How dirty money moves

What you can do to fight the latest evolution of money laundering

BAE SYSTEMS

INSPIRED WORK

Executive summary

As long as we've had currency, we've had money laundering. Lately, we've been fighting a more effective battle against it. But what used to be a stable, predictable evolution of regulation, compliance, and on the criminals' side, evasion, has collapsed in a year of revelations.

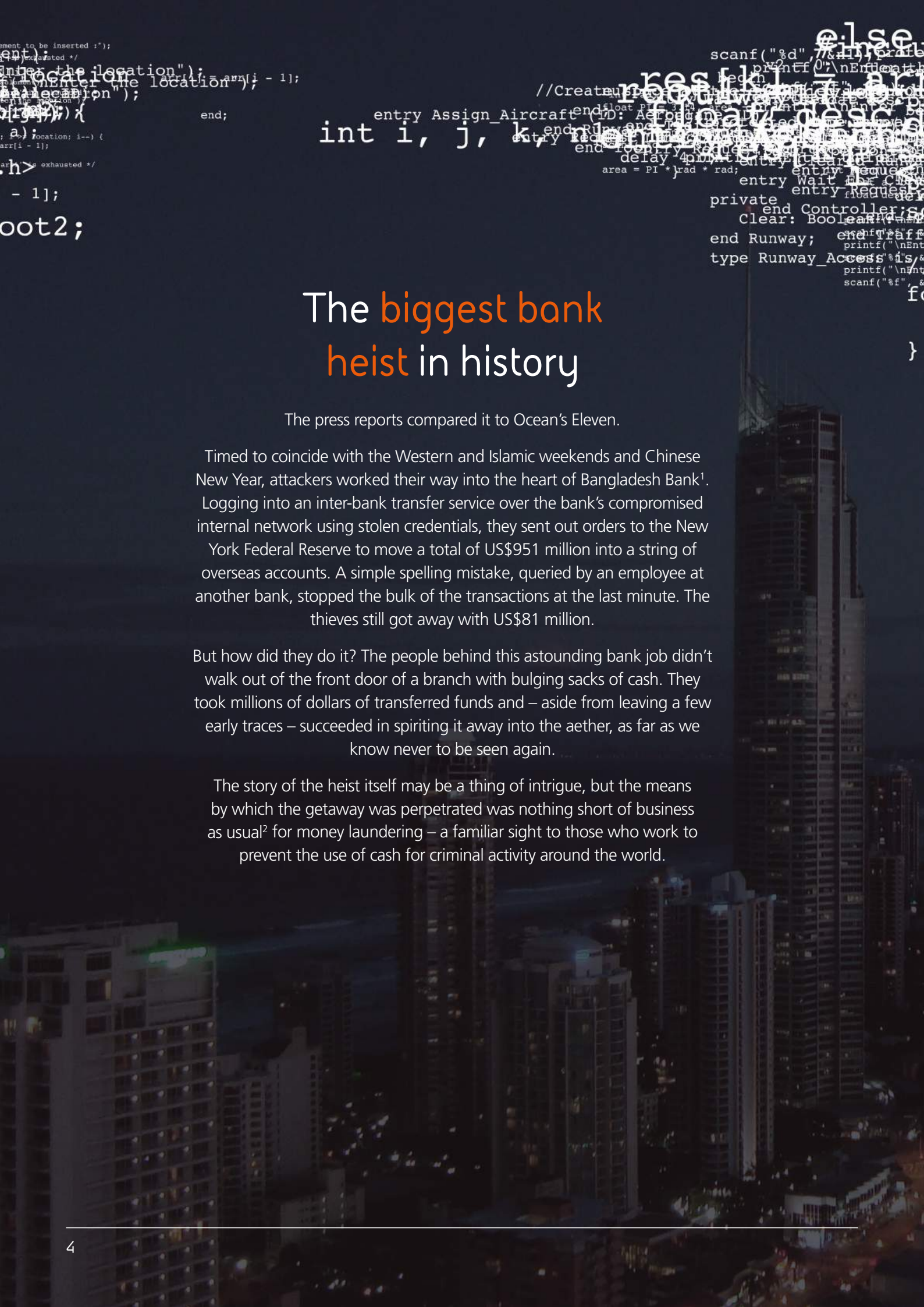
In the course of 2016, there have been sensational information leaks about the use of shell companies in offshore locations to hide beneficial ownership on a massive scale, a bank heist that led to massive individual money laundering efforts, and a sovereign wealth fund scandal. All have involved money laundering. These have been joined by revelations about bribery in the energy sector and a shock vote in the UK, one of the world's financial centres, to leave the European Union. This is a decision that, while yet to take place, has led to a great deal of uncertainty as to what the future holds.

Meanwhile, cyber-crime and money laundering is growing and evolving at a faster pace than many organisations can detect and prevent, while staying within their industry's regulatory requirements. The result is an uncertain and rapidly-changing global financial landscape.

So, how do we fight this ever-growing threat?

This report is divided into two parts; the first, *How dirty money moves*, lays out the current situation. The second, *The fight against money laundering*, proposes remedies and suggests how all those involved in the fight against money laundering can work together towards a mutual objective: making it as difficult as possible for criminals to profit from their crimes.

We may never eradicate money laundering, but we can certainly make it a riskier, more difficult proposition for criminals, and this report sets out possible steps in that process.



The biggest bank heist in history

The press reports compared it to Ocean's Eleven.

Timed to coincide with the Western and Islamic weekends and Chinese New Year, attackers worked their way into the heart of Bangladesh Bank[1]. Logging into an inter-bank transfer service over the bank's compromised internal network using stolen credentials, they sent out orders to the New York Federal Reserve to move a total of US$951 million into a string of overseas accounts. A simple spelling mistake, queried by an employee at another bank, stopped the bulk of the transactions at the last minute. The thieves still got away with US$81 million.

But how did they do it? The people behind this astounding bank job didn't walk out of the front door of a branch with bulging sacks of cash. They took millions of dollars of transferred funds and – aside from leaving a few early traces – succeeded in spiriting it away into the aether, as far as we know never to be seen again.

The story of the heist itself may be a thing of intrigue, but the means by which the getaway was perpetrated was nothing short of business as usual[2] for money laundering – a familiar sight to those who work to prevent the use of cash for criminal activity around the world.

How dirty money moves

Money makes the world go round – and one of the biggest movers is dirty money, stolen by criminals and cleaned for use in law-abiding society. Invariably the result of crime, dirty money is also used to fund conflict across the world. How we push back against the march of dirty money, and how we will fight it in the future, is of vital importance to society and economies across the world.

Laundered money represents between two and five per cent of global Gross Domestic Product (GDP), according to the UN[3]. That's the equivalent of the fifth largest economy in the world; in 2009, the UN estimated 3.6% of the world's GDP was tied up in criminal proceeds. Much of this was laundered: 2.7% of GDP, the equivalent of US$1.6 trillion.

With globalisation and innovation in technology facilitating the transfer of large sums quickly and easily, this problem is growing daily. Dirty money and ill-gotten gains are no longer hidden in safes or buried – they are increasingly turned into electronic funds and moved at the click of a mouse, popping up as cash, property and other tangible assets half a world away.

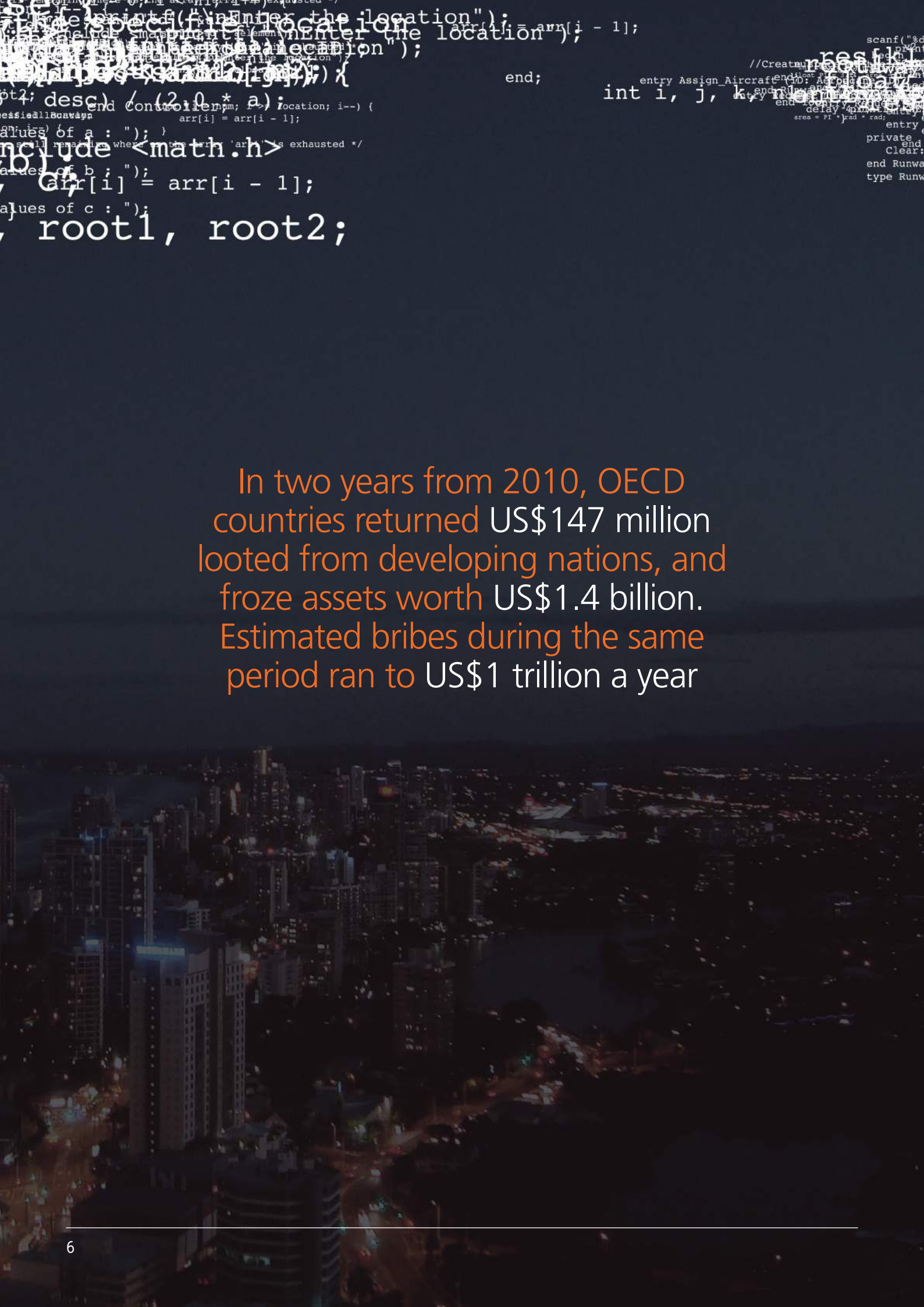
Yet it's arguably now harder than ever before to launder money. Since 2001, great efforts have been made to ensure that financial institutions can spot, alert and defeat money laundering. This has been driven by both legislation and prosecution, and has delivered significant results. Fifty-two per cent of those surveyed for BAE Systems' Financial Crime Survey 2016[4] say they expect investment budgets in Anti Money Laundering (AML) to increase over the next three years.

The penalties for banks that fail to identify and stop money laundering activity are high – personal responsibility for senior managers and criminal sanctions for breaches are now commonplace – and financial penalties are similarly steep. Analysis from consultancy CEB Tower[5] in 2014 put the cost of AML-related fines against banks increasing at a Combined Annual Growth Rate (CAGR) of 187% between 2007 and 2014.

But there are other costs to offenders, too – and far-reaching, sometimes unintended knock-on effects for society as a whole [see The impact on society, page 11]. Banks become more wary, and are less likely to enter into business transactions that carry a greater degree of risk. This has contributed to the decline of Correspondent Banking[6], a key means for businesses in emerging economies to trade with the wider world [see case study, page 14].

For large banks faced with tough questions about the ability of their correspondent banks in other countries to meet money laundering sanctions and Politically Exposed Person (PEP) requirements, the safest option is to remove the risk and simply stop trading.

If money laundering were a country, it would rank as the fifth largest economy by GDP in the world.



In two years from 2010, OECD countries returned US$147 million looted from developing nations, and froze assets worth US$1.4 billion. Estimated bribes during the same period ran to US$1 trillion a year

Understanding the threat

The history

Since 2001, the pace of regulation, international co-operation and active pursuit of money launderers, terrorist financiers and those who facilitate their activities has increased, reaching the rapid tempo we see today. The focus and attention is often on banks - but there's more to it than that.

According to the Organisation for Economic Cooperation and Development (OECD)[7], the 34 countries it represents signed 'roughly' 1,300 bilateral Exchange of Information agreements with developing countries between 2000 and 2013.

CEB reports[8] that, between 2007 and 2013, the six largest banks saw their compliance costs more than double, from US$34.7 billion to US$70.1 billion. In the UK, a report by KPMG[9] found that more than four fifths of banks' technology budgets over the last five years had been directed to addressing regulatory requirements, reducing litigation and streamlining.

Much of this has been driven by US foreign policy and the nation's Treasury Department over the last 15 years, and the actions of a little known organisation within the department: the Office of Foreign Assets Control (OFAC), which started issuing lists of Specially Designated Nationals to US Federal Reserve Banks in 1986[10].

This list, which effectively prevented any US national, business or institution from dealing with those it named, also made it very difficult for overseas businesses to trade with these people and still be able to do business in the United States.

Following the events of September 2001, the US Government, via OFAC, mounted a concerted push against money laundering[11]. The train of regulation, international agreement and relentless pursuit has continued apace – and is unlikely to let up any time soon, not least because it produces results.

Between 2010 and 2012, for example, OECD countries returned US$147 million looted from developing nations, and froze almost US$1.4 billion in looted assets. At the same time, the OECD estimated the total value of bribes paid worldwide to be around US$1 trillion per year.

Although a dubious measure of success, enforcement actions against institutions found to have been negligent or complicit in the laundering of illicit funds, sanctions or tax evasion have also risen – from two actions and US$25 million in fines in the USA in 2007-2008, to 18 actions and US$14,878 million in 2013-14[12] , according to the Financial Times.

Real estate agents, lawyers, currency exchange institutions and Trust and Company Service Providers (TCSPs) are often the preferred means of entry into the financial system for criminals, and their efforts and endorsement fool even the most sophisticated public and private sector attempts to spot foul play.

A 2011 investigation by the Financial Times[13] into fiduciary service companies in the Cayman Islands noted the scale at which some operate. At least four individuals held more than 100 non-executive directorships each, and 14 had more than 70 such positions. Law firms, accountants, and real estate agents also have far less in the way of resources to look for potential illegal activity than large banks or government agencies. Acquire the trappings of legitimacy through these gatekeeper organisations, and the banking system is – theoretically at least – laid open for the launderers to exploit.

Launderers are more than willing to change their tactics to avoid restrictions and capitalise on emerging weaknesses.

The role of banks

Banks remain on the front line when it comes to preventing money laundering, not least because of their central position in the world of finance. As compliance requirements have evolved, their need to bring resources to bear on tackling financial crime has grown. This is reflected in the interest taken by the boards of major financial institutions. KPMG found that 88% of respondents to its 2014 AML survey[14] said the Board of their company took an active interest in AML issues.

BAE Systems' Financial Crime Survey 2016[15], conducted in conjunction with Operational Risk, found that those surveyed – compliance professionals at major banks – expected spending on AML and non-AML compliance would continue to increase, much as it has done, by a significant margin. This year's survey also saw a significant migration to third-party PEP screening and sanctions solutions. Almost one third (31.3%) went outside their organisations in 2013; that figure rose to 43.8% in 2016.

This is broadly in line with other industry watchers; CEB found that 59% of those they surveyed expected to increase spending on AML systems, while also noting that AML solutions are the third-oldest installed technologies at their bank.

A survey by KPMG in 2013/14[16] found respondents saw the risk of AML compliance growing year on year. In fact, the trend was so marked that the report's authors compared the expected and actual increases in spend recorded all the way back to 2001.

Respondents in 2004 said they had seen costs increase 61% over the years 2001-2004. In 2007, this figure was 58% in the three proceeding years. In 2011, cost increases over the previous four years ran to 45%. The next iteration, in 2014, showed a 53% increase in the three years to 2014.

At every stage, these recorded increases in spend had been underestimated by the AML professionals surveyed.

Meanwhile, criminals are shifting tactics at a rapid pace. By diversifying into peer-to-peer lending, Hawala[17], casino gambling, abuse of diplomatic pouches, real estate, trade financing, fraud, fake invoicing and a variety of other areas, they can both spread their risk and avoid the area under most scrutiny: banks.

Money launderers are more than willing to change their tactics to avoid restrictions and capitalise on emerging weaknesses. For example, Wire Stripping – a term describing the removal of material information from wire payments or payment instructions to mask the contentious nature of a transaction – is becoming

popular again, after dying out as a money laundering tactic nearly ten years ago.

The other gatekeepers

While banks remain the connector of activity, spending and interest, they represent just a fraction of the issue when it comes to money laundering. Various gatekeepers – lawyers, real estate agents and organisations such as TCSPs – are all able to provide near-invisible entry to the financial system by disguising the ultimate owner of assets or cash: the Beneficial Owner.

While banks remain the connector of activity, spending and interest, they represent just a fraction of the issue when it comes to money laundering.

The events of 2016 have confirmed long-held suspicions within the world of AML and sanctions screening that gatekeeper organisations can provide all kinds of people and organisations with the tools to mask beneficial ownership, either unknowingly or willingly. The controls and regulations placed on these intermediaries also varies widely between countries.

With a duped or dubious gatekeeper to mask beneficial ownership, banks are effectively powerless; they will (and do) act on suspicion, but a sufficiently sophisticated approach has a high chance of going undetected.

Measuring the scale of this problem is very difficult, but at least one attempt to understand the problem has been made: a study by three academics for Griffith University called Global Shell Games[18]. Run as an experiment, the team sent out thousands of emails impersonating both high and low risk would-be customers, to more than 3,700 corporate service providers.

Nearly half of replies (48%) did not ask for proper identification, and over a fifth (22%) did not ask for any identification at all to form a shell company.

Contrary to perceived wisdom, those selling shell companies from tax havens and developing countries were more likely to push for compliance with financial rules than those from OECD countries such as the United States and United Kingdom. Failing to respond to an email does not count as acceptance of the sender's position – and may actually be a sign of what the researchers described as 'soft compliance'. In the US, 77.3% of law firms did not respond, compared to 49.3% internationally.

These entry points are smaller, more numerous and even harder to regulate than banks. Yet they represent poorly-guarded gates through which dirty money and criminal individuals and groups can gain the trappings of legitimacy.

Contrary to perceived wisdom, the research seemed to suggest that those selling shell companies from tax havens were more likely to avoid working with money launderers.

The fight against money laundering

An integrated approach

The last few years have seen AML evolve at breakneck speed, and that has sometimes made it difficult to identify common problems, and even more importantly: common solutions. Years of changing requirements and updated threats have created a tangle of remedies for many organisations.

Throwing more people, systems and money at the problem can work in the short term, but it never creates a long term fix.

What's more, money launderers don't explain what they plan to do, so strategic planning can only go so far.

The end result is that highly trained, experienced staff are often required to firefight, working with less-than-perfect systems. They need time and space to focus on really thorny problems, but all too often they are dealing with an avalanche of false positives and a tangle of systems piled on top of each other.

AML professionals are as aware as anyone else of the need to think and plan strategically, as well as reacting to short term events. But are often forced by circumstance to respond. This puts the emphasis on the vendors of these solutions to make simpler, more efficient tools that allow for flexibility, without creating layer upon layer of complexity.

We think three things can be done to help: Tackle the shortage of people, work collaboratively and finally, get the right technology in place and working in an efficient, optimised environment.

The impact on society

The impact of money laundering stretches far beyond business, to the economy and society as a whole.

1. London property prices are being inflated by offshore criminal assets, according to the NCA[19], while in Ireland 60% of house purchases are being paid for in cash[20]. More than half of property in Miami Dade Country in the United States is bought with cash, double the national average for the United States[21].
2. Corporations with favourable tax arrangements are distorting global trade and attracting scrutiny and censure[22].
3. Although international money transfer organisations like SWIFT and to a lesser extent Travelex and Western Union have good oversight of payments, large portions of global trade are still 'fictitious' – shoes sold to a foreign country that don't actually exist, except on paper, for example – because it's harder to detect trade-based money laundering than traditional money laundering.
4. The emergence of virtual currencies means that some of the current AML defence mechanisms will be invalid and impossible to enforce in the future.

Talent

Tackling the skills crisis

By 2017, the UK alone will need 745,000 more workers with digital skills. Businesses lacking the necessary knowledge within their four walls face increased security threats if the problem is not addressed, according to a report by the Commons Science and Technology Committee[23].

Activity over the last decade and a half has left any organisation that needs financial crime experts competing to hire increasing numbers of qualified, experienced staff. This is not limited to banks: regulators, law enforcement and gatekeeper organisations must also keep up with demand. The problem is made worse by the need to hire trained, qualified people, which often rules out new entrants from the job market – or at least, the more lucrative end with better advancement prospects.

There are several things that businesses can and are doing to combat these challenges:

- Upskill junior talent - Building from within, with an effective training programme or online learning to get them up to speed, is essential
- Automate systems - Automating repetitive work empowers junior-mid level staff to become decision-makers. Giving them the opportunity to be proper risk managers, as opposed to doing the grunt work, is a far more attractive proposition
- Give managers peace of mind - Senior managers now have personal responsibility for compliance. Investing in boosting the efficiency of systems, which can help them manage their costs, but also deliver effectiveness, reduces their risk of incarceration in the event of the discovery of money laundering
- Build a community - Creating a learning culture that will deliver the best Return on Investment, keeping the channels of communication open and being receptive to new ideas and different ways of working. Organise hackathons and forums that enable teams to learn from each other
- Don't focus solely on technical skills - As much of the 'day to day' of technology is now outsourced or hosted in the cloud, the emphasis, more and more, is around innovation and human interaction

Collaboration

Joining forces

The fields of financial crime prevention and cyber security are becoming more closely entwined; aside from the use of cyber attacks to commit straightforward theft and fraud, as seen in the Bangladesh Bank heist, cyber techniques are also being used to both carry out and defend against a wider range of crimes covered by compliance reporting requirements.

For many financial institutions, the roles of IT security and business compliance are often separated – both organisationally and physically. While some organisations – Citibank, with its Fusion centres, for example – are consciously connecting compliance, fraud prevention and cyber security, we need to see this sharing of information and actionable intelligence across the board.

A number of banks have invested in Strategic Financial Intelligence units to encourage more harmonious sharing. Key among their attributes is the ability to develop an integrated view of risk, fraud and compliance. This comes by uniting the compliance, security and other specialist staff across both business units and regions. This strategic organisation works with existing compliance set-ups, provides intelligence,

insight and analysis to senior management decision-makers, and upholds best practice in tackling financial crime.

A shared intelligence hub

As the worlds of fraud and cyber security continue to collide, it is inevitable that techniques used by both fields are compared. Whilst cyber security researchers often share intelligence as a matter of course, and provide intelligence-sharing services to clients, this technique is not as common among the financial services community. There are many reasons for this, not least a culture, laws and moral imperative towards discretion and secrecy that makes the discussion or sharing of what may be privileged information something of a taboo.

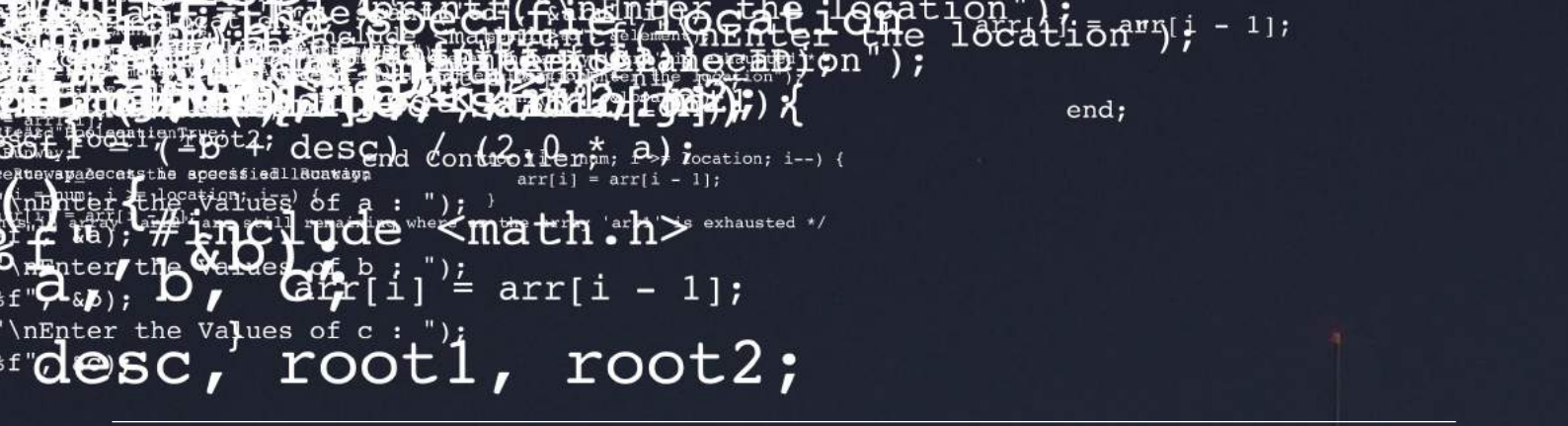
Yet there is much to be gained from intelligence sharing; a known bad identity for one bank can, at the moment, be used elsewhere with ease – an example of how criminals are quick to exploit the borders between their opponents. At the same time, the private sector holds much of the data that law enforcement and peers can put to use in the fight against money laundering. One example is the work BAE Systems Applied Intelligence has done with HM Treasury to create the Joint Money Laundering Intelligence Taskforce (JMLIT) (see Sharing intelligence, right).

Sharing intelligence – the JMLIT pilot

The Joint Money Laundering Intelligence Taskforce (JMLIT)[24] was established by HM Treasury in the UK in February 2015, to test the sharing of information between law enforcement and the financial services industry. The initial pilot performed well, resulting in 11 arrests and the seizure of £500,000 in illicit funds, and it is currently in the process of being added as a service within the British Bankers Association's Financial Crime Alert Service (BBA FCAS).

Financial institutions function on the basis of discretion, and information sharing is not always easy or desirable for many reasons. It is, however, another limitation that can be exploited by those with bad intent – both within and outside of the industry.

The means to share and act on intelligence already exists, but the means to do so without falling foul of banking secrecy laws and reputational damage must be created and nurtured. The moral imperative to prevent acts of terrorism and criminality must be balanced against the right of individuals to privacy in their daily affairs – an issue which many organisations outside this sector struggle with on a daily, if not hourly, basis.



Case study: Developing countries and Correspondent Banking

An early casualty[25] of the current wave of regulation has been Correspondent Banking. If a bank in one country does not have a branch in another – and a customer needs to transfer funds to that country – it will call upon a bank in the second location to deliver or collect the funds on its behalf. This relationship, and more complex variations, once powered global trade, ensured expat workers could send money home, and opened rich economies to businesses based in poorer nations. The system helps money and goods to flow easily between rich and poor economies, especially when it comes to countries where large global banks may not have a ready presence, enabling those in developing nations access to markets in established economies.

But Correspondent Banking has fallen victim to a practice generally referred to as de-risking, in which financial institutions back away from transactions that are inherently risky, or where the cost of mitigating that risk is simply too high [see Closing the gaps, page 18]. A significant driver of this is ensuring compliance. If it is impossible to establish the source of the funds, or the ultimate beneficial owner, the bank at the receiving end of the chain is at risk of handling dirty money.

Half of emerging market and developing economies have seen a decline in correspondent services, according to the World Bank, and of the 20 large global banks surveyed, 15 admitted to a fall in the number of Correspondent Banking Relationships (CBRs), with even more admitting to ending relationships with banks in entire nations[26].

CBRs have allowed bad people to launder dirty money as well as allowing everyone else to undertake legitimate business, and made it relatively easy to transfer bribes, stolen public funds and cash for terrorist activity to established, stable countries where it can be put to use. But the problem may not lie with banks in emerging economies – where it would appear that corporate service providers are more likely to comply with financial crime regulations than their counterparts in richer economies.

The difficulty of ensuring the other end of a Correspondent Banking relationship is able to defend against money laundering means that financial institutions often make risk-based assessments on the relationships they have. Local banks in emerging economies may lack the same level of resources – people, technology, and investment – to spend on compliance capabilities as global banks, so it's unsurprising that they may struggle to meet requirements that larger institutions regularly spend millions of dollars on and assign hundreds or thousands of staff to.

According to a staff discussion note published by the International Monetary Fund[27], there has been an impact on countries currently operating under international sanctions – but also developing economies in the Caribbean, Africa, Central Asia, Europe and the Pacific, reaching critical levels in some countries, potentially having a systemic impact on those countries' economies, if not addressed in time.

Banks frozen out of CBRs have looked to work around the problem by setting minimum activity thresholds, applying higher costs to cover more extensive compliance, or simply denying customers from certain sectors access, such as money transfer and value transfer businesses, according to the IMF. The problem with this is that setting minimum activity levels encourages middlemen to handle funds on behalf of multiple customers, disguising the beneficial ownership of the funds. A second problem is that value and money transfer businesses often handle the wages of expatriate workers, potentially cutting off the flow of funds from rich to poor economies. In the case of a country like Eritrea, overseas remittances from Eritreans working abroad represent almost a third of the country's GDP[28].

A further problem is that credit and cash still needs to be transferred – and these transactions may well move underground.

Correspondent Banking continues to grow, despite fewer and fewer banks maintaining relationships for this purpose. Efforts by lawmakers, law enforcement and banks themselves has exposed bad actors, and in the meantime, the technology to give oversight has improved. But the problem of bad banks remains. All that's happened is that their correspondents have reduced their own risk.

Fig 1. Correspondent Banking in decline

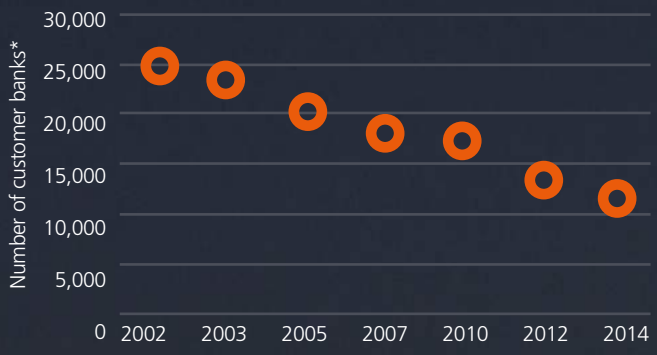


Fig 2. OECD countries' compliance with FATF Recommendations 7,10, 11, 12[29]

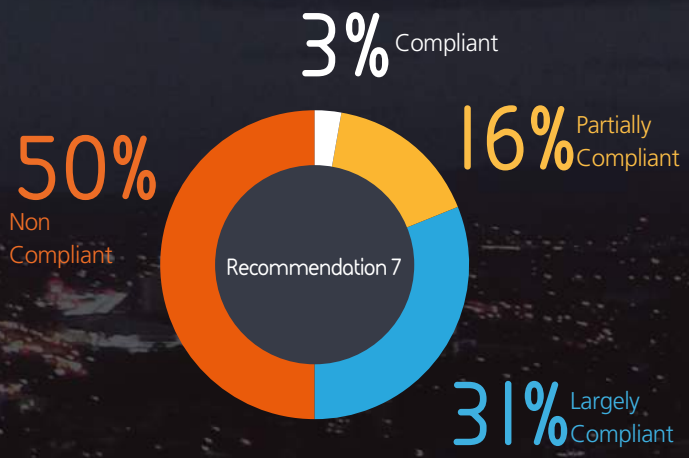
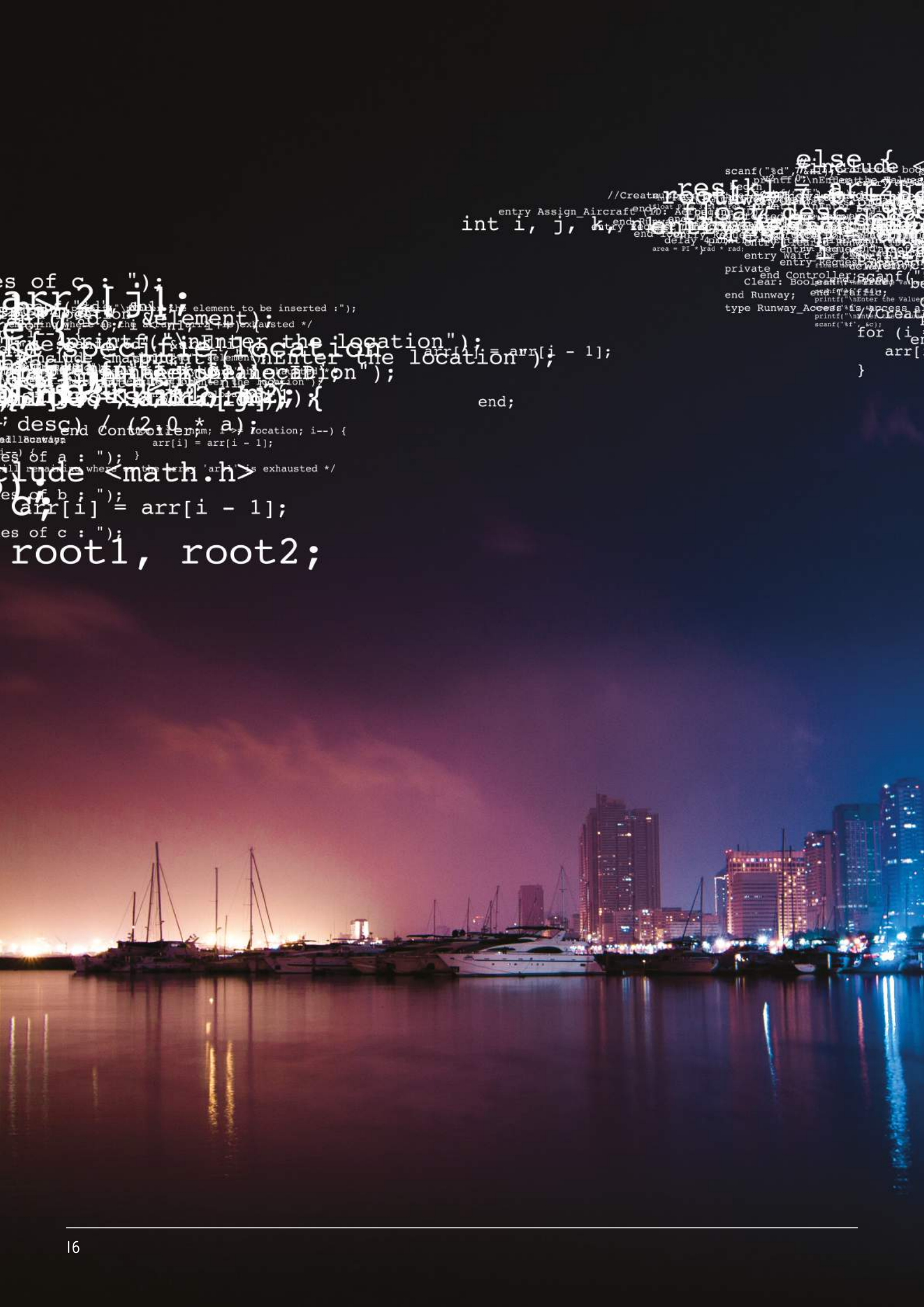


Fig 3. Transaction volume up, value of transactions, down

* Figure represents Loro transaction units. Banks measured had a minimum of EURO 1 billion turnover on loro accounts

Credit: European Central Bank: https://www.ecb.europa.eu/pub/pdf/other/surveycorrespondentbankingineuro201502.en.pdf


int i, j, k, n;
end;
root1, root2;

Technology

The right technology

Any organisation with a strong AML capability will know that technology represents a dichotomy: On the one hand, it gives scope, power and scale to investigation and management. On the other, it can become a cumbersome, layered beast that hinders as much as helps. The stratospheric growth of the last few years has created complicated solutions with layers of technology from different eras and different suppliers for most end user companies. Creating efficiency and optimising what exists will generate further returns from what's already in place – and both lift the burden of managing complexity and automate more repetitive tasks for users. The end result should be detection and prevention.

That said, two new technology areas promise to deliver further efficiency and shake up the way money laundering is managed.

Blockchain

Blockchain is a technology that allows the creation of a database of transactions that are effectively tamper-proof. For Bitcoin, it provides a public, shared ledger recording transactions permanently.

Blockchain-based technologies are a hot topic when it comes to fighting money laundering. Certainly, in the realm of creating an audit trail and mapping beneficial ownership, the technology has already proven popular, helping investigators track illicit transactions, fraud and theft. Blockchain was used to identify, trace and prosecute two law enforcement agents who helped to take down the Silk Road black market site, helping themselves to virtual cash in the process[30].

Bankers also hope to use Blockchain to reduce costs, augmenting or replacing traditional tools to ensure compliance. Santander, for example, expects to shave US$15-20 billion a year from its regulatory compliance, securities and cross-border trading by 2022, in part thanks to Blockchain[31].

Machine learning

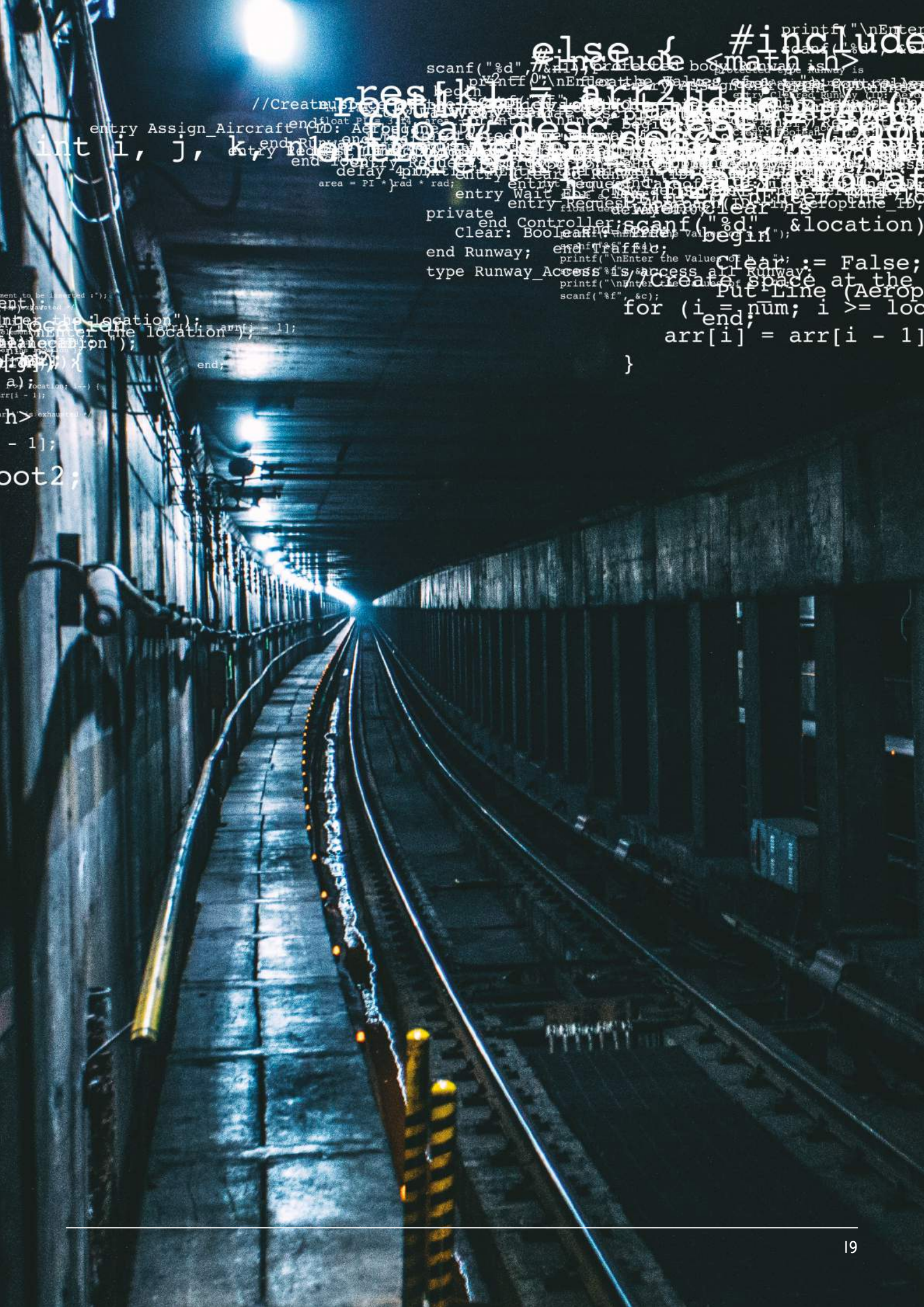
It has been difficult to escape the hype over Big Data for the last few years, but many organisations have been quietly putting it to use. Automating the exploitation of insight provided by big data tools is a natural next step. Regulators and industry bodies are also more willing to accept machine learning as a useful addition to trained, experienced professionals. Applying the capabilities of Big Data Analytics and other techniques strengthens the arm of an organisation's compliance team if done correctly. This focus also helps drive efficiency. Many institutions take up technological tools such as Hadoop, and techniques, including predictive and prescriptive analytics, in order to optimise their infrastructure and software licenses.

The caveat is that having a variety of data scientists and machine learning capabilities to call upon is not the solution to the problem. The creation of such engines is, more often than not, accompanied by the need to ensure that regulatory requirements are met and understood.

Closing the gaps

It's actually possible to prevent certain types of money laundering – an example might be misuse of the Correspondent Banking relationship, where it has become prohibitively complicated or expensive to launder via a certain method. Illicit funds can be frozen, appropriated, and returned. Close off one route, however, and the money still has to go somewhere. It's which 'where' that remains the issue. Mobile payment platforms, peer-to-peer lending, money exchanges and other mechanisms might appear to be viable alternatives – yet they often deal in relatively small individual chunks of money, and in the case of Peer to Peer lending, the frameworks, experience and tools are already available, known and likely employed.

Bigger volumes of dirty money need to go somewhere, and often the attention focuses on two things: the possible level of scrutiny at the placement stage of a money laundering attempt, and the gaps between AML regimes for different nations or professions.


#include <math.h>
int i, j, k,
scanf("%d",
printf("\nEnter
else {
entry Assign_Aircraft (ID: Aeroplane_ID;
private
end Controller;
end Runway;
type Runway_Access is access all Runway;
Clear := False;
Put_Line (Aerop
for (i = num; i >= loc
arr[i] = arr[i - 1]
}
begin
end Traffic;

Conclusion

This year has been extraordinary for money laundering. Cyber-enabled fraud on a massive scale and the possible departure of one of the largest financial centres in the Western world from the EU has created great uncertainty, and the revelations around the abuse of offshore trusts and shell companies has laid bare the reality of what many have warned of and suspected for decades.

Banks remain a target, if not *the* target, for regulation because of their position at the terminus of many roads. This will not change and neither will their ongoing struggle to remain compliant, identify criminality and remain profitable in the process. Banks must meet their obligations to prevent criminality in order to stay in business, and as a result must move in synch with developments.

Yet banks do not operate in isolation. They operate in a world where intermediaries – lawyers, real estate agents, services companies and others – can, knowingly or otherwise, act on behalf of those with bad intent. Criminals and terrorists know this, and they also look for cracks in the wall to exploit.

What you can do

Enhanced collaboration, better technology and an empowered, skilled workforce should be the three priorities for those who fight financial crime. The first step is for you, the reader, to share your thoughts on money laundering and proposals for tackling it with us at: learn@baesystems.com

Sharing intelligence and information is hugely desirable, but from the perspective of many, working in sectors that mandate anonymity and privacy, it is also hugely difficult to do without risk of falling foul of the law.

However, there are reasons to be hugely optimistic when it comes to fighting money laundering and associated financial crime going forward. Law-making in the last 15 years has created a worldwide drive against crooked money and the resolve is present in many countries and industries. Technology is moving apace and will continue to strengthen the hands of those who act against crime. One thing is certain: there will be no let-up in this war.

What to do next

The three remedies we propose, centred around people, process and technology, represent long term goals for banks. However, financial organisations and senior managers can take active steps to handle compliance effectively in the short term, too. In doing the following, they can continue to work efficiently, meeting their obligations to society on an ethical level, as well as their legal obligations to regulators like the United Kingdom's Financial Conduct Authority (FCA). With so many forces pulling in different directions, organisations need to work with specialists who are dedicated to pursuing these and harnessing them, building out a plan to track and improve on each.

Analytics – Look at transactions and customer data. Identify unusual or suspicious activity, flagging it to investigators. Then look at the history of those decisions, in conjunction with the data. Use analytics and artificial intelligence to feed back into the typologies themselves whatever it was in the data that flagged money laundering, so the system learns to be better over time.

Automation – Use technology to automate certain decisions. This can be hugely cost-effective because transaction volumes are so big.

Value Data – Third parties that consolidate and aggregate data can be extremely useful for those at the frontline of financial crime – to understand, for example, whether a new customer is reputable. Employ them to help you differentiate between the good and the bad when it comes to new customers.

Technology – Technology is moving on, and banks need to focus more on innovations like mobile telecommunications and self-service. Core banking systems and financial crime detection systems must be able to meet the challenges these new technologies present.

Regulation – Regulators and cross-sector organisations such as FCAS provide vital guidance that financial institutions need to be aware of. Staying on top of regulation requires significant effort, especially for large banks with many different operating units.

A five-point plan

1. Get off the treadmill – evaluate the value of detection systems and typologies
2. Assess source data quality – and plug data and compliance gaps to improve value
3 Systematically review, classify and reclassify assets and outcomes of the investigation process. This will help identify areas for improvement
4. Measure effectiveness, which is easy to say, but harder to do. When you understand your effectiveness you can relentlessly pursue efficiency
5. Have a buffer. Unexpected events happen, like political sanctions – you need to have some flexibility in your capacity to plan for the unexpected

1. http://baesystemsai.blogspot.co.uk/2016/04/two-bytes-to-951m.html
2. http://www.baesystems.com/en/cybersecurity/as-money-laundering-scams-go-the-bangladesh-bank-heist-wasnt-that-sophisticated
3. http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html
4. risk.net Operational Risk/BAE Systems Financial
5. https://www.cebglobal.com/blogs/infographic-the-price-of-dirty-money/
6. http://www.economist.com/news/finance-and-economics/21604183-big-banks-are-cutting-customers-and-retreating-markets-fear
7. GFI / OECD: Illicit Financial Flows in Developing Countries: Measuring OECD Responses, P 12, http://www.gfintegrity.org/report/illicit-financial-flows-from-developing-countries-2004-2013/
8. "Combating rising threats with aging infrastructure: AML Systems Market Update February 2016" – CEB Tower
9. http://www.ft.com/cms/s/2/7bfd4794-0095-11e6-99cb-83242733f755.html
10. Treasury's War by Juan Zarate, 2013, ISBN 9781610391153
11. Treasury's War by Juan Zarate, 2013, ISBN 9781610391153
12. https://blogs.ft.com/ftdata/2014/03/28/bank-fines-data
13. http://www.ft.com/cms/s/0/913e31b6-114a-11e1-a95c-00144feabdc0.html
14. https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf
15. risk.net Operational Risk/BAE Systems Financial Crime Survey 2016
16. https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf
17. https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf
18. https://www.griffith.edu.au/business-government/centre-governance-public-policy/research-publications/?a=454625
19. http://www.cityam.com/220931/foreign-criminals-laundering-money-drive-london-house-prices
20. http://www.thejournal.ie/housing-market-ireland-cash-buyers-funds-2-2895200-Jul2016/
21. http://www.worldpropertyjournal.com/real-estate-news/united-states/miami-home-sales-february-2015-miami-condo-sales-condos-for-sale-in-miami-beach-south-beach-condo-sales-new-condo-projects-in-miami-2015-cash-buyers-in-miami-foreign-real-estate-investors-8955.php
22. https://www.theguardian.com/business/2016/aug/30/apple-pay-back-taxes-eu-ruling-ireland-state-aid
23. http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf
24. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf
25. http://www.economist.com/node/21604183
26. http://fwsp.ifslearning.ac.uk/docs/default-source/default-document-library/northedge.pdf
27. NB: This note does not represent the policy of the IMF. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf
28. http://www.bbc.co.uk/news/world-africa-36786965
29. Illicit Financial Flows From Developing Countries: Measuring OECD Responses, PP34: https://www.oecd.org/corruption/Illicit_Financial_Flows_from_Developing_Countries.pdf 23. http://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught/
30. http://arstechnica.com/tech-policy/2016/08/stealing-bitcoinswith-badges-how-silk-roads-dirty-cops-got-caught/
31. http://santanderinnoventures.com/fintech2/

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST
CESG Certified Service
Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure