the Anti-Money Laundering Act 2020 in the US.

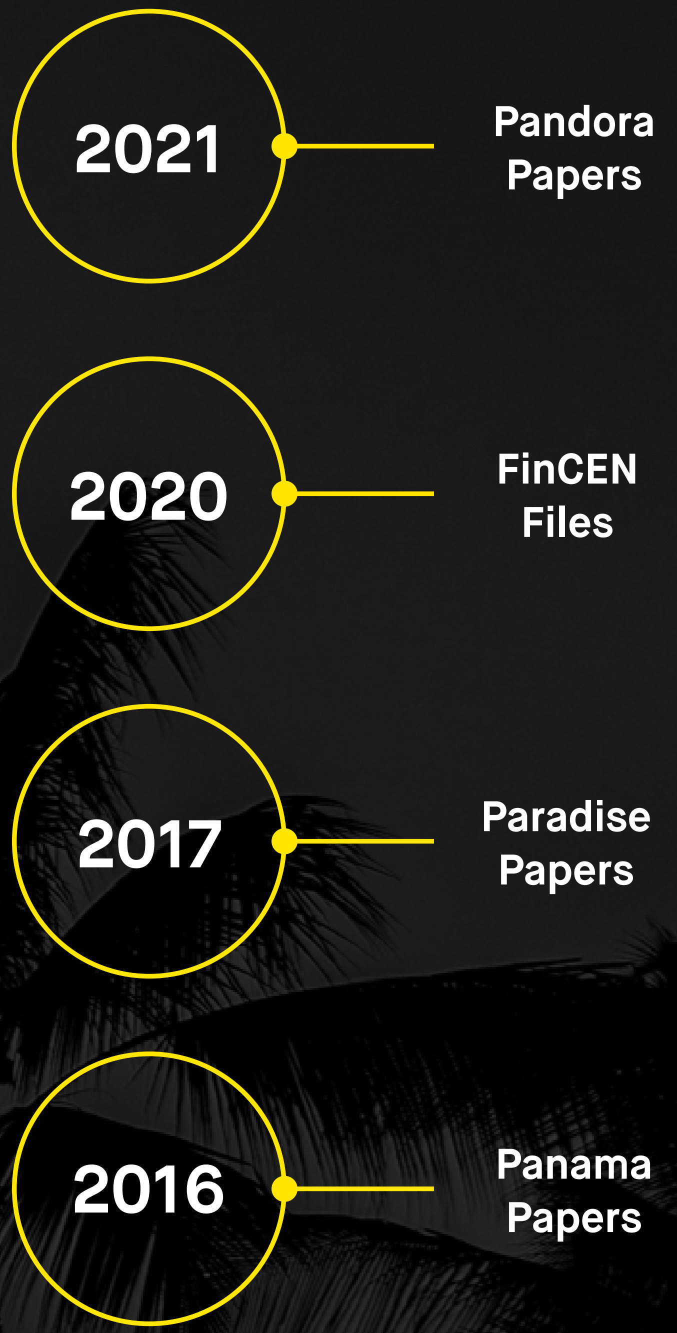
Corruption, though, has long been considered a predicate crime for money laundering and the most recent typology details from FATF date back to 2011.

Preventative controls revolve around identifying customers who may be at risk of corruption - politicians and their associates - usually referred to as Politically Exposed Persons (PEPs). Screening against established lists of 'names' and then applying higher standards of due diligence where PEPs are identified is a standard part of the customer onboarding process.

Determining UBOs is also usual practice, though complex corporate structures including multiple trusts and shell companies in offshore jurisdictions are still incredibly difficult to unpick.

In terms of detecting suspicious activity relating to corruption, financial institutions must understand the indicators of possible laundering of the laundering of the proceeds of corruption, many of which need to be understood in the context of whether a customer is a PEP, or is linked to a PEP as a family member or known associate.

HIGH-PROFILE LEAKS



The crimes behind the crime: how they converge

The crimes behind the crime: how they converge
Discussing these three types of predicate crime separately also risks glossing over some of the added complexities associated with the convergence of various types of predicate crime.

Very rarely does an organised crime group focus on only one type of offence - they are more likely to have multiple revenue streams, which they can switch between should one stream face any risk of exposure.

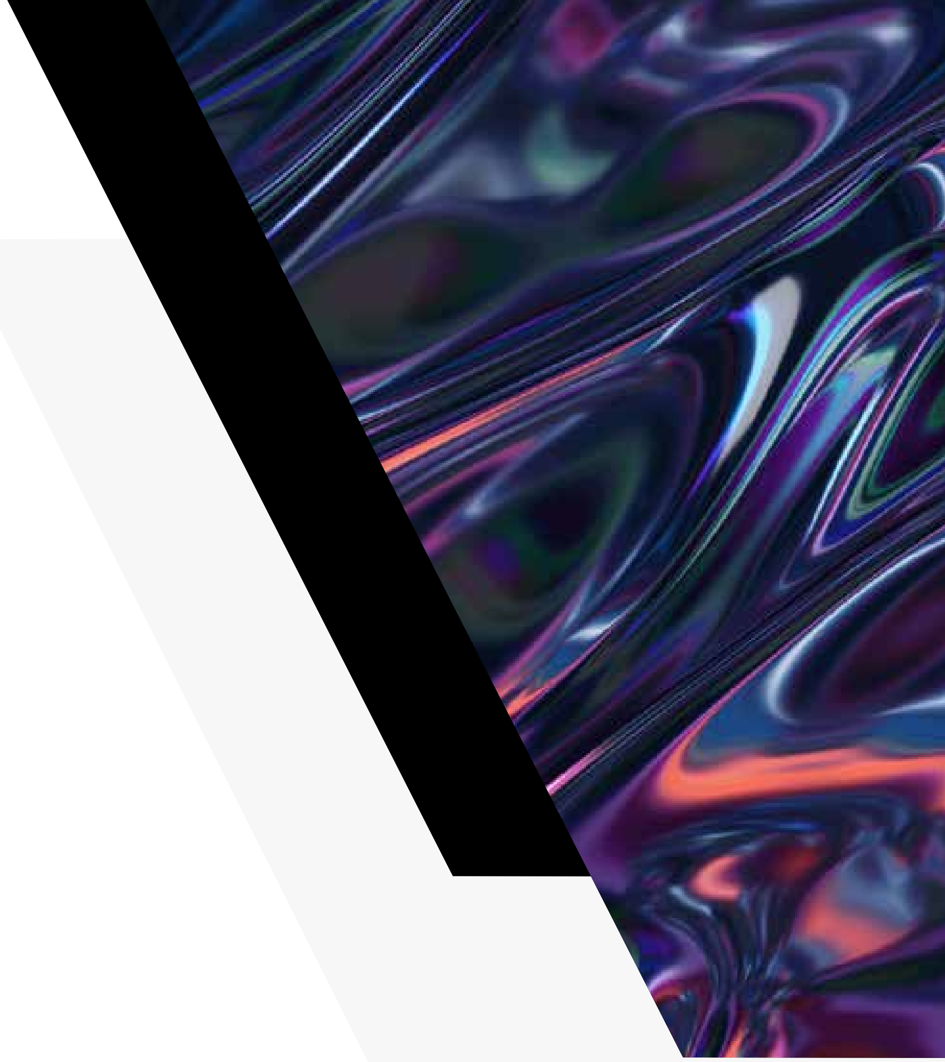
For example, research has shown that IWT and corruption often go hand-in-hand.

Research on the problems and solutions to IWT, even the types and methods, through the lens of anticorruption is in short supply. The gap in knowledge urgently needs addressing, as IWT is driven by corruption as for trafficking networks to be able to move their illicit goods and for IWT to thrive, it's necessary for the perpetrators to build relationships with public officials through corrupt means such as bribery.

Elsewhere, drug trafficking groups may also be implicated in human trafficking, utilising similar networks and channels to traffic both narcotics and people.

For both financial institutions and law enforcement, crime convergence makes it harder to make the links between money laundering red flags and predicate crimes, exacerbating the already challenging process of following the money.

> Very rarely does an organised crime group focus on only one type of offence.



02 Red flags and negative spaces

Despite the unsatisfactory recovery rates associated with the global anti-money laundering (AML) framework, there is a wealth of knowledge about predicate crimes and how criminals use the financial system to legitimise their ill-gotten gains.

Sharing this intelligence between standard setters, law enforcement, and regulated institutions forms a critical part of the efforts to combat money laundering.

International organisations (such as FATF and the Egmont Group) and national FIUs (for example the US Financial Crimes Enforcement Network (FinCEN) and the Australian Transaction Reports and Analysis Centre (AUSTRAC)) conduct research on the methods that criminals are using to place, layer, and integrate dirty money into legitimate economies.

Different types of predicate crimes are often associated with the same typologies for money laundering, largely because the perpetrators are organised crime gangs who are continually expanding their operating range.

For example, setting up shell companies which appear as legal business structures and allow them to infiltrate the legitimate market.

Recent research has shown that, irrespective of the predicate crime, the five most prevalent means for laundering money in 2020 included cash or quasi cash deposits, cash deposits through third party channels, use of 'money mules', use of money services businesses (MSBs), and the use of complex company structures to conceal UBO.

These are all well-known and well-documented techniques, with well-defined risk indicators.

Yet that same research also found that less than 65% of organisations surveyed believed themselves to be effective at mitigating just 50% of these money laundering methods.

Despite the high levels of research and intelligence sharing by FIUs and others, the work that is being done to identify typologies and red flags is not translating into sufficient levels of detection and prevention of money laundering.

Some of the terminology associated with this financial crime intelligence can be confusing, especially when trying to understand the distinction and relationship between predicate crimes, typologies and red flags.

Table 1 - Definitions of Key AML Terms

TERM	DEFINITION	EXAMPLE	ALSO KNOWN AS
Predicate Crime	Specific types of unlawful activities which give rise to prosecution for money laundering	Trafficking of human beings	Threats
Typology	Various techniques used by criminals to conceal, launder or move illicit funds	Funnel accounts - an account in one geographic area that recieves multiple cash deposits and then funds are withdrawn in a different geographic area	Methods
Red Flags	Warning signals that could indicate suspicious situations, transactions or activities	Frequest, multiple cash deposits made via an ATM under the usual cash reporting threshold	Risk Indicators

With respect to typologies and indicators, there are four factors to consider in explaining why the work being done to identify typologies is currently not as effective as it should be:

01 Intelligence on financial crime typologies is not generally made public. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), and initiatives such as the Joint Money Laundering Intelligence Taskforce (JMLIT) restrict access to such information.

Information that is public is also accessible to those wishing to launder their illicit funds, who will likely adapt their methods by finding the negative space to avoid those known risk indicators.

02 Red flags are used by regulated firms to create rules within their transaction monitoring systems, often using thresholds. These rules are deterministic and, if understood by criminals, are easy to avoid. For example, a bank may have a threshold for the amount that can be deposited in cash, so criminals will deposit slightly less than this amount to avoid triggering the alert.

03 As with most types of risk management, financial crime typologies are based on historical data. Trying to predict the future based on the past will not uncover unknown threats or new techniques being used by money launderers.

04 One red flag or indicator alone is not sufficient to identify a pattern of suspicious activity relating to a typology. Financial institutions must ensure they have the relevant contextual information relating to that red flag, such as customer behaviour and other transactions, to determine the next course of action.

These shortcomings are well rehearsed, and some of the public/private intelligence sharing initiatives mentioned above are working towards addressing them. Technologies such as artificial intelligence also strengthen regulated firms' ability to analyse customer behaviour and contextual information as well as identify new and unknown indicators of financial crime.

03 Closing the gaps with artificial intelligence

Artificial Intelligence (AI) is an umbrella term for a range of statistical techniques that are increasingly being used to automate and accelerate tasks usually performed with human intelligence.

In AML, solutions largely utilise the branch of AI known as machine learning that uses algorithms to make predictions on data that it has not previously seen.

Machine learning is especially good at identifying things that are the same and things that are different in large patterns of multidimensional data.

This makes it the perfect candidate for AML solutions, since both customer due diligence and transaction monitoring involve vast data sets.

Machine learning is particularly useful when used to identify items that cannot be detected by rules-based solutions and for reducing the white noise associated with false positive alerts.

When combined with additional contextual data, such as customer behaviour, AI becomes even more powerful.

> Machine learning is particularly useful when used to identify items that cannot be detected by rules-based solutions and for reducing the white noise associated with false positive alerts.

How Napier's solution uses AI

Napier's Client Activity Review (CAR) is an example of how AI can be used to surface more valuable insights than traditional rules-based monitoring systems.

CAR is an AI-enhanced anti-financial crime solution that creates profiles of customers, aggregating data from onboarding with transactions and then monitoring customer behaviour over time.

Customers who share similar characteristics (same professional industry, geographic location, age, income bracket) can be grouped together and any unexpected or unusual behaviour by a customer within that group produces an alert to be investigated further.

There are two main ways that these insights can be used to improve the effectiveness of financial crime fighting:

01 Improving the detection of suspicious behaviour

AI on its own should not be viewed as a replacement for the rules-based approach that is more traditionally used in transaction monitoring.

Red flags and risk indicators remain a critical component in the detection of money laundering and can act as the first line of defence, picking off the 'low hanging fruit'.

Rather, systems such as CAR can enhance rules-based systems and be used to better combat the agility of the financial criminals and the emergence of new threats.

In a recent advisory from FinCEN on human trafficking, four new typologies of money laundering were identified and communicated, with associated behavioural and financial risk indicators.

One of these is the use of 'front companies' to disguise the true nature of an organisation and act as a cover for its illicit activities.

Typically, these companies are in the hospitality sector, such as bars and restaurants, massage businesses, and escort services.

Because these companies have the correct registrations and licenses and they generate income from the sale of drinks and food, they appear to be legitimate and are likely to be classified as low risk.

> **Red flags and risk indicators remain a critical component in the detection of money laundering**

However, AI solutions can compare the financial activity and behaviour of these businesses with others in the same industry to throw up any anomalous behaviour that could point to it being a front company for predicate crimes like human trafficking.

This might be, for example, transactions that are not expected in that line of business such as covering medical expenses, housing, transport and/or clothing.

By identifying these transactions as unusual, they can be flagged for further investigation.

02 Providing better insights for financial investigations

Transaction monitoring alerts are generally subject to a 'triage' system, where they are initially assessed by analysts, then escalated to team leads and/or more senior or specialist teams for further investigation.

Alerts at the highest level of triage tend to be the types of investigation where new typologies and risk indicators are identified by financial intelligence analysts with huge amounts of experience and knowledge.

By using AI, CAR can surface these types of anomalies much more quickly and can also provide analysts with more information and context about the alert.

For example, additional data sets can be integrated, along with the customer's full history. Link analysis can also be used to identify patterns involving more than one customer or client.

FIUs within financial institutions can then monitor whether these and other similar alerts are indicative of novel typologies and even, using pattern matching techniques, determine their applicability to predicate crimes.

A picture can then be built of the emerging ways in which criminals are exploiting the financial networks that can then feed back into the development of new risk indicators to share across the AML ecosystem and further shore up its defences.

How AI can deliver business value

Automate ongoing client activity reviews

Ongoing reviews ensure risk is assessed and monitored continuously.

- AI rapidly identifies key risk indicators based on discrepancies between real and expected behaviours
- AI automates client activity reviews by processing historical data and highlighting risks
- Supports faster decision-making with explainable AI

Reduce false positives in client screening

Screening customers is a regulatory requirement that also reduces exposure to risk.

- Accuracy is increased by automating a four-eyes check process
- Screening for PEPs / adverse media is automated
- Efficiency is increased by reducing time to review hits and through better prioritisation of alerts

Detect unusual and unknown patterns

Static rules have limitations in capturing unusual behaviours because they comprise pre-defined criteria which cannot be rapidly adapted to detect evolving criminal behaviours. AI-enhanced rules-based systems offer a powerful solution to this problem.

- AI improves the quality of alerts by creating a challenger score to use with rules-based scoring, thus reducing overall risk
- AI decreases risk by detecting unusual data correlations
- AI increases efficiency by providing additional insights and pointing analyst towards clients with higher risk

DATA: THE CRITICAL INGREDIENT

Emma Miller, Global Head of Strategic Partnerships, Data & Analytics, London Stock Exchange Group

Sophisticated technology solutions can help tackle the sheer volume of data that regulated firms manage as part of their AML endeavours.

The number of records in the Refinitiv World-Check database has increased significantly in the past two years by over 50% and the number of sanctioned entities and individuals has gone up by over 25% in a year.

Our 2021 Global Risk and Compliance Report shows that the appetite to invest in new technologies is strong – 86% of respondents agreed that technology has helped identify financial crime and 57% want to increase their tech spend, specifically on automation and digitisation.

Using AI and machine learning offers significant advantages in terms of speed, efficiency and accuracy. But to work effectively, attention must first be paid to data - a critical ingredient in the success of any AI approach.

> 86% of respondents agreed that technology has helped identify financial crime

DATA QUALITY

Data quality can be one of the biggest hurdles in implementing and maximising the use of AI and machine learning driven solutions.

And data quality isn't just about completeness and accuracy, though of course they are important, it is also about understanding the provenance of your data.

- **Where is it from?**
- **How was it collected?**
- **What are the implications for using that data to train machine learning models?**

This is especially important when sourcing data from third-party providers.

We make sure that we have strict inclusion criteria for World-Check, which reduces noise and helps to ensure accuracy.

Managing or handling your data in line with regulations should also be considered.

If you are integrating different data sets, you need to understand where and how data is being stored and whether it is being transferred from one jurisdiction to another.

All this needs to be done within the bounds of applicable data protection laws.

DATA: THE CRITICAL INGREDIENT - CONTINUED

DATA STRUCTURE

A key dependency for AI and machine learning systems is the structure of the data. Ingestion, normalisation and the combination of structured and unstructured data need to be considered - though some of the newer tools on the market are agnostic to data type and structure, which avoids the need for a costly and cumbersome data cleansing exercise.

You need to be able to specify how you want to slice and dice your data to the level of granularity and specificity you require.

For example, within World-Check we are in the process of introducing Special Interest Categories to records to indicate the specific offence or offences with which individuals and entities are allegedly associated.

Filtering data based on these categories will help you to focus on just what you need.

Combining structured and unstructured data can be a lengthy exercise but tools like Natural Language Processing are available to help find the most relevant pieces of information in context within unstructured data such as adverse media.

DATA COMPLETENESS

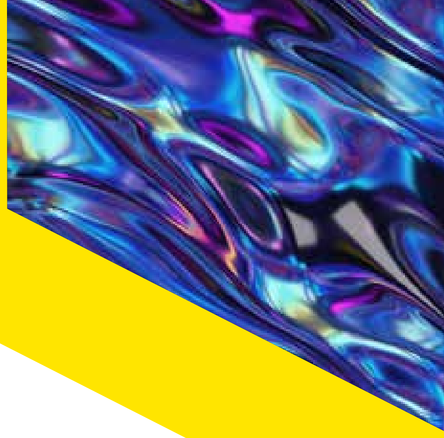
One of the significant advantages of tools like Napier's CAR is that it provides a single view of a customer. It is through the linking of data sets - in this case know your customer (KYC) and transaction monitoring - which enables AI to spot signals that would otherwise be invisible to a human analyst or impossible to connect over multiple links.

> We know that we are at an inflection point in the fight against financial crime.

For organisations to derive the best insights from this data, it needs to be complete.

We know that we are at an inflection point in the fight against financial crime. As an industry, we are asking difficult questions about effectiveness and the need to go beyond just meeting the technical compliance requirement.

It is easy to get lost in data, processes and documentation - though these are clearly important - and forget that the real purpose is providing actionable information to law enforcement to help them disrupt and fight crime.



04 Information sharing and collaboration

> **"It takes a network to defeat a network."**
>
> *FCA Techsprint 2019*

The idea of sharing financial crime typology information is not a new one, and was the theme of the UK's Financial Conduct Authority's (FCA) 2019 AML Techsprint which focused on how technology can be leveraged to better share information about financial crime without compromising data privacy standards.

FATF and global FIU publications have set the standard for information sharing over the last two decades. But the world of financial crime has accelerated, and despite the increasing willingness and participation in public/private for intelligence sharing, financial crime fighters cannot keep up with the pace at which criminals are adapting to not only evade detection of their existing techniques but to exploit new methods as a result of technological innovation such as virtual assets.

AI is well-placed to help the AML industry catch up, and tools such as Napier's Client Activity Review can make a huge difference in the effectiveness of detecting suspicious activity relating to some of the most heinous predicate crimes.

To enhance efficacy further, data from systems such as CAR can help to identify and build new typologies and networks of actors involved in new patterns of money laundering which can then be shared more speedily.

There are, however, two significant obstacles to this.

The first is that there is a 'tension between an institution's regulatory obligations and what it chooses to do to be a good corporate citizen'.

The work done by financial investigators within financial institutions to identify suspicious activities associated with predicate crimes is often voluntary.

Efforts to disrupt predicate crimes are not currently a regulatory obligation. Financial institutions therefore must make difficult decisions about the resources they allocate to activities to achieve technical compliance versus those that are for the greater good.

The second obstacle is that collaborative data sharing of new typologies and/or new risk indicators is in direct conflict with regulatory obligations stemming from data protection regulations such as the EU's General Data Protection Regulation.

What is clear is that collaboration is key, but it needs to happen at a greater pace to avoid more human suffering, damage to the environment, and further economic disruption. By working together as an industry and a global community, we may be able to improve that figure of 1% of illicit funds recovered.

05 Introducing Napier's Client Activity Review

Napier's CAR aggregates transaction data and customer profile data from KYC onboarding systems to form a single view of the customer across the entire customer lifecycle. Consolidating fragmented customer data sets allows organisations to obtain a complete record of a customer's accounts across lines of business, geographies and products, and to use that data more effectively to detect anomalies.

CAR's trigger-based alerts allows regulated organisations to conduct ongoing reviews of customers to measure risk and detect suspicious financial behaviour. AI-enhanced behavioural analytics give a 360-degree view of every customer in real-time to help identify any new or suspicious patterns.

Integrate data from existing systems

CAR doesn't require the complete rearchitecting of data infrastructure as it can integrate data from existing KYC and transaction monitoring systems to immediately provide a full view of the customer.

Real-time graphical analysis

Analysts can view real-time graphical representations of a customer's behaviour over a dynamic period, allowing for deep investigations into suspicious activity without having to switch between different views or applications. The analyst can view anomalies through multiple lenses and compare a customer's behaviour against a previous period, and against expected behaviour. By analysing behaviour as it happens, any necessary action can be taken immediately.

Full view of the customer in a single dashboard

CAR is designed to provide a 360-degree picture of the customer by aggregating KYC data, intelligence from payment and client screening, and transaction monitoring outcomes into a single dashboard. This complete picture helps the analyst to determine more quickly if the customer's observed behaviour is out of line with expected behaviour.

Trigger-based alerts

Customer reviews can be undertaken manually or scheduled to take place automatically according to the required frequency and organisation's risk appetite, whether that be daily, weekly or monthly. CAR can be configured so that reviews are triggered by changes in a customer's behaviour, and not risk score alone.

About the authors

Dr Janet Bastiman - Chief Data Scientist at Napier

Janet started coding in 1984 and discovered a passion for technology and problem solving. She holds degrees in both Molecular Biochemistry and Mathematics and has a PhD in Computational Neuroscience where she started her work in Artificial Intelligence.

Janet has spent 20 years in industry pushing the boundaries of data science in telecommunications, marketing and the financial sector, where she has helped both start-ups and established businesses implement and improve their AI offering prior to applying her expertise as Chief Data Scientist at Napier.

Janet is a committee member for the Royal Statistical Society Data Science Section and treasurer of the IEEE Stem Strategy Committee. She regularly speaks at conferences on topics in AI including explainability, testing, efficiency, and ethics.

Emma Miller - Global Head of Strategic Partnerships, Data & Analytics at London Stock Exchange Group (LSEG)

Emma is the Global Head of Partnerships for Risk & Compliance at Refinitiv, driving strategic relationships with leading technology providers in the risk and compliance space, and bringing Refinitiv's reports to the heart of customer workflows.

Emma is passionate about the role that data and technology can play in the fight against financial crime, and the real impact this has both on victims' lives and society at large. Emma joined Refinitiv (previously Thomson Reuters) in 2014 and has held various roles across strategy, transformation and business operations; she also served as Chief of Staff to the CEO. Emma is a board member for Refinitiv Charities, and a Trustee for Urban Synergy.

She has an MBA from London Business School, and a Bachelor of Science in Foreign Service from Georgetown University.

ABOUT NAPIER

About Napier

Discover how Napier can transform your compliance processes./

We are compliance technology specialists, who help financial institutions to fight financial crime more efficiently and effectively.

Founded on broad experience and deep expertise, Napier's cutting- edge platform increases efficiency and minimises risk by successfully combining big data technologies with AI and machine learning.

Our intelligent approach to financial crime compliance underpins organisational policy, process and procedure, so financial institutions can focus on being more effective at detecting suspicious financial activity; in a more cost-efficient way.

The Napier platform is fast, scalable and easily configurable. It rapidly strengthens financial crime defences while meeting compliance obligations and challenges in any sector.

Learn more about how Napier can transform your screening processes at www.napier.ai where you can book a demo or contact us.

Email us

Book a demo