

FUTURE FINANCIAL CRIME RISKS 2020

WHAT KEEPS AML & CFT PROFESSIONALS **AWAKE AT NIGHT?**



01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

01: FOREWORD BY NIRVANA FARHADI, FINANCIAL SERVICES REGTECH PIONEER AND EXPERT



The impact of COVID-19 pandemic has accelerated our timeline to embrace digital transformation, out of sheer necessity. We are now forced to operate in a new world, with “new norms”, and new risks and threats as a result of this pandemic, especially in the financial services sector.

Criminals are getting more sophisticated and the current environment is proving an extremely advantageous breeding ground for criminal scams and laundering opportunities associated with this crisis.

In a recent report issued on 4 May 2020 (FATF May 2020 Statement), FATF identified the new types of exploitative threats from criminal organisations, for example;

- » Deliberate attempts to bypass customer due diligence measures;
- » Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
- » Misuse and misappropriation of domestic and international financial aid and emergency funding; and
- » Increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds.

With the above in mind, we now face the insidious invasion of our rights, privacy, political narratives, money flows, storylines, and social cohesion. It is imperative that in this new world, the role of regulatory oversight, should be to serve as a kind of filter.

A filter designed to protect, enhance, clarify and support the lives, privacy, health and well-being of society and the consumer.

What that filter dictates and who gets to design it, will bend the continuum of technology and its impact on our lives. The stakes will only get higher and the need more complex.

How do we find the maximum efficacy of technology's impact whilst ensuring a fair playing field for everybody? How do we protect the consumer without stifling creativity? This is where RegTech can be applied to imagine, design and create that “filter” through which technology must pass, to embed compliance by design at the development stage of the product, to enable us to pre-empt these types of threats and to not be stuck fighting the wars of yesterday!

Nirvana Farhadi

Financial Services RegTech Pioneer and Expert

01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

02: INTRODUCTION BY STEVE ELLIOT, MANAGING DIRECTOR – LEXISNEXIS RISK SOLUTIONS UK & IRELAND

“Serious and organised crime kills more of our citizens every year than terrorism, war and natural disasters combined.”

LYNNE OWENS, DIRECTOR GENERAL OF THE NATIONAL CRIME AGENCY*



The National Crime Agency estimates that serious and organised crime costs the UK economy around **£37bn a year**. Latest figures reveal **4,629 organised crime groups** inside the UK, each with tens of thousands of members, and at least **100,000 victims of modern slavery** in the UK.

Financial crime – money laundering, terrorist financing, fraud and cybercrime – forms a major part of the serious and organised crime threat that continues to grow in the UK, both in terms of volume and sophistication.

The people at the frontline of our fight against financial crime in the UK and Ireland are from both the public and private sectors. They include law enforcement and regulators, but also financial crime compliance professionals with responsibility for KYC/customer due diligence checks, sanctions and payments screening, financial crime compliance, and risk management.

These professionals, alongside the wider financial services sector, bear an enormous burden of responsibility to help detect, disrupt and deter the estimated **\$100bn** being laundered through the UK's global financial centre every year.

With such a heavy burden resting on their shoulders, we wanted to find out how confident professionals in the financial sector feel in their ability to identify and tackle money laundering and terrorist financing risks, particularly as these threats evolve. We wanted to understand what worries them most, and the approach they're taking to detect the crimes, manage the risk and meet their compliance obligations.

Our sincere thanks to all 313 financial crime compliance professionals from UK and Irish banks, Fintechs and asset and wealth management firms who participated in our research. As a result, this report provides industry-driven insights to help you:

- » Keep abreast of current and emerging financial crimes.
- » Identify ways that financial firms are addressing financial crime risks.
- » Understand key financial crime risks and challenges faced by financial institutions.
- » Learn about effective approaches for getting in front of evolving threats.

Steve Elliot

Managing Director – LexisNexis Risk Solutions UK & Ireland

* Source: The Guardian newspaper in May 2019: <https://www.theguardian.com/world/2019/may/11/police-cuts-organised-crime-national-crime-agency>

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?**
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

03: WHAT KEEPS AML & CFT PROFESSIONALS AWAKE AT NIGHT?

The challenges facing financial crime compliance professionals are both external – from the criminal world – and internal, from within their organisations.

The sorts of questions playing on the minds of AML & CFT professionals every day, include:

1. Are we doing enough to detect and prevent money launderers and other types of financial criminals from taking advantage of our organisation, particularly in light of the increasing volumes and sophistication of some of these crimes?
2. Are we confident we're fully compliant with the latest AML regulations?
3. Are we doing the right things? Is all the effort we're putting into AML and CFT compliance actually making enough of a difference to combat the growing threat of financial crime across the UK & Ireland?

But their concerns are by no means limited to external threats and regulatory requirements. For many, there are also major headaches associated with data quality, system failures, IT gaps or ineffective internal tools and outdated technologies. There is also the very real fear of waking up to some damaging newspaper headline that your organisation has been facilitating financial crime, and having to deal with the reputational and financial impact that comes with it.

The battlefield for financial crime compliance professionals comprises external, internal, resource-driven and business impact threats and challenges, often overlapping to create a complex web of pressures.

Figure 1: Multiple types of threats/challenges faced by financial institutions (n=300)

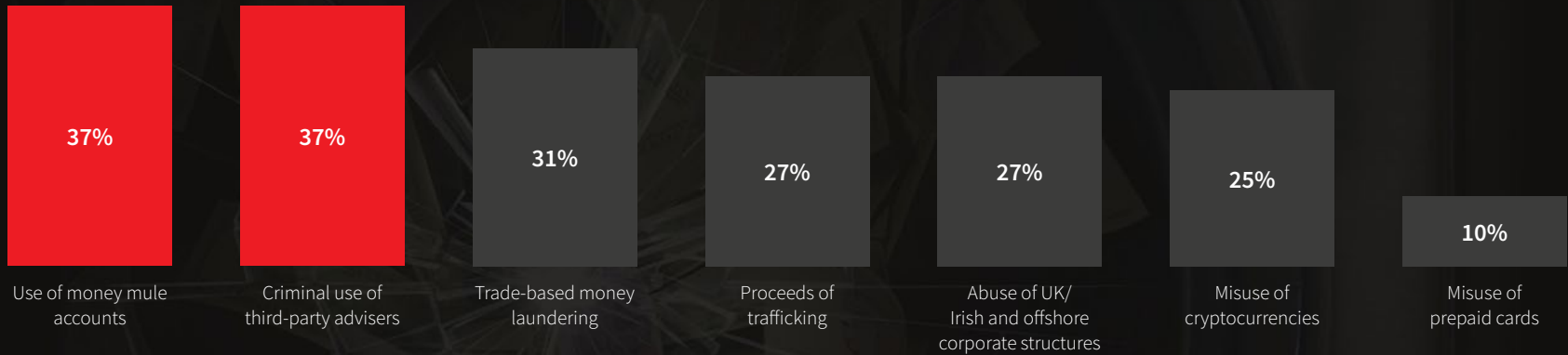


- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
 - Part 1
 - Part 2
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

04: LEADING TYPES OF FINANCIAL CRIME ATTACK (PART 1 OF 2)

UK and Irish financial institutions are currently being exposed to a diverse range of financial crimes.

Figure 2: To which of the following has your UK business been exposed in the last 12 months? (n=300)



Whilst around a third of firms cited exposure to money mules and criminal use of third-party advisers as two key financial crime risks detected during the past 12 months, there is no single financial crime that a majority of institutions have commonly indicated.

That may be at least partly due to criminals targeting different organisations with specific types of crime, where controls are seen as weakest. This can be observed when comparing the types of crime reported by various types of financial organisation over the past 12 months, as shown in figure 3.

Figure 3: Types of crime reported by various types of financial organisation over the past 12 months (n=300)

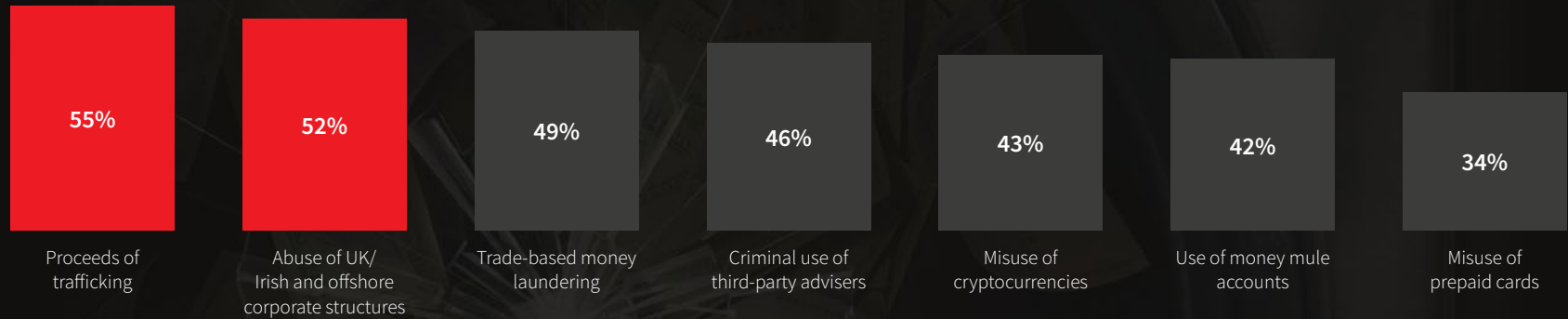
<p>Fintech and challenger banks</p> <ul style="list-style-type: none"> 60% – Use of money mule accounts 45% – Trade-based money laundering 35% – Misuse of cryptocurrencies <p>Building societies</p> <ul style="list-style-type: none"> 44% – Criminal use of third-party advisers <p>Private banks</p> <ul style="list-style-type: none"> 42% – Criminal use of third-party advisers 42% – Proceeds of trafficking 	<p>Mid to large asset management firms</p> <ul style="list-style-type: none"> 56% – Trade-based money laundering 39% – Proceeds of trafficking <p>Pre-paid card providers</p> <ul style="list-style-type: none"> 32% – Proceeds of trafficking
---	---

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
 - Part 1
 - Part 2
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

04: LEADING TYPES OF FINANCIAL CRIME ATTACK (PART 2 OF 2)

Over half of firms are less than fully confident in their ability to detect some of the most prevalent financial crimes they're exposed to today.

Figure 4: Types of crime organisations are **less than fully confident** in being able to detect and prevent (n=300)



Financial crime compliance professionals are least confident in their ability to detect the proceeds of trafficking (55%) and abuse of UK/Irish and offshore corporate structures (52%), both of which over a quarter of firms (27%) reported as having been exposed to in the past 12 months. Confidence levels were only slightly higher when it came to other leading types of financial crime attack.

The data suggests criminals are focussing attacks on firms they perceive to be weaker at detecting these crimes: overall 46% of banks reported exposure, but within that category 56% of building societies and 60% of challenger banks reported mule attacks. Newer and online-only firms may be in the criminals' sights because a) they have less historic customer behaviour data to help with detection, and b) there's no real-person interaction at all.

Figure 5: Types of crime organisations are **only somewhat confident** in being able to detect and prevent (n=300)



01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

05: COMPLEX TRANSACTIONS THAT ARE DIFFICULT TO DETECT

Remote channel anonymity adds to the complex nature of financial crimes.

Regardless of whether you're a bricks & mortar or digital firm, financial crimes typically involve complex networks of accounts and relationships that make detection difficult.



Money mules – hard to discern between legitimate and criminal transactions

- » Complex criminal networks confuse transaction monitoring.
- » Newer institutions, such as Fintechs and Challenger Banks, lack long-term account history to detect behavioural changes.
- » Less in-person opportunity for Fintechs and Challenger Banks to assess anomalies between the person and transaction.

“We can't determine if they opened an account with the intention of becoming a money mule or were coerced later in the life cycle.”

HEAD OF FINANCIAL COMPLIANCE,
UK Fintech



Proceeds of trafficking – easy to conceal, hard to detect

- » Illicit trafficking funds are hard to spot, particularly as online transactions.
- » Individual financial institutions can only see their own data, so it's hard to identify the types of funds, transaction patterns and flows of money associated with trafficking.
- » Strong links to funding of terrorist activities, particularly through pre-paid cards.
- » Limited data and CDD tools may result in fewer transactions being tagged as suspicious, since compliance teams are concerned about damaging client relationships if they turn out to be wrong.

“Human trafficking is very hard for us to figure out in the digital world. It looks as if the individual is going to work and spending their pay. In a traditional bank, you can look at types of people, who accompanies them and make assessments that we can't.”

DEPUTY MLRO, UK Challenger Bank



Criminal use of third-party advisers – lending legitimacy to illicit transactions

- » Third-party advisers such as lawyers, accountants and estate agents, are attractive to criminals because they confer an air of credibility, and offer skills the criminals need.
- » Financial institutions must always conduct due diligence on third-party advisers.

“It comes down to complacency. It's in your interest to get the deal done, and your sales people want the fees, etc. That opens up the firm to perhaps being complacent and relying on and putting their trust into...what appears on first glance, to be a professional advisor. I am also well within my rights to rely on the KYC [checks] of another regulated MiFID investment firm.”

HEAD OF COMPLIANCE,
UK Asset Management Firm



Trade-based money laundering – hiding illicit funds in legitimate transactions

- » Increasing globalisation means more UK firms trading with countries outside the UK and in unfamiliar regulatory environments in which they lack experience and insight.
- » They may not understand the intricacies of trade cycles, flows and finance or the associated threats. For example, inspection reports: how they're completed, the role they play in letter of credit bundles and the legitimacy of those reports.

“People can open multiple accounts – a personal account, a sole trader account, a business account, and then a Euro account. It is very easy to launder money essentially to themselves...there is a legitimate purpose in moving money from your own business to a personal account. It evades a lot of transaction monitoring.”

HEAD OF FINANCIAL COMPLIANCE,
UK Fintech

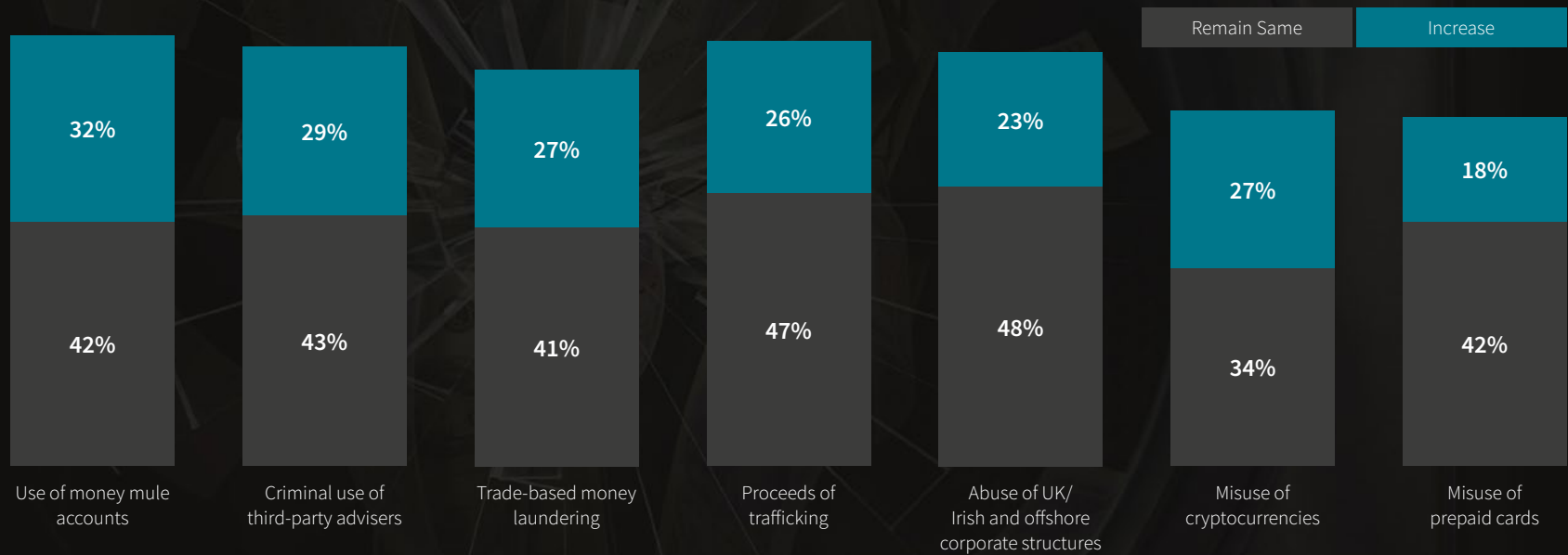
- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

06: A RELENTLESS VOLUME OF ATTACKS WITH NO END IN SIGHT

There is little expectation that these financial crime attacks will subside any time soon.

When asked, a majority indicated that they expect exposure to these types of financial crimes to either remain the same or increase during the next 18-24 months. That's a somewhat mixed reaction. There is a particular expectation among some that exposure to money mules and criminal use of third-party advisers will increase, and nearly half expect that the prevalence of proceeds of trafficking and abuse of UK/Irish and offshore corporate structures to at least remain constant. The upshot is that very few expect any of this financial crime activity to diminish in the near-term. At the same time, the mixed expectations suggests confusion among financial institutions as to what the future actually holds.

Figure 6: Please rate the degree to which you expect the following to increase or decrease over the next 18-24 months, as compared with now. (n=300)



Segment Expectations – Challenger Banks

Challenger banks – most likely to report past 12 month exposure to money mules and trade-based money laundering threats – are also more likely than others to expect these criminal activities to increase during the next 1-2 years. They also expect proceeds of trafficking crime to increase.

55% expect money mule activity to increase

51% expect proceeds of trafficking activity to increase

35% expect trade-based money laundering activity to increase

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
 - Part 1
 - Part 2
 - Part 3
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

07: THE INCREASING SOPHISTICATION OF CYBERCRIME (PART 1 OF 3)

Sophisticated digital crime is viewed as a key risk in the next 18-24 months, along with regulatory challenges.

In the following pages, we explore the mix of external and internal challenges consecutively at play:

- » **The sophisticated nature of criminals**
- » **A higher risk to those with a digital business model**
- » **Lack of internal IT knowledge and technology**
- » **Increased regulations with a lack of centralised resources**
- » **The potential impact of a softening economy increasing financial crime recruitment.**



01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
Part 1 Part 2 Part 3
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

07: THE INCREASING SOPHISTICATION OF CYBERCRIME (PART 2 OF 3)

It's not just technology and systems challenges that make cybercrime a real threat to financial organisations. Business models and culture add to this as well.

Modern cybercriminals aren't typically students hacking into a system for fun and games. These days they tend to be professional, and can even be privately or state-backed in terms of their technical expertise and resources. They also hold an additional advantage inasmuch as criminal activity is their sole focus, unlike a business that faces many competing priorities on any given day. However, financial institutions may not be as prepared for the digital battle as they could be – even Fintechs and Challenger Banks whose business model is intrinsically digital.

“Cyber risk is probably the one that's growing. That is probably the one that's most sophisticated and it's the one that we're still sort of reactive to instead of being proactive.”

HEAD OF RISK & COMPLIANCE, Irish Fintech

Digital attacks – sophisticated nature of cybercrime

- » Professional criminals with sophisticated tools and technological expertise.
- » Mindset of a criminal.
- » Sheer volume of ongoing attacks.

“I think the sheer scale of cybercrime can keep people wide-awake at night. We're not talking about small garages and back bedrooms. Professional hackers have lots of resources and we can't keep up with them.”

ASSOCIATE DIRECTOR, UK Bank

The 'business culture' model – this is how we've always done it

- » Traditional banks and asset management firms are slow to change and add technology to fight crime in the digital space.
- » Fintechs and Challenger Banks have been pressured to show aggressive return on investment; some have had to prioritise sales resources over risk technology investments – and are therefore playing catch-up.
- » Fintechs' and Challenger Banks' differentiator is a faster and easier customer experience; savvy criminals will take advantage of this by testing and re-testing digital identities (breached or fake) to access accounts.
- » Traditional firms are less inclined to bring in outside consultants to help introduce process and system changes.

“Fintechs grew quickly. We prioritised growth initially, now we are focused on governance.”

CEO, UK Fintech

Technology gap – systems and expertise

- » Financial institutions are not software companies; they lack technology expertise to fight digital financial crime.
- » Some may lack the mind of a cybercriminal in order to understand how they work to gain access to systems and customer accounts.
- » Legacy systems and multiple databases weaken security controls.

“I actually think that our threat is internal because I don't think that we really know what we should be looking for. We're not as tech savvy in financial crime as the criminals are who are able to conduct these threats.”

SR, FINANCIAL CRIME MANAGER, UK Bank

“Generally speaking, banks are not software houses. We've got complex systems, with acquisitions. The systems controls aren't quite as they should be and the risk of cybercrime is actually quite high.”





HEAD OF GLOBAL BANKING, UK Bank

01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
Part 1 Part 2 Part 3
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

07: THE INCREASING SOPHISTICATION OF CYBERCRIME (PART 3 OF 3)

Cryptocurrencies were also identified as a major risk. As a measure of just how risky virtual currency is viewed, a number of financial institutions that we spoke to admitted to not accepting these types of transactions. However, there is a widely-held expectation that demand may pressure them to do so, at some point.

Key concerns with cryptocurrency include:

-  Ease with which criminals can disguise illegal transactions behind virtual currencies.
-  Limited ability for transaction monitoring systems to detect illegal activities.
-  Easy to move crypto through small, less noticeable transaction amounts.
-  Lack of transaction transparency – you can track the transaction but not the buyer.

“Digital currency has exploded onto the market over the past three or four years, compared to the previous five. So it’s the development of products and services, and the ability to use digital products, which is probably outstripping the ability for traditional financial institutions to keep up with that technology, in order to make sure that their systems can monitor these types of transactions, and that the systems they have are appropriate for the bank.”

HEAD OF GLOBAL BANKING, UK Bank

“So we can track the transaction. So we can track back to the quantity of the coin or the token that has been bought and sold, but we cannot go and track who the buyer of the money or the coin was.”

CEO, UK Asset Management Firm

“The only crypto that we allow through our customer accounts is personal crypto trading. That’s it. We can see the transactions and where they’re purchasing Bitcoin.”

DEPUTY MLRO, UK Challenger Bank

“As a bank, we do not even touch cryptocurrency. We just decided that is too much risk for us. But, how long we’ll be able to maintain that stance is unknown. I think it will be difficult to ignore cryptocurrency when it begins to infringe on regular transactions.”

ASSOCIATE DIRECTOR, UK Bank

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

08: TRULY UNDERSTANDING PEOPLE AND THEIR NETWORKS

Digital identity authentication is central to successfully detecting and preventing financial crime in the new digital world.

Among the firms that identify internal gaps and systems as one of the biggest threats they face, nearly half (45%) specified difficulty distinguishing between legitimate and suspicious transactions as a major challenge. Fake and synthetic identities significantly add to this dilemma.

Pre-paid card providers particularly, spoke to these challenges through their distributor channels. These challenges are not just related to detecting and fighting account takeover and hacks (cybercrime), but also to other key threats, such as money mules, proceeds of trafficking, illicit funds, misuse of cryptocurrencies and trade-based money laundering.

“Digital identity authentication for us, is the biggest part of financial crime prevention.”

FINANCIAL CRIME LEAD, UK Fintech

“There’s the risk that digital profiles can be altered to access and open bank accounts.”

HEAD OF GLOBAL BANKING, UK Bank

“Digital identity authentication is massive for us. We rely on distributors and third parties to conduct KYC. Some are more advanced than others in terms of systems and processes.”

HEAD OF RISK & COMPLIANCE, Irish Fintech

Financial crime challenges

Common across financial crime types

- » Complex networks, hidden relationships.
- » Establishment of multiple accounts for illicit activities.
- » Difficulty establishing ultimate beneficial ownership.
- » Difficulty in distinguishing legitimate from criminal transactions.
- » Limited visibility through accounts and supply chains.

Digital channel transaction challenges

- » Fintechs and Challenger Banks lack account behaviour history.
- » Limited ability to assess individual attributes against transactions.
- » Ongoing botnet attacks to access accounts, open new accounts using breached or fake identity data.

Digital risk detection techniques

- » **Location and entities** – intelligence on devices, email addresses, physical addresses, credit cards, and other digitally-presented data.
- » **Behavioural** – analysis of human-device interactions and online behaviour patterns.
- » **Threat intelligence** – transactional data indicators that detect anomalous and high-risk behaviour based on digital footprints that criminals leave behind.
- » **Identity verification** – who an individual claims to be, based on submitted data.
- » **Identity authentication** – determining if it’s actually that person on the other end of the transaction.
- » **Assessing transaction risk** – how the entity behaves online, with other types of transactions, on other sites.
- » **Untangling complex networks** – identifying hidden relationships related to transactional data, using sophisticated artificial intelligence tools and techniques.

Positive outcomes

- ✓ Gaining a fuller view of the entities, relationships and typologies related to transactions.
- ✓ Visibility into complex transaction networks; identifying use of stolen, spoofed credentials; gathering history of behavioural data.
- ✓ Preventing intrusion by sophisticated synthetic or fake identities and breached data.

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
 - Part 1
 - Part 2
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

09: INTERNAL GAPS AND CHALLENGES (PART 1 OF 2)

Inefficient structures and tools, legacy technology and concerns over human error are holding back the industry from greater effectiveness.

Figure 7: Specific types of crime threats mentioned by the group as a result of internal gaps (n=300)



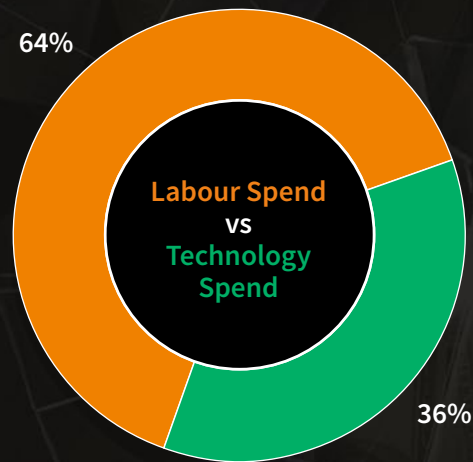
Many of the challenges and barriers to the fight against financial crime come from within the organisations themselves. Respondents cited several internal process, resource and structural issues as holding them back, including data quality, system failures, gaps in IT infrastructure and ineffective internal tools and outdated technologies being used against highly complex and sophisticated attacks. Many fear the potential repercussions of a compliance failure on the organisation in terms of reputational damage and loss of customer confidence, influencing a culture of over-cautiousness leading to over-reporting of suspicious activity and adding to work volumes.

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
 - Part 1
 - Part 2
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

09: INTERNAL GAPS AND CHALLENGES (PART 2 OF 2)

Labour vs Technology

Technology can increase operational efficiency and effectiveness of financial crime compliance, yet organisations are still spending almost twice as much on costly labour.

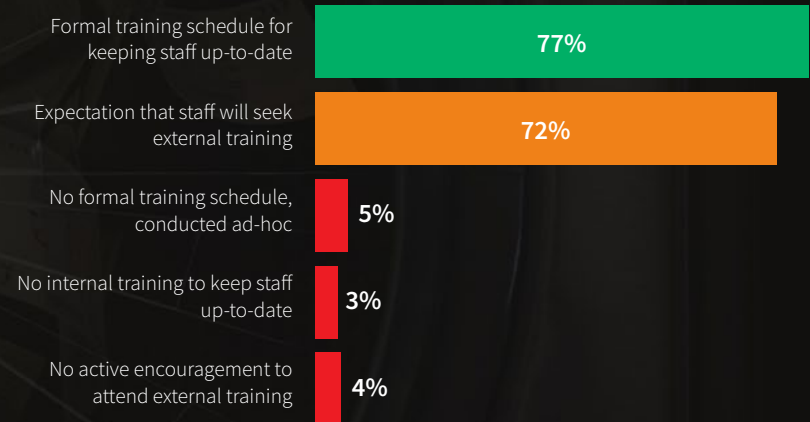


“Especially in some of the larger financial institutions you’re working with historic legacy data, legacy systems, some of that’s very difficult and expensive to change. We don’t work very agile at all. So a lot of costs come from that.”

SENIOR FINANCIAL CRIME MANAGER – AML Advisory

Training

Whilst 77% of firms have a formal training process in place to keep staff updated on new criminal methodologies, half of banks also expect their staff to independently seek external training to supplement their understanding of emerging financial crime methodologies, resulting in inconsistency across the sector.



“If you think about it, it’s cheaper in the short-term to throw human resources at a problem than to implement large-scale automated systems. The regulator expects financial institutions to demonstrate that they have the appropriate resources to combat the financial issues.”

HEAD OF GLOBAL BANKING, UK Bank

01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

10: REGULATORY PRESSURE TO BETTER UNDERSTAND THE COMPLEX WORLD OF FINANCIAL CRIME

The need for a fuller view of entities, relationships, complex networks and behaviours increases with the EU's 5th Money Laundering Directive (5MLD) and expected 6MLD regulation.

The objective of 5MLD is to further tighten anti-money laundering regulations and put more responsibility on businesses to carry out thorough due diligence on the people they're doing business with. This includes all 'obliged entities', which can be any business or individual covered under the legislation.

5MLD expands regulatory influence to a range of new sectors, including letting agents, crypto-asset exchanges, digital wallet providers and even high value art dealers. In addition to placing regulatory reporting requirements on the businesses themselves, any financial services organisation transacting with them must also conduct enhanced due diligence. This implies more work and more reporting.

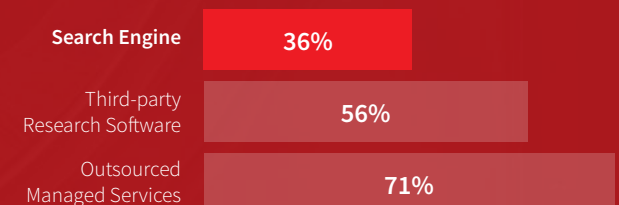
Need for stronger due diligence data and tools

The new legislation increases the requirements for enhanced due diligence measures.

- » In addition to high risk countries, enhanced due diligence (EDD) should now cover any transaction that is complex or unusually large, or where the pattern of transactions is unusual.
- » Identity verification procedures for the beneficiaries of life insurance policies need to be fully vetted before any payment is made.
- » Certain higher risk sectors, in particular, must now be subject to enhanced due diligence requirements, including oil, arms, precious metals, tobacco and anything to do with trafficking of protected species or cultural artefacts.
- » Enhanced due diligence will need to be applied whenever dealing with a country where AML controls are weak, or the situation is potentially higher risk.

A third of financial institutions use standard search engines to conduct their enhanced due-diligence

It's no longer enough for financial services organisations to rely on basic online searches. Institutions will, more than ever before, need to invest in robust software that digs deeper into relationships, behaviours and networks.



- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

11: FUTURE OBLIGATIONS TO UNDERSTAND AND DETECT PREDICATE OFFENSES

A significant number of financial organisations are concerned about their ability to detect many of the 22 predicate offences of money laundering.

In addition to the difficulties of detecting and preventing emerging digitally-based crimes, many of the financial organisations surveyed expressed at least some concern about their ability to understand and spot the financial patterns that underpin the serious criminal activities listed in the predicate offences of money laundering. Furthermore respondents expressed concern around the implications on their organisation and on other individuals, of flagging an activity as potentially linked to a predicate offence that subsequently turns out to be incorrect, highlighting the responsibility and pressure individuals may feel to ‘get it right’.

Figure 8: Degree to which your organisation is able to identify the following predicate offences (n=300)

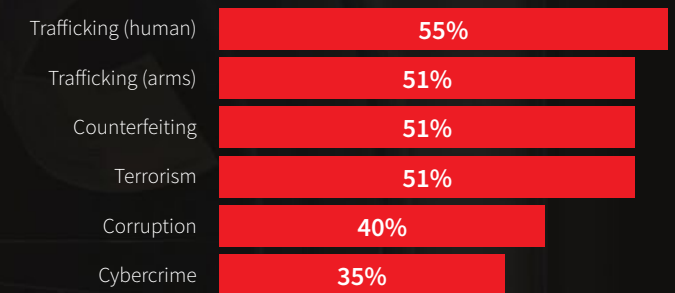


“We don’t have the data points for identifying these offences. Large institutions and small institutions are saying the same thing because they don’t know what would happen if they wrongly tagged a transaction as something that it isn’t.”

MANAGING PARTNER, UK Asset Management Firm

Fintechs and Challenger Banks

Fintechs and Challenger Banks, which have significantly digitally-focused business models, were more likely to indicate challenges with a number of these and other offences. Financial criminals may be taking advantage of this, particularly where pre-paid card services are offered.



“When you don’t have that physical presence, you can’t look at people, or assess indicators that don’t make sense given the transaction.”

DEPUTY MLRO, UK Challenger Bank

“Proceeds of illicit activities is massively relevant to Fintechs. The prepaid card market has come under scrutiny, which goes back to the on-boarding process and cardholder identification. We’ve seen an increase in the last three months of attempts on these cards.”

HEAD OF RISK & COMPLIANCE, Irish Fintech

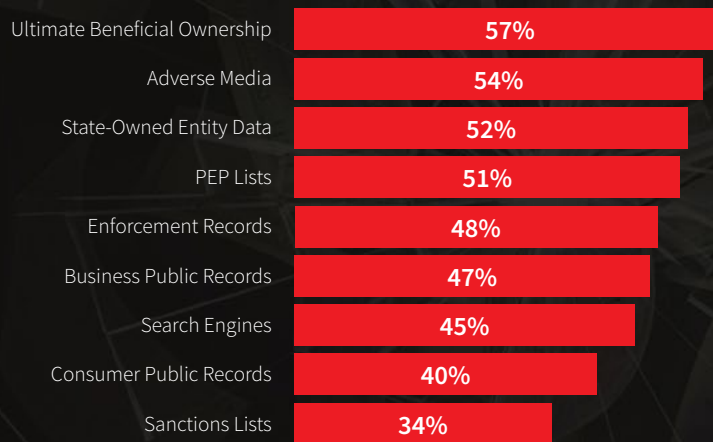
01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

12: THE QUALITY AND AVAILABILITY OF PUBLIC DATA

Many financial institutions point to current public data sources as a frustration with KYC and identity verification, in detecting those involved in predicate offences

Around half of respondents indicated less satisfaction with types of data intended to provide insights into entity relationships, criminal backgrounds and other risk factors.

Figure 9: Percentage indicating less than very satisfied with the following data sources (n=300)



Data frustrations

Lack of a centralised and trusted registry with proper controls from government was cited as a key reason for data dissatisfaction. Companies House was particularly cited as problematic, because it relies on an honour system of complete and accurate input from entities (which can include criminals). Companies House has no regulatory remit to verify the accuracy and completeness of the information submitted.

“Companies House is reliant on the people being honest about who’s behind their companies. Well, that defies the whole point because a criminal is not going to be honest about it. So how are you going to pick that up?”

SR. FINANCIAL CRIME MANAGER, UK Bank

“Ireland has no formal or official database, so to run checks on individuals can be quite challenging and manual.”

HEAD OF RISK & COMPLIANCE, Irish Fintech

“The issue for me isn’t necessarily around banks. It’s around the fact that governments haven’t put sufficient resources into things like company registries, where they actually verify the information. And, there is no real work being done by governments with lists of Politically Exposed Persons. Plus, enforcement records are patchy with agencies that are out there.”

HEAD OF GLOBAL BANKING, UK Bank

But there’s an even bigger impact...

When one data source is less effective, that can weaken the overall effort. One such example is with ultimate beneficial ownership, where cross-checking UBO data against other information sources, such as PEP and sanctions lists and adverse media, increases reliability of results. If one or more of these is inaccurate or incomplete, that reduces the overall reliability of due diligence efforts.

“With UBO, if you screen it against political exposure and sanctions and adverse media and corruption, it’s only then that you can say you’ve done enhanced due diligence on offshore companies.”

FINANCIAL CRIME LEAD, UK Fintech

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion:
Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

13: THE TRUE COST OF COMPLIANCE

The cost of financial crime compliance can be overwhelming.

The average annual cost of financial crime compliance varies across UK and Irish banks, asset management and fintech firms. It also varies by organisation size. The vast majority of this cost is based on labour, particularly among UK firms. Below is the average annual cost of compliance for financial institutions in the UK and Ireland.

Average annual cost of financial crime compliance

The overall cost of financial crime compliance, as defined in this report, comprises resources and labour, systems, solutions, data, and other governance activities. It encompasses the full range of compliance activities, including customer due diligence, sanctions screening, transaction monitoring, investigations, reporting, analytics, risk assessment, auditing, training, and others.



Regulatory reporting, rising alert volumes and higher salary demands of skilled professionals were cited as key reasons for additional labour costs. So too, are upgrades to legacy systems and training that new regulations require of organisations. That said, traditional mindsets and culture towards technology appear to be an underlying driver of all of this.

"We have so many reporting requirements that most of our financial crime team spends most of their time filling out reports and uploading information to different databases."

HEAD OF FINANCIAL CRIME, UK Fintech

"Our tendency is people don't look to make the investments into technologies until they have the Central Bank of Ireland coming in and doing a review and inspection."

HEAD OF AML ON-BOARDING, Irish Asset Management Firm

"I think there's definitely an aversion to letting a machine decide things entirely for you. But there's also a very big churn of specialists because of salary considerations."

FINANCIAL CRIME LEAD, UK Fintech

"Costs are inevitably going to come from regulation and the amount of change that has to happen. Trying to put controls in, costs money. Working with historic legacy data systems – that's very difficult and expensive to change."

SR. FINANCIAL CRIME MANAGER, UK Bank

Getting it wrong with due diligence and cybersecurity has a cost, too

Reputational risk is a huge concern amongst financial services organisations, particularly where that impacts customer acquisition and retention efforts. Added to this, firms are under considerable pressure to strike a balance between thorough and effective due diligence processes and achieving quality customer experience by minimising customer friction and false positives.

"If your bank is subject to cyber-attacks, the reputational risk and the impact that it has on your business is quite big."

HEAD OF GLOBAL BANKING, UK Bank

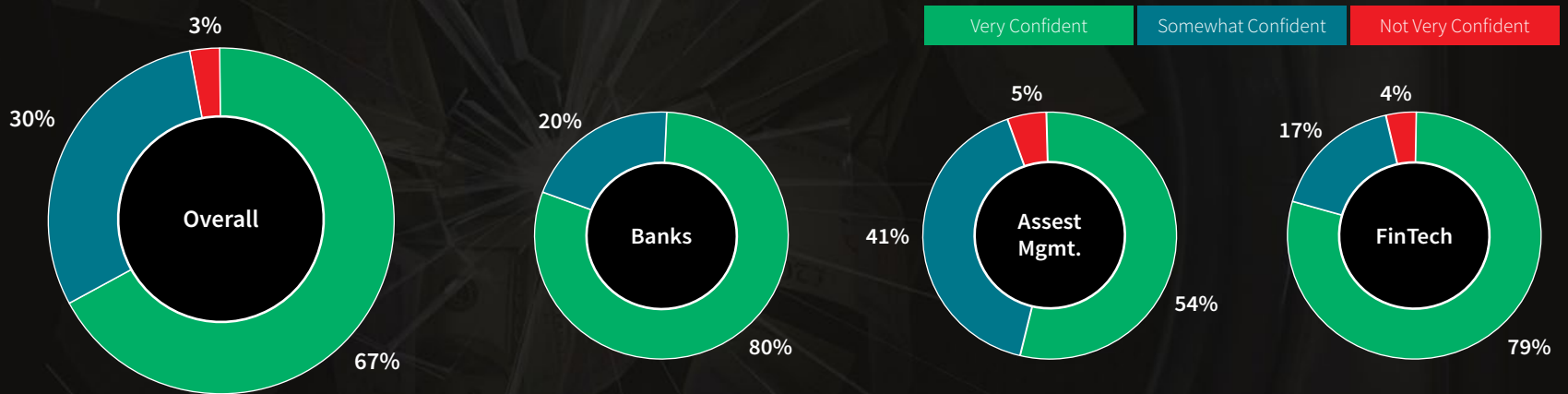
- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?**
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

14: HOW CONFIDENT ARE FIRMS AT DETECTING FINANCIAL CRIME?

Despite the numerous challenges, a majority continue to express surprisingly high confidence in their ability to identify and track new crimes and criminal methods.

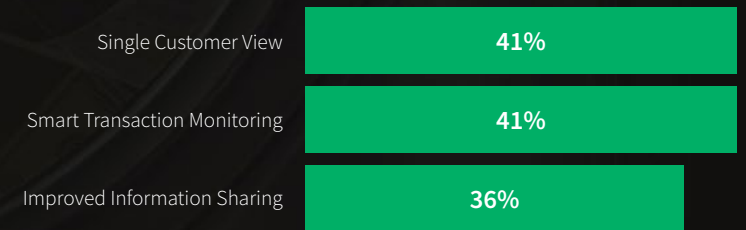
When asked to rate confidence levels against specific financial crime attacks, over half of firms expressed at least some doubt in their ability. However, when asked about their ability to identify and track new crimes and criminal methods in general, firms displayed remarkable levels of confidence, with over two thirds (67%) of firms overall saying they are very confident. Those levels increased further among fintechs (79%) and banks (80%).

Figure 10: Confidence in organisation's ability to identify and track new crime and criminal methods (n=300)



What's on financial institutions' wishlists?

Despite the apparent confidence, most respondents expressed a number of concerns about financial crime. When asked what tools would have a significant positive effect on their ability to fight crime, a single customer view was high on the list, along with better information sharing and smart transaction monitoring.



- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- 17: Appendix

15: CONCLUSION: LEARN, ADAPT, CHANGE, APPLY

Financial crime is rapidly changing – on an almost daily basis. Not only is it imperative for organisations to keep pace with these changes, but it is also essential to adapt our mindsets when it comes to fighting it.

Traditional approaches, data and systems, are no longer sufficient; using standard online search engines for background information checks isn't going to tell you everything you need to know to remain compliant with the newest anti-money laundering regulations. The good news is that the data and technology required to effectively detect and prevent all of the predicate offences cited within the EU money laundering directives are already widely available, cost-effective, and easy to source and implement across organisations of any size.

In order to more effectively fight financial crime, firms must focus on effectiveness and outcomes by:



Broadening their KYC focus to look at the wider ecosystem

Financial crime isn't limited to the immediate transaction entities that sit within the financial services sector. It moves through a much wider ecosystem that crosses sectoral boundaries, through supply and distribution chains, professional third-party enablers, such as legal and accountancy firms, and a fifth layer of business or personal relationships. Financial Institutions need to have processes, data insights and supporting technology to enable an expanded KYC view across the full ecosystem in which criminals operate.

In the digital age, we are more than just a name, address and date of birth. We are the people that we live and interact with; we are the devices and networks that we use, and more. Access to digital identity data and insights is critical to fighting financial crime, including cybercrime.

In conclusion:

Tech and biometrics, entity linking, digital identity data, deep centralised databases of PEPs, sanctions lists, enforcement data and adverse media, and more are very effective ways to authenticate the right people, identify the hidden risks and minimise friction. It's also important for firms to be able to achieve a single customer view across the organisation so that they can quickly access and dynamically monitor the risk associated with an individual or entity, right across the business.



Using data and technology to provide better insights

An increased understanding of how data and technology delivers deeper insights is essential for decision makers to implement the right systems and approaches. There is more data on individuals and entities than ever before. But one needs capable technology to shed light on linkages, behaviours and trends, and to understand who people really are.

Learning about best practices from other industry sectors, especially those within the financial services ecosystem, continues to build necessary knowledge in an ever-changing and complex environment.

Training programmes that teach more than just compliance rules are essential for getting ahead of emerging criminal methods. There is significant advantage to understanding the wider ecosystems at play and how illicit transactions move through them, such as supply and distribution channels, third-party enablers and trade-based environments. The ability to effectively spot anomalies in, for example, credit documents, or to understand new technology innovations that criminals are leveraging, would significantly enrich the collective ability of organisations to detect and stop financial crime more effectively.

Financial organisations could benefit from moving beyond rules-based compliance processes, towards a more complex analysis of patterns, behaviours and trends, enabling them to take more proactive rather than reactive action in relation to signals.

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction**
 - Part 1
 - Part 2
- 17: Appendix

16: INDUSTRY REACTION (PART 1 OF 2)

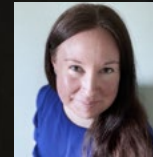


Matt Elton

Regulatory and Supervisory Technology Specialist

“There is clearly a stark contrast between, on the one side, firms resistant to change, be that in knowledge, process or the implementation of technology solutions, and on the other, a continuously evolving, and ever more sophisticated financial criminal.

With a £37bn annual cost to the UK economy from money laundering, there is an urgent need to do things differently, in a way that rebuilds a brand of trust. Establishing a reputation for the UK and its financial sector as one which takes financial crime seriously, and acts in the interest of the stability of the UK financial system, is good for the country and the industry as a whole. Technology alone may not be the silver bullet, but an approach in which all actors embrace the use of technology as an enabler to identifying suspicious and unusual activity, together with a greater degree of collaboration and information exchange between the financial sector, regulator and law enforcement agencies, could well be the answer.”



Virginie O'Shea

Founder, Firebrand Research

“The clear gaps in financial crime compliance are due to its constantly evolving nature—financial institutions must pit their compliance teams against the innovation of well-resourced cybercriminals. There is a lot of incentive for criminals to evolve, whereas compliance is constantly playing catch-up. The more digital a firm becomes, the more entry points there are for a cybercriminal to attempt to exploit. While hiring talented compliance professionals is a key requirement, firms also need to be deploying the latest in RegTech to be able to keep on the front foot. AI continues to evolve and though it is certainly not currently a replacement for humans, it can provide good support for tasks such as suspicious activity monitoring, as it is uniquely-positioned to help support pattern recognition in large volumes of data.”

- 01: Foreword
- 02: Introduction
- 03: What keeps AML & CFT professionals awake at night?
- 04: Leading types of financial crime attack
- 05: Complex transactions that are difficult to detect
- 06: A relentless volume of attacks with no end in sight
- 07: The increasing sophistication of cybercrime
- 08: Truly understanding people and their networks
- 09: Internal gaps and challenges
- 10: Regulatory pressure to better understand the complex world of financial crime
- 11: Future obligations to understand and detect predicate offenses
- 12: The quality and availability of public data
- 13: The true cost of compliance
- 14: How confident are firms at detecting financial crime?
- 15: Conclusion: Learn, Adapt, Change, Apply
- 16: Industry reaction
- Part 1 Part 2
- 17: Appendix

16: INDUSTRY REACTION (PART 2 OF 2)



Emmanuel Schizas

Regulation and RegTech Expert

“This is welcome new evidence on the potential of technology to help fight financial crime. While firms might be confident that their policies and controls are compliant, compliance is not the same as sound management of risks, and technology is key to identifying, measuring and controlling risks in this area. In 2019, the CCAF’s first RegTech Benchmark Survey found that some 60% of RegTechs claimed to be active in the AML space.

RegTech vendors might welcome the news that about half of the practitioners surveyed are dissatisfied with the information available for the purposes of customer due diligence. Adverse media and PEP screening are the sort of inputs that technology should, in principle, be well-placed to facilitate; and so we might expect to see greater penetration of RegTech solutions in such areas.

But the remaining ‘humans in the loop’ – who account for nearly two thirds of the cost of compliance - are going to prove hard to dislodge as tolerance for error is low and improving awareness of risks only creates more, not less, work for humans down the line.”



John Cant

Financial Sector Consultant

“Given the regulatory consequences, I am not surprised that most firms express high confidence levels in their abilities. However, the other findings in the report indicate that - for many - these confidence levels are achieved as a result of having to expend “super normal” levels of effort, and that these levels are not sustainable unless there is material change.”

01: Foreword
02: Introduction
03: What keeps AML & CFT professionals awake at night?
04: Leading types of financial crime attack
05: Complex transactions that are difficult to detect
06: A relentless volume of attacks with no end in sight
07: The increasing sophistication of cybercrime
08: Truly understanding people and their networks
09: Internal gaps and challenges
10: Regulatory pressure to better understand the complex world of financial crime
11: Future obligations to understand and detect predicate offenses
12: The quality and availability of public data
13: The true cost of compliance
14: How confident are firms at detecting financial crime?
15: Conclusion: Learn, Adapt, Change, Apply
16: Industry reaction
17: Appendix

17: APPENDIX: RESEARCH METHODOLOGY

A comprehensive survey was conducted with 300 financial crime compliance professionals from a variety of different types and sizes of financial institutions across the UK & Ireland, including banks, asset management firms, fintech and challengers. An additional 13 in-depth discussions were conducted with the same mix of professionals and organisations to provide further context to the quantitative survey findings.

- » Just over half (60%) of respondents came from banks, with the other 40% split evenly across asset management firms and fintechs.
- » 250 organisations were from the UK; 50 from Ireland.
- » Banks included a mix of retail, commercial, investment and private organisations; building societies were also included.
- » Reflecting the importance of the growing digital environment, fintech organisations included those providing financial services, mostly payment providers but also including a number of challenger banks and virtual currency providers.

Respondents were screened for qualification to ensure they had:

- » Responsibility for KYC/CDD, sanctions, financial crime, AML and/or risk compliance.
- » Senior level decision making responsibility for their organisation's compliance programmes and oversight for AML transaction monitoring, sanctions monitoring and/or KYC remediation activities.

For more information, please call 029 2067 8555
or email ukenquiry@lexisnexis.com

risk.lexisnexis.co.uk



About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers across industries. For more information, please visit risk.lexisnexis.co.uk and www.relx.com.

The paper is provided solely for general informational purposes and presents only summary discussions of the topics discussed. The report does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their legal advisors, compliance departments and other professional advisors about any questions they may have as to the subject matter of this paper. LexisNexis Risk Solutions shall not be liable for any losses incurred, howsoever caused, as a result of actions taken upon reliance of the contents of this paper. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies. No part of this document may be reproduced without the express permission of LexisNexis. LexisNexis Risk Solutions UK Ltd is a company registered in England & Wales at 1st Floor, 80 Moorbridge Road, Maidenhead, Berkshire SL6 8BW. Registration number 07416642. Tracesmart Limited is a LexisNexis company, operating under the trading name of LexisNexis, with an England & Wales Registration Number 3827062. Registered Office is Global Reach, Dunleavy Drive, Cardiff CF11 0SN. Authorised and regulated by the Financial Conduct Authority (Firm Reference number 742551).
Copyright © 2020 LexisNexis Risk Solutions. 361/MK/WP/1. NXR14368-00-0720-EN-UK