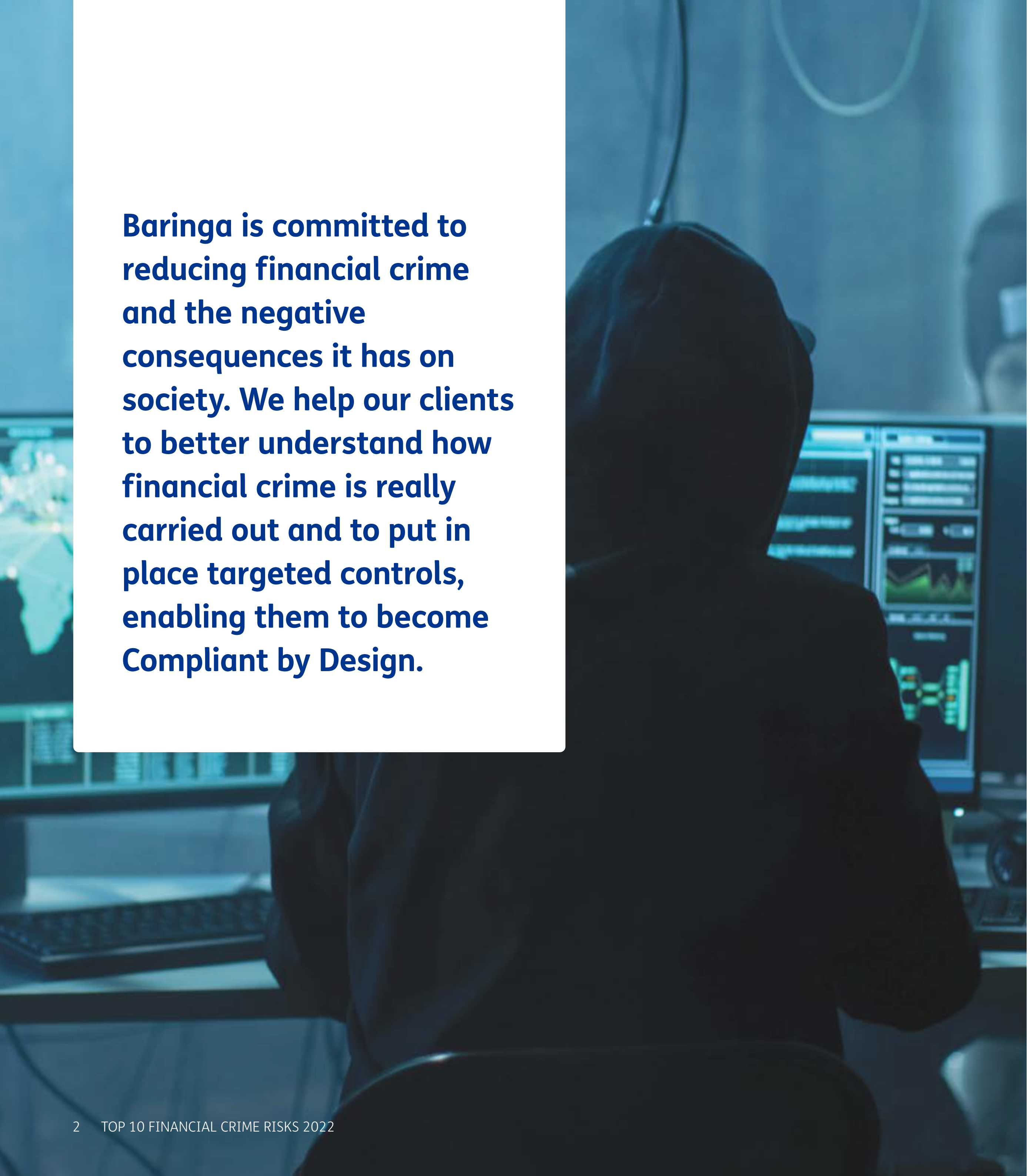
Baringa

Top 10 Financial Crime Risks 2022

The most prevalent money laundering typologies which the financial services industry is exposed to in 2022

»



Baringa is committed to reducing financial crime and the negative consequences it has on society. We help our clients to better understand how financial crime is really carried out and to put in place targeted controls, enabling them to become Compliant by Design.

Contents

Introduction 3
Executive summary 4
Top 10 analysis 10
Risk prevalence 11
Risk mitigation 14

Sector specific analysis 16
Retail Banking 17
Business Banking 18
Corporate and Wholesale 19
Capital Markets 20
Money Services Businesses 21
Insurance 22
Asset and Wealth Management 23
Trade Finance 24

Improving prevention 25

Appendices 26
Appendix A - Top 10 Typologies 27
Appendix B - References 32

Introduction

Top 10 financial crime risks research

Baringa has undertaken further research into the most prevalent typologies for carrying out financial crime in the financial services industry and across different sectors, building on findings from our previous report run in 2020, accessible via Baringa's website[1]. As a part of this study, we compiled a list of typologies, split across the main sectors within the financial services industry and covering Retail Banking, Business Banking, Corporate and Wholesale Banking, Capital Markets, Trade Finance, Money Services Businesses, Asset Management, Wealth Management and Insurance. The list of typologies is:

- An extension of the list of typologies we compiled for the previous iteration of this study
- Based on our experience of working with investigations and intelligence teams in financial services as well as with law enforcement and government bodies across the globe
- Corroborated using publicly available information from government and industry bodies, as well as high profile cases of money laundering in the media.

This list was then shared with Financial Institutions (FIs) from each sector across the globe in the form of a survey. Institutions were asked to:

1. Assess how often their organisation encounters each typology
2. Evaluate how effective their organisation is at mitigating each typology
3. Highlight any additional typologies which they have encountered which were not on the initial list

This report describes the findings of the study and the survey undertaken, with a particular focus on the 'Top 10' typologies considered to pose the greatest risk to the financial services industry. Results have been aggregated to identify the Top 10 typologies overall and also at an individual sector level. We have also compared the results to the previous study to understand if the risks that FIs are exposed to has changed with time. Please contact us if you would like to discuss any of the content of this report in more detail.

Thank you to all organisations who participated – your contribution to these valuable industry insights is much appreciated.

It is worth noting the following key points about this exercise:

- The list of typologies referred to in this report does not represent the full range of typologies used by criminals to launder money – our objective is to draw attention to the most prevalent typologies that need to be mitigated
- The focus of our study is money laundering, not terrorist financing, fraud or other types of financial crime (these may be considered in future research)
- As this is only Baringa's second financial crime risks benchmark, we expect it to evolve over time as readership and the number of participants increase
- We created a unique survey for each sector included in the study, to identify the most prevalent typologies for that sector. Participants that had experience of working in more than one sector were asked to respond to the survey for each sector
- A single typology may be applicable to more than one sector and therefore would be ranked for frequency and effectiveness in every sector that it appears in
- In some cases, a typology will have equal frequency and/or effectiveness score as another. In such cases we have assigned the same ranking for both typologies
- Financial crime typologies could be presented at significantly different levels of granularity; the level included here is intended to group typologies where the characteristics are broadly similar, even if they may be executed in slightly different ways. For example, whilst the following two examples are different, they both involve the use of high value assets to transfer value:
  - **Example 1:** A drug trafficker purchases second-hand cars with cash and then sells them on to local car dealerships, enabling seemingly legitimate bank transfers into her account
  - **Example 2:** A fraudster convinces vulnerable customers to transfer money into his bank account, uses the funds to purchase jewellery, and then sells it abroad in his home country
- Similarly, the typologies are presented independently of the predicate crimes that generated the illicit funds – in the examples above, the fact the funds were generated using drug trafficking or fraud is considered inconsequential to the means by which they were laundered
- The survey considers typologies which impact FIs only
- References to all third-party sources used are provided in Appendix B of this document.

1 'Baringa Top 10 Financial Crime Risks Report', https://www.baringa.com/en/insights-news/points-of-view/baringa-top-10-financial-crime-risks-report/

Executive summary

To be effective at preventing financial crime, and the negative consequences it has on our society, we must first establish consensus on the primary risks we are attempting to mitigate.

Collectively across the financial services industry, a huge amount of time is spent on implementing and refining financial crime control frameworks. Resources are prioritised according to a 'risk-based approach' by devising risk taxonomies, conducting enterprise-wide risk assessments and directing attention towards the areas of the business with the greatest number of Ambers and Reds. However, these risk taxonomies tend to give a disproportionate amount of attention to regulatory requirements, and the risk of not meeting them, rather than the means by which financial crime is actually carried out – that is, the financial crime typologies the organisation is at *risk* of being exposed to.

This may be an appropriate way of prioritising a compliance programme, but it is not the most effective way of preventing financial crime. No amount of culture programmes, gap analyses or machine learning algorithms will help to stop criminals reaping the benefits of their illicit gains if their mechanisms for doing so are not understood.

This study is intended to uncover the most prevalent means for laundering money, to enable FIs across each sector within the financial services industry to be more proactive in reducing financial crime and the negative consequences it has on society. It is intended to support you in reducing crime by providing greater clarity about how criminals are exploiting your organisation. By tackling it head on, your organisation will become Compliance by Design and realise compliance much more efficiently.

The 'Top 10' most prevalent money laundering typologies[2] encountered across the financial services industry in 2022, based on the findings of this study, are outlined here:

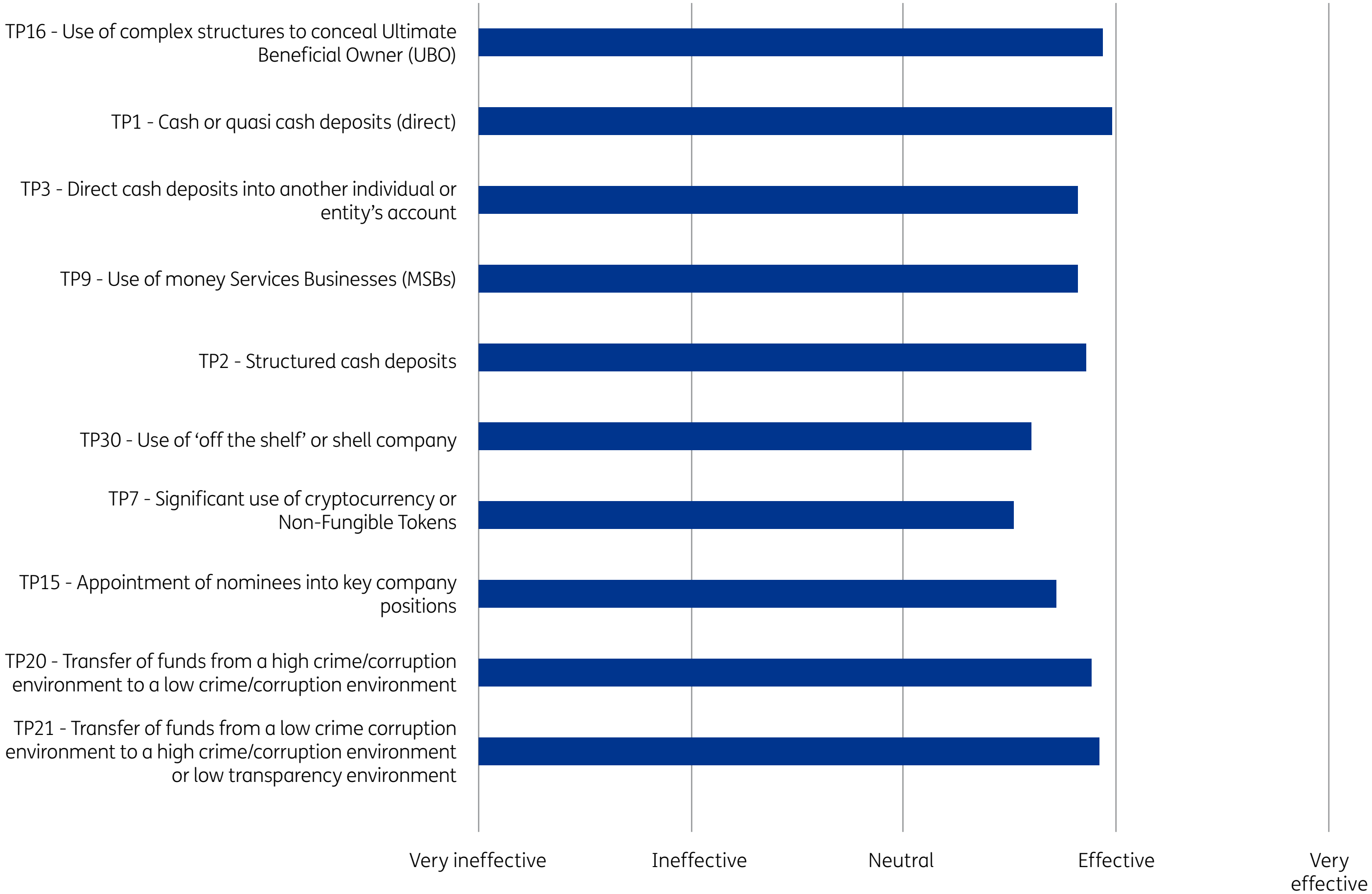
Baringa

Top 10 Financial Crime Risks 2022

1. Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)
2. Cash or quasi cash deposits (direct)
3. Direct cash deposits into another individual or entity's account
4. Use of Money Services Businesses (MSBs)
5. Structured cash deposits
6. Use of 'off the shelf' or shell company
7. Significant use of cryptocurrency or Non-Fungible Tokens
8. Appointment of nominees into key company positions
9. Transfer of funds from a high crime/corruption environment to a low crime/corruption environment
10. Transfer of funds from a low crime/corruption environment to a high crime/corruption or low transparency environment

2 Typologies have been ranked according to the aggregate number of times they were encountered by survey respondents over a given time period. Participants were asked to rate how frequently they encountered a typology across the following categories; 'Never (No known occurrences)', 'Exceptionally (Less than annually)', 'Rarely (Annually or more)', 'Frequently (Quarterly to monthly)', 'Very frequently (Monthly or more)'. For the purposes of simplifying the aggregation of the number of occurrences of each typology, it has been assumed that 'less than annually' means once every two years.

The average perceived level of effectiveness at mitigating each of the Top 10 typologies across the industry is summarised below[3]:



3 Effectiveness has been measured here by averaging the level of effectiveness selected by each of the respondents for each typology. Participants were asked to rate how effective they believe their organisation to be at preventing each typology by selecting one of the following options: 'Very ineffective', 'Ineffective', 'Neutral', 'Effective' or 'Very Effective'.

For the typologies included in the previous report, the change in effectiveness and/or frequency has been mapped as follows:

The x axis shows how the frequency of a typology has changed from the previous report, moving from left, representing a decrease in frequency, to right, representing an increase in frequency. Effectiveness has been plotted on the y axis, moving from the bottom of the y axis, representing a decrease effectiveness, to the top of the y axis, representing an increase in effectiveness.

TP4 - Use of 'mules' (complicit or non-complicit)

TP5 - Control of another person to deposit funds

TP6 - Cash deposits through third party

TP8 - Cash deposits through Bitcoin ATMs

TP10 - Use of informal remittance systems

TP11 - Use of gambling outlets

TP12 - Use of merchants to process illicit transactions

TP13 - Repayment of loans using illicit funds

TP14 - Integration of illicit funds into illicit cash intensive businesses

TP17 - Use of senior public or corporate position to extricate misappropriated funds

TP18 - Use of 'shell accounts' to pool illicit funds

TP19 - Abuse of crowdfunding platforms to pool funds

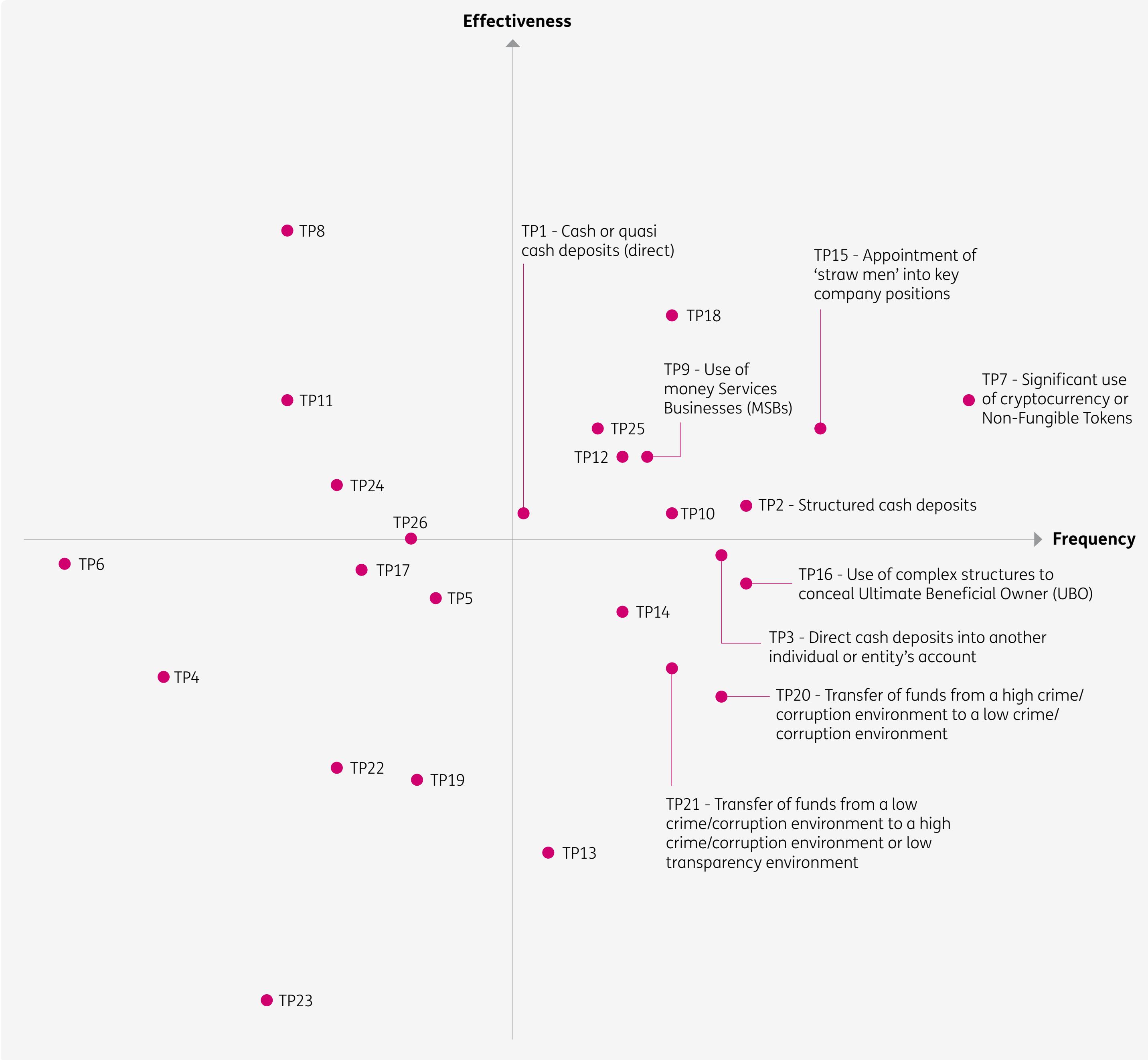
TP22 - Use of complex lending schemes

TP23 - Mirror trading

TP24 - Use of high value assets to transfer value

TP25 - Use of falsified or phantom trade shipments

TP26 - Takeover of financial systems



Whilst the prevalence of some of these typologies will be very familiar, some interesting conclusions can be drawn from the results:

The Top 10

- Despite a slight decrease in prevalence since the previous report, 50% of all cash-based typologies still appear in the Top 10, comprising 30% of the most prevalent typologies overall
- Consistent with our findings from our previous report, the controls in place across the industry are still not considered to be effective at mitigating any of the Top 10 risks, highlighting that there is still significant room for improvement

There continues to be a relatively weak correlation between the prevalence of a risk and how effectively it is being mitigated, which suggests the current approach to mitigating financial crime is not truly 'risk-based'.

- Many of the Top 10 typologies enable individuals who are unknown to an FI to place funds into that organisation, whether directly or via third party organisations; as long as FIs continue to permit channels which offer such a high degree of anonymity, criminals will continue to exploit them
- Three of the Top 10 most prevalent typologies, *use of complex corporate structures to conceal UBO, use of 'off the shelf' or shell companies* and *appointment of nominees into key company positions* all relate to corporate structures and highlight how they can be abused for the purposes of money laundering. Subterfuge in business activities is clearly a compelling way to carry out financial crime and ongoing scandals highlighted by investigative journalism and increased awareness of the lack of controls in place for company registration may have helped to bring this to the fore
- Of the Top 10 most prevalent typologies, organisations are most confident in their ability to mitigate money laundering via *cash or quasi-cash deposits*. This is likely to be because it is such a well-established typology and cash's physical nature means there are a broader range of controls that can be put in place to reduce misuse. However, the FCA's recent first criminal prosecution[4] is a timely reminder of how important it is to understand source of funds, even for clients where high cash usage might be expected
- Use of crypto and Non-Fungible Tokens (NFTs) for laundering money is the biggest riser between 2020 and 2022 and, if anything, the effectiveness of controls to mitigate this typology have reduced. This change is likely as a result of a heightened awareness of this medium for laundering money coupled with a recognition that not enough is currently being done to address this risk
- Some sectors within FS are by nature more susceptible to money laundering than others, given the products and services offered. For example, we identified 25 typologies relevant to Business Banking, versus five typologies for Asset Management and Wealth Management. This does not mean that Asset Management and Wealth Management organisations are not at risk of money laundering, rather that there are fewer ways by which they can be used to launder money.

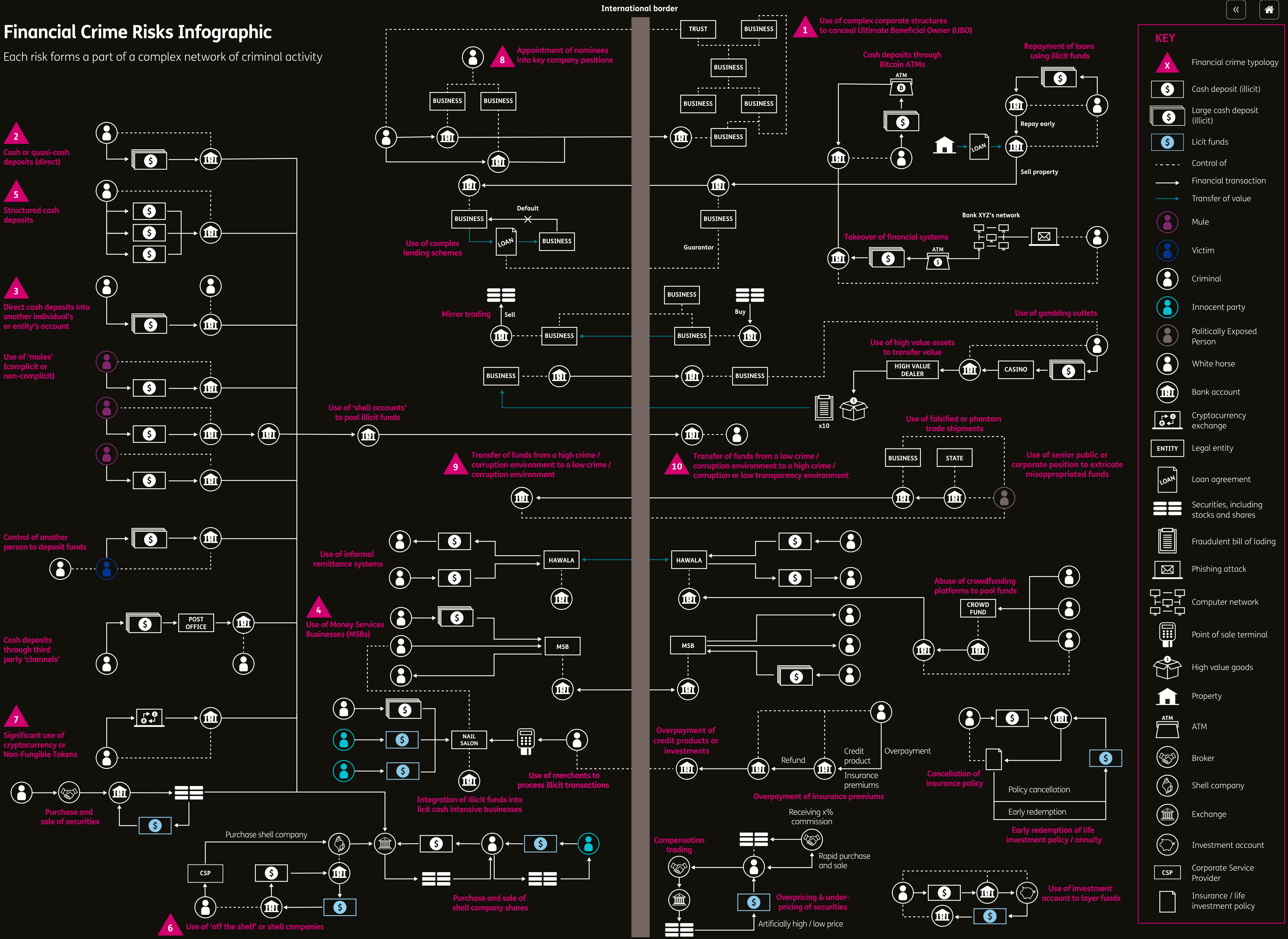
Beyond the Top 10

- Mirror trading has reduced in frequency between 2022 and 2020 – this may be a recognition of the fact that, whilst it has led to large scale incidents of financial crime, these incidents were actually relatively contained and not pervasive across the industry
- The least effectively mitigated typologies are specific to particular products or sectors, for example *abuse of crowdfunding* and *early redemption of life investment policy or annuity*. This may suggest that ostensibly lower risk sectors still need to do more to ensure that the risks that they do have are appropriately mitigated
- The *use of mules* did not appear in the overall Top 10, however it continues to feature in the Top 10 for Retail Banking and Business Banking. In alignment with our experience, this typology continues to be pervasive but is limited to a small number of sectors. There may also have been a slight drop as a result of greater difficulty in making physical deposits during the pandemic
- Some of the less prevalent typologies – e.g. *takeover of financial systems* – are relatively poorly mitigated but have a high business and customer impact, which should be taken into account when evaluating them against the organisation's risk appetite
- Typologies relating to *early*, or *overpayments*, are some of the least effectively mitigated risks, which highlights the need for organisations to differentiate what constitutes a legitimate redemption request from suspicious behaviour.

4 'NatWest fined £264.8 million for anti-money laundering failures', FCA, https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures

Financial Crime Risks Infographic

Each risk forms a part of a complex network of criminal activity



How Baringa can help

Baringa's Financial Crime team are specialists in helping clients to identify their unique financial crime risks and implementing proportionate controls to detect and mitigate these risks.

We have worked on the front line with both financial institutions and government departments to reduce financial crime. Our deep financial crime knowledge, market insights and regulatory experience enables us to effectively support our clients in navigating the complex regulatory and criminal environments. Recognising that each financial institution has a unique business model, risk profile and risk appetite, we provide a tailored approach to each of our clients, whilst sharing insights into common industry challenges.

Please contact us for more information about the services we provide and how we can help your organisation. Our contact details can be found on the last page of this document.

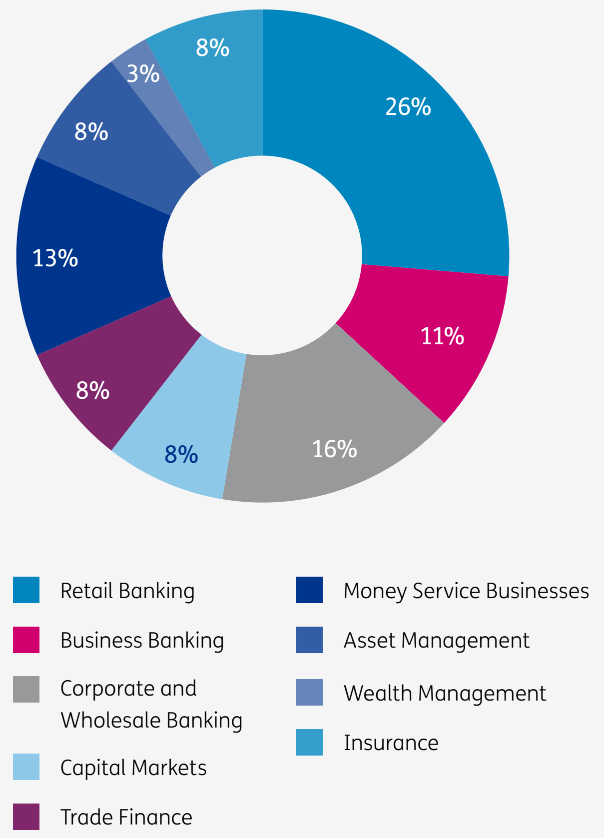
Top 10 analysis

Survey respondents

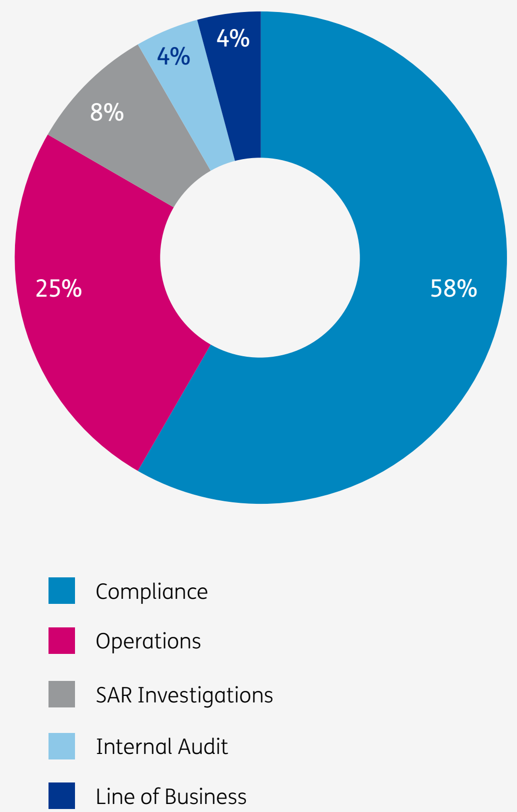
Respondents were primarily based in the UK and were split across the following sectors;

- Retail Banking
- Business Banking
- Corporate and Wholesale Banking
- Capital Markets
- Trade Finance
- Money Service Businesses
- Asset Management
- Wealth Management
- Insurance

The proportion of respondents across each sector were as follows:

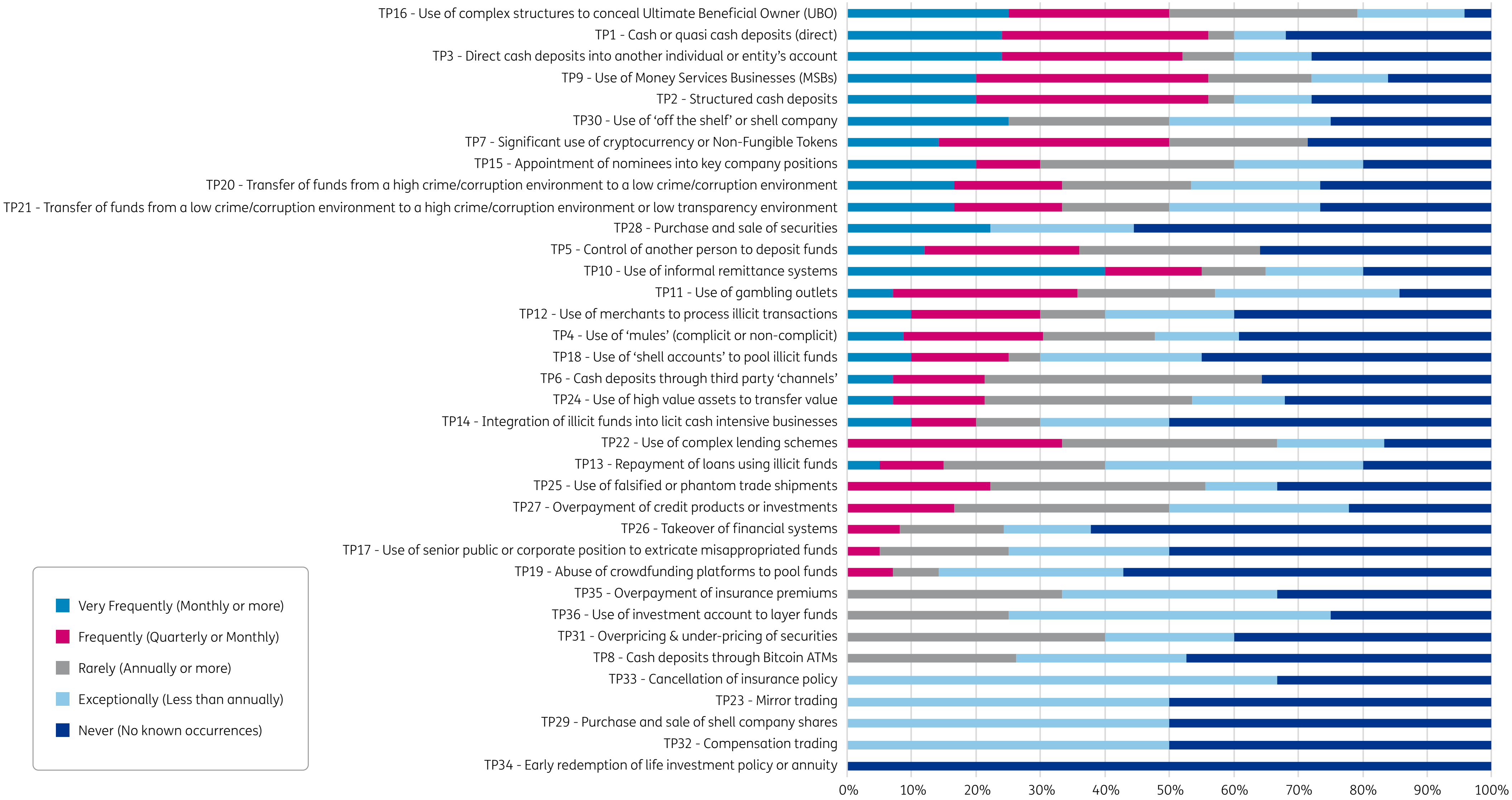


The majority of respondents (58%) work within the second line of defence, whilst 38% work in the first line of defence (Operations and Lines of Business) and 4% work in the third line of defence (Internal Audit):



Risk prevalence

Industry participants were asked to rank how frequently they observed each typology. The breakdown of their responses is summarised below:



When comparing the Top 10 typologies in 2022 to 2020, we see their prevalence has changed, as illustrated below:

2020			2022
TP1 - Cash or quasi cash deposits (direct)			TP16 - Use of complex structures to conceal Ultimate Beneficial Owner (UBO)
TP6 - Cash deposits through third party 'channels'	↓18		TP1 - Cash or quasi cash deposits (direct)
TP4 - Use of 'mules' (complicit or non-complicit)	↓16		TP3 - Direct cash deposits into another individual or entity's account
TP9 - Use of money Services Businesses (MSBs)			TP9 - Use of money Services Businesses (MSBs)
TP16 - Use of complex structures to conceal Ultimate Beneficial Owner (UBO)			TP2 - Structured cash deposits
TP11 - Use of gambling outlets	↓14	NEW	TP30 - Use of 'off the shelf' or shell company
TP3 - Direct cash deposits into another individual or entity's account		↑21	TP7 - Significant use of cryptocurrency or Non-Fungible Tokens
TP2 - Structured cash deposits		↑14	TP15 - Appointment of nominees into key company positions
TP5 - Control of another person to deposit funds	↓12	↑13	TP20 - Transfer of funds from a high crime/corruption environment to a low crime/corruption environment
TP24 - Use of high value assets to transfer value	↓19	↑12	TP21 - Transfer of funds from a low crime/corruption environment to a high crime/corruption environment or low transparency environment

Key:

↓x: Moved down to x most frequent typology in 2022, having been in the Top 10 in 2020

↑y: Moved up from y most frequent typology having not been in Top 10 in 2020

NEW: Typology is new to this iteration of the report

We made the following observations as a part of our 2022 analysis of risk prevalence, and compared with the previous report:

- Results show that cash-based typologies continue to play a significant role in the Top 10, with 30% of the most frequent typologies in 2022 being linked to cash. This has only reduced slightly from the previous survey in which 40% of the Top 10 were cash-based, suggesting that despite the impact of the COVID-19 pandemic on the use of cash, it remains a significant vehicle for money laundering
- *Use of complex corporate structures to conceal UBO* was the most frequently observed typology overall, which was witnessed by 94% of organisations in relevant sectors. This is an increase from the previous report that identified this as the 5th most prevalent typology. This could be explained by the increased focus that organisations are placing on identifying UBOs following revised regulations, such as the 5th Money Laundering Directive ('5MLD') which mandated public accessibility of UBO lists and put additional requirements in place for organisations to verify the senior managing official of corporates and to collect proof of the company's registration on, or excerpt of, the PSC Register
- When compared with results from the previous survey, only 50% of the Top 10 also appeared in the 2022 top 10. For example, frequency in the *use of mules* has significantly decreased, from 3rd to 16th most frequently observed typology. However, it still features in the Top 10 for the Retail Banking and Business Banking sectors and so the decrease may be partially explained by the breadth of sectors represented in this version of the report. It is also possible that consumer education campaigns – such as those from Europol and ActionFraud[5] – have started to have an impact
- *Cash deposits through third party 'channels'* was the biggest faller, decreasing from the 2nd to 18th most frequent typology– this may have been as a result of far fewer cash-based businesses being in operation during the COVID-19 pandemic, making this a less viable option for laundering. It is noteworthy that the FCA recently publicly mentioned the use of the post office – an example of one of these channels – for laundering money for the first time[6]
- Another notable change was the reduced frequency that organisations witnessed money laundering through *use of high value assets to transfer value* which has reduced from the 10th to 19th most prevalent typology. The pandemic may have also impacted this typology, with the closure of the physical outlets of jewellers and pawnbrokers, for example, reducing the opportunity for anonymous deals
- Money laundering through *early redemption of life investment policy or annuity* was the only typology never witnessed by any organisation. The respondents highlighted that they had relatively effective controls in place in order to mitigate this typology and, given there are far easier ways to launder money, this may simply not be attractive to criminals
- As may be expected, the rising popularity of cryptocurrency has led to a dramatic rise in awareness of crypto and NFTs being abused for the purposes of money laundering, with this typology moving from 21st to the 7th in 2022. In our experience, more FIs have recognized the need to identify customer transactions involving crypto exchanges which may increase the likelihood a customer is carrying out nefarious activity, even if they do not deal with transactions in cryptocurrencies directly
- It is surprising to see the decrease in frequency of money laundering via *gambling outlets*, given the number of AML failings that have been highlighted across the gambling industry recently, including Betfred, that was fined £2.9m (GBP) for failure in its money laundering controls[7], and the increased focus from AUSTRAC on the gambling sector, following its investigations into Crown Resorts and Star Entertainment for AML failings.[8] It is possible that the rationale for excessive gambling activity on customer accounts is too opaque and consequently treated as fraud or credit risk concerns
- Overall, the limited correlation between risk prevalence and mitigation suggests that organisations are still struggling to deploy effective controls to their most prevalent risks; out of the Top 10 most frequent typologies in 2022, only 60% appeared in the Top 10 most effectively mitigated.

5 'Money muling', Action Fraud, https://www.actionfraud.police.uk/a-z-of-fraud/money-muling

6 'Fighting financial crime – the force multiplier effect', FCA, https://www.fca.org.uk/news/speeches/fighting-financial-crime-force-multiplier-effect

7 'Betfred fined almost £2.9m over gambling safety check failings', The Guardian, https://www.theguardian.com/society/2022/sep/28/betfred-fined-pounds-2-point-9m-gambling-safety-checks-money-laundering-controls

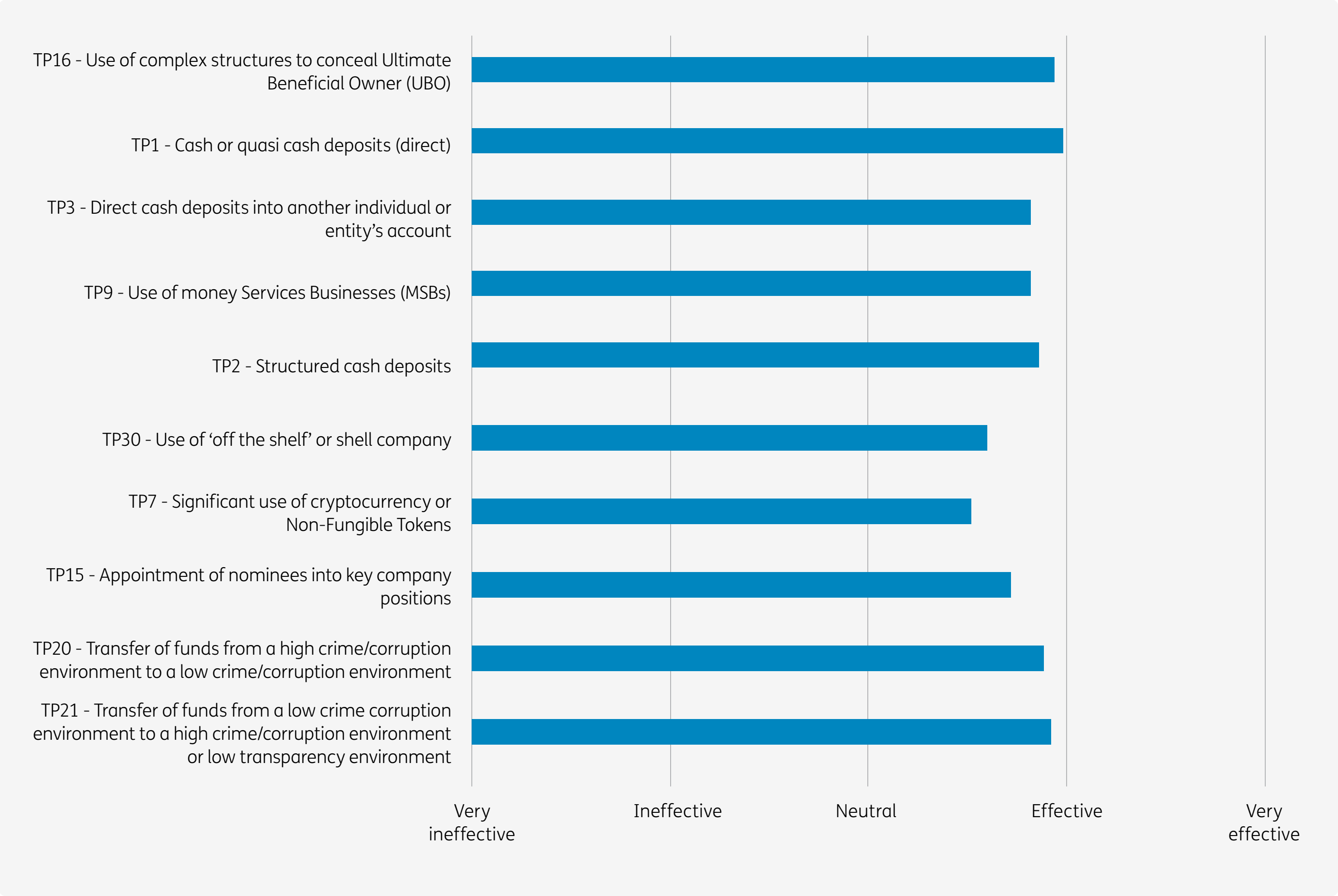
8 'Star Entertainment: Shares fall on money laundering claim', BBC, https://www.bbc.co.uk/news/business-58866576 and 'AUSTRAC claim alleges A$69 billion laundered through Crown Resorts', Thomson Reuters, https://insight.thomsonreuters.com.au/business/posts/austrac-claim-alleges-a69-billion-laundered-through-crown-resorts

Risk mitigation

Mitigation of the Top 10

Industry participants were also asked to comment on how effective they considered their institution to be at mitigating each typology. The results were then compared to the Top 10 most prevalent typologies to determine how effective organisations' controls are relative to their risk exposure.

On average the financial services industry does not consider itself to be effective at mitigating any of the Top 10 most frequent risks, including cash-based typologies that are the most effectively mitigated.



- Despite the prevalence of typologies linked to corporate structures in the Top 10, the results also show that organisations are lacking effective controls to mitigate the risk of *'off the shelf' or shell companies and appointment of nominees into key company positions*, which are two of the least effectively mitigated typologies of the Top 10
- The upcoming Companies House reforms planned as part of the Economic Crime and Corporate Transparency Bill will seek to improve transparency over ownership of UK companies. However, the effectiveness of these reforms in reducing money laundering remains to be seen, particularly given that it will still be possible for UK companies to be controlled by offshore companies that will not be subject to the reforms and may continue to enable opaque ownership structures
- Organisations felt they were least effective at mitigating the risk of money laundering through the *use of cryptocurrency or Non-Fungible Tokens* for the most prevalent risks. In fact, this is one of the least well mitigated typologies overall – at 28th – which implies it requires much more attention. This could be explained by the increased attention that FIs are paying to the money laundering risks presented by crypto and the attention this is receiving from the regulator, highlighted by the extended definition of 'obliged entities' within the 5MLD to include crypto asset exchange providers and custodian wallet providers. Based on our experience, FIs are starting to consider the source of funds for crypto deposits specifically as part of their KYC processes.

Beyond the Top 10

- On average the only typologies that are mitigated effectively are *overpayment of insurance premiums and compensation trading*, which are exclusive to the Insurance and Capital Markets sectors respectively. These are quite sector-specific and also considered very infrequent which may enable confidence they are mitigated appropriately
- The least well mitigated typology overall was *use of mirror trading*. This is clearly a difficult typology to mitigate given the complexity of identifying related trades where the beneficiary may be one and the same. However, the decrease in its perceived prevalence between 2020 and 2022 may also highlight an acknowledgement that, following the initial regulatory and media attention, the instances of this typology have been established to be relatively contained and may not require significant attention from the broader industry
- Despite its prevalence, *use of MSBs* was the 11th most effectively mitigated typology, suggesting that whilst organisations are aware of this typology, they struggle to mitigate it. Historically, this has been a challenge because incomplete originator and beneficiary information is provided to the FI processing the MSBs transactions, making it difficult to quantify the risk. Insisting that this is provided, as required by the EU Funds Transfer Regulations (and FATF Recommendation 16)[9], can be at odds with retaining lucrative business and, where it is provided, may be difficult to integrate with existing financial crime detection systems. MSBs may also exploit the regulatory provision that allows for CDD not to be carried out on customers undertaking 'occasional transactions' below 1,000 euros by having limited controls in place to identify transactions which are linked to the same customer
- Cash deposits through bitcoin ATMs had a significant increase in effectiveness of mitigation whilst also becoming much less prevalent. This is likely to be as a result of the FCA highlighting that they have not approved any firms to offer crypto ATM services, rendering them all illegal[10].

9 'Wire Transfer Regulation (WTR), Regulation (EU), 2015/847 (WTR)', Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=ET, and 'The FATF Recommendations', Financial Action Taskforce, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf

10 'Warning on illegal crypto ATMs operating in the UK', FCA, https://www.fca.org.uk/news/news-stories/warning-illegal-crypto-atms-operating-uk

Baringa

Sector specific analysis

Retail Banking

Typology	Frequency ranking (2022)	Frequency ranking (previous)[11]
TP3 - Direct cash deposits into another individual or entity's account	1	7
TP1 - Cash and quasi cash deposits (direct)	2	2
TP2 - Structured cash deposits	3	3
TP7 - Significant use of cryptocurrency or Non-Fungible Tokens	4	12
TP10 - Use of informal remittance systems	5	10
TP9 - Use of Money Services Businesses (MSBs)	6	=4
TP5 - Control of another person to deposit funds	=7	=4
TP4 - Use of 'mules' (complicit or non-complicit)	=7	1
TP11 - Use of gambling outlets	9	6
TP27 - Overpayment of credit products or investments	10	New to this survey

- Cash continues to be king when it comes to laundering money, and this is shown to be particularly true for Retail Banking evidenced by the top three most frequent typologies which are all cash-based
- The increase of cash deposits into another person's account is particularly interesting, perhaps implying this is seen as a more favourable method of moving the proceeds of crime than the account holder paying them into their own account and then transferring them on. Certainly, some institutions still do not require ID&V checks for individuals depositing funds into an account, making this typology difficult to mitigate
- Individual responses to how frequently cash-based typologies are witnessed vary substantially between organisations that witness them 'very frequently' and others that responded 'never'. This can be explained by the distinction between organisations such as neo-banks that tend to restrict cash usage, and more traditional FIs that typically witness much more cash-based activity
- Whilst the *use of mules* decreased significantly in overall prevalence in 2022 from the previous report, it appears in the Top 10 most frequently witnessed typologies for Retail Banking in both surveys. This is consistent with our experience, which suggests mules continue to be a common means for laundering money
- *Use of informal remittance systems* has increased in frequency within the Top 10 for Retail Banking, compared with the previous report (from 10^{th} to 5^{th}). The impact of the pandemic on travel may have led to criminals increasing their reliance on remittance services to send money internationally. This is aligned with research carried out by the IMF, which found that containment measures introduced by the pandemic that might have been expected to cause a decrease in remittance use was outweighed by the need for migrants to send funds to their families.[12] Additionally, the emergence of 'off chain' crypto transactions, whereby criminals share details of virtual wallets to transfer value, may also have led to an increase in this typology
- One respondent highlighted Chinese underground banking and 'Daigou' as another example of an *informal remittance system* which allows Chinese nationals to move value out of China in excess of capital control limits by exchanging it for illicit funds in the UK[13]
- Overall, the Top 10 in Retail has remained relatively consistent, with only two typologies being replaced. This implies criminals have tried and trusted methods for laundering money in this sector. Yet, on average, Retail institutions consider themselves effective at mitigating only two of these typologies – *use of MSBs* and use of *informal remittance systems*. All others have more significant room for improvement.

11 Whilst it has been possible to compare the prevalence of typologies between surveys for Retail Banking, this has not been possible for the remaining sectors. This is due to the limited sector information that was collected in the previous survey.

12 'Defying the Odds: Remittances During the COVID-19 Pandemic', IMF, https://www.imf.org/-/media/Files/Publications/WP/2021/English/wpiea2021186-print-pdf.ashx

13 'Chinese Underground Banking and 'Daigou'', NCA, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/445-chinese-underground-banking/file

Business Banking

Typology	Frequency ranking (2022)
TP9 - Use of Money Services Businesses (MSBs)	1
TP1 - Cash and quasi cash deposits (direct)	=2
TP2 - Structured cash deposits	=2
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	=4
TP30 - Use of ‘off the shelf’ or shell companies	=4
TP15 - Appointment of nominees into key company positions	=4
TP3 - Direct cash deposits into another individual or entity’s account	=7
TP5 - Control of another person to deposit funds	=7
TP4 - Use of ‘mules’ (complicit or non-complicit)	9
TP10 - Use of informal remittance systems	10

- The Business Banking sector included the largest number of typologies compared with other sectors, with 25 out of 36 typologies identified. This highlights the breadth of ways in which this sector can be abused for the purposes of financial crime. It can be very attractive to criminals given the ease with which accounts can be opened and the greater level of anonymity afforded when compared to Retail
- Consistent with Retail Banking, responses for Business Banking varied substantially between organisations that witnessed cash-based typologies more frequently than others, on account of traditional FIs offering more cash-based services and products than neo-banks
- *Use of MSBs* was the most frequently observed typology for Business Banking organisation. It is often difficult to establish the source and destination of funds when there is frequent activity with an MSB. For small businesses, this can make it very difficult for the FI to determine whether this activity is likely to be suspicious or not. This may help to explain why, despite Business Banking respondents highlighting that this typology is prevalent, it is also one of the least effectively well mitigated typologies in the Business Banking Top 10 risks. It also highlights the importance of FIs putting pressure on MSB clients to provide information required to identify the payer and payee
- Similarly, the *use of informal remittance systems* was ranked as one of the least well mitigated typologies, which is an interesting contrast to Retail Banking given that *use of MSBs and use of informal remittance systems* were the two typologies most effectively mitigated. This may highlight the difficulty of understanding whether these types of transactions are or are not aligned with the expected behaviour of the organisation, which is simpler to understand for individual customers
- *Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)* was the most effectively mitigated typology in Business Banking, which was also ranked the most effectively mitigated of the overall Top 10 typologies in the previous report. Despite this, its continued prevalence as a method for laundering money means organisations must ensure their controls remain effective at mitigating this risk. With the upcoming reforms to Companies House proposed as part of the UK’s Economic Crime and Corporate Transparency Bill, it remains to be seen if this typology will become less prevalent with more scrutiny of UK company ownership.

Corporate and Wholesale

Typology	Frequency ranking (2022)[14]
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	1
TP9 - Use of Money Services Businesses (MSBs)	2
TP20 - Transfer of funds from a high crime/corruption environment to a low crime/corruption environment	3
TP21 - Transfer of funds from a low crime/corruption environment to a high crime/corruption or low transparency environment	4
TP30 - Use of 'off the shelf' or shell companies	5
TP18 - Use of 'shell accounts' to pool illicit funds	6
TP1 - Cash and quasi cash deposits (direct)	=7
TP2 - Structured cash deposits	=7
TP22 - Use of complex lending schemes	9
TP3 - Direct cash deposits into another individual or entity's account	10

- Given the level of anonymity it provides, it follows that the use of complex corporate structures is a prevalent method of laundering money via Corporate and Wholesale organisations. On average, the Corporate and Wholesale Banking industry do not think they are currently effective at mitigating this typology, in contrast to Business Banking, and this is likely to be due to the complexity of some of the clients banked in this space. As mentioned previously, the effectiveness of the upcoming Companies House reform in mitigating risks associated with complex corporate structures remains to be seen
- Cash-based typologies featured in 30% of the Top 10 typologies for Corporate and Wholesale in this year's survey, highlighting the susceptibility of cash to being used for laundering money even within more established corporations which might be considered 'safer'. As was highlighted by the recent FCA criminal prosecution, really understanding the nature of the business, beyond just qualifying whether it may process cash, is critical to being able to determine if the cash deposits are proportionate.[15]

However, perhaps such incidents are limited rather than systemic as respondents in Corporate and Wholesale Banking do consider themselves to be effective at mitigating all of these cash-based typologies

- 60% of the Top 10 most frequent typologies for Corporate and Wholesale were in the Top 10 most effectively mitigated for this sector, which demonstrates that improvements to controls are required for the less effectively mitigated risks
- 35% of the typologies in Corporate and Wholesale are considered to be effectively mitigated on average, which is one of the highest ratios across all sectors. Perhaps the higher touch time with clients as a part of KYC processes in this sector makes it possible to mitigate the risk more effectively.

14 Business and Corporate Banking were not explicitly distinguished in the 2020 survey and so there is no prior sector specific data to compare this year's data to for these two sectors.

15 'Fowler Oldfield jury see CCTV footage of cash arriving', Telegraph & Argus, https://www.thetelegraphandargus.co.uk/news/20133036.watch-fowler-oldfield-jury-see-cctv-footage-cash-arriving/

Capital Markets

Typology
TP28 - Purchase and sale of securities
TP21 - Transfer of funds from a low crime/corruption environment to a high crime/corruption or low transparency environment
TP20 - Transfer of funds from a high crime/corruption environment to a low crime/corruption environment
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)
TP30 - Use of 'off the shelf' or shell companies
TP31 - Overpricing & under-pricing of securities
TP36 - Use of investment account to layer funds
TP23 - Mirror trading
TP29 - Purchase and sale of shell company shares
TP32 - Compensation trading
TP26 - Takeover of financial systems

- Respondents in the Capital Markets sector indicated that the majority of the typologies were observed very infrequently. Combined with a relatively limited number of respondents from this sector, it is difficult to draw many meaningful conclusions about their ranking. However, the *purchase and sales of securities* – for example, where retail investors purchase securities via a broker using illicit funds and then sell them shortly after – did feature as the most prevalent
- Arguably within this sector, opportunities for laundering money are more limited which explains why they are infrequently observed. However, it is clear that given the value of transactions involved, where incidents do occur, they can be very substantial. Mirror trades executed through Deutsche Bank were a good example of this, so it is interesting to note that this is the least well mitigated typology across all sectors.[16]

16 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings', FCA, https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure

Baringa

Money Services Businesses

Typology	Frequency ranking (2022)
TP20 - Transfer of funds from a high crime/corruption environment to a low crime/corruption environment	=1
TP21 - Transfer of funds from a low crime/corruption environment to a high crime/corruption or low transparency environment	=1
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	3
TP9 - Use of Money Services Businesses (MSBs)	4
TP2 - Structured cash deposits	=5
TP3 - Direct cash deposits into another individual or entity's account	=5
TP1 - Cash and quasi cash deposits (direct)	=7
TP24 - Use of high value assets to transfer value	=7
TP5 - Control of another person to deposit funds	9
TP4 - Use of 'mules' (complicit or non-complicit)	=10
TP26 - Takeover of financial systems	=10

- Given the prevalence of cross-border transactions undertaken by MSBs, it follows that the two most prevalent typologies involve the transfer of funds to different jurisdictions. The results show that organisations in this sector are less effective at mitigating these risks compared with respondents in other sectors. This is despite the increased regulatory scrutiny that MSBs have faced on account of the sector's susceptibility to money laundering, evidenced, for example, by HMRC fining of money transfer company MT Global Limited (January 2021) for breaches to Money Laundering Regulations.[17] Indeed, the UK government highlights the susceptibility of MSBs to money laundering through cross-border transactions in its supervisory guidance for organisations in this sector[18]; the results show that despite this, MSBs are not effectively mitigating the risks associated with cross-border transfers
- Interestingly, there are 3 cash-based typologies in the Top 10 for MSBs. This may seem surprising given that many MSBs do not accept cash. However, this reflects the breadth of business represented in this sector which for the purposes of this report include foreign exchange providers, high value dealers and fintech apps as well as online remitters
- Of all the Top 10 typologies for MSBs, *control of another person to deposit funds* and *use of high value assets to transfer value* are considered to be effectively mitigated on average. This may be reflective of better controls being put in place for ID&V and identifying the origin of goods. There is still greater opportunity for improvement for the other typologies
- It may seem anomalous that *use of MSBs* features within the Top 10 for the same sector. However, the question for this sector was whether they see nefarious customer behaviour which is typical of this sector – for example, many transactions between the same originator and beneficiary over a short period of time or between very specific geographical locations even where the customers differ.

17 'HMRC issues record £23.8m fine for money laundering breaches', HMRC, https://www.gov.uk/government/news/hmrc-issues-record-238m-fine-for-money-laundering-breaches

18 'Anti-money Laundering Supervision: Money Service Businesses', HMRC, https://www.gov.uk/government/publications/anti-money-laundering-guidance-for-money-service-businesses

Insurance

Typology	Frequency ranking (2022)
TP36 - Use of investment account to layer funds	1
TP26 - Takeover of financial systems	=2
TP35 - Overpayment of insurance premiums	=2
TP27 - Overpayment of credit products or investments	=4
TP33 - Cancellation of insurance policy	=4
TP28 - Purchase and sale of securities	6

- The variety of methods available for laundering money in the Insurance sector are relatively small compared with sectors such as Retail and Business Banking, with only eight typologies having been identified as relevant to the sector, including *use of mules* and *early redemption of life investment policy or annuity*, which were identified by our experience but not witnessed by any respondents and therefore have been excluded from the table above
- Most of the typologies in this sector were observed very infrequently, with only *use of investment account to layer funds* observed more often. This implies that it is quite unusual for this sector to be exploited for the purposes of laundering money and, where it is, it is typically at the layering stage to further distance the funds from their origin
- Typologies relating to the *overpayment of premiums, credit products or investments were considered*, on average, to be effectively mitigated. Organisations may find it easier to mitigate these typologies because overpayments will typically be accompanied by a direct request for a repayment of funds – and therefore a clear red flag for illicit activity, which with appropriate staff training can be more easily controlled than other typologies.

Asset and Wealth Management

Typology	Frequency ranking (2022)
TP28 - Purchase and sale of securities	1
TP26 - Takeover of financial systems	2
TP27 - Overpayment of credit products or investments	3
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	4
TP31 - Overpricing & under-pricing of securities	5
TP36 - Use of investment account to layer funds	6

- As with Insurance, the Asset and Wealth Management sector featured fewer number of typologies (seven, including *use of mules* that was identified by our experience but not witnessed by any of the respondents) compared with other sectors, highlighting that there are fewer products and services susceptible to money laundering in these sectors
- The *purchase and sale of securities* was rated one of the least effectively mitigated typologies for both sectors. Despite this, the red flags associated with this risk should be relatively easily monitored, for example patterns of trading activity common to customers across the same broker, or securities that are purchased and quickly sold or liquidated
- The most frequently observed typology in this sector – *purchase and sale of securities* – was considered to be, on average, effectively mitigated by respondents. This may be because there are controls in place which restrict the methods which can be used for depositing funds into investment accounts, which makes it more difficult to place illicit funds into these accounts, as well as where they can be withdrawn too
- It is somewhat surprising that *use of investment account* to layer funds is not more frequent. Our experience suggests this is one of the more common typologies in this sector and, indeed, where controls are less mature that investment accounts can be used in a similar way to 'shell' or 'funnel' accounts in banking
- *Overpayment of credit products or investments* were rarely witnessed. This may be because there are only certain types of products which can be 'overpaid' and in quite specific ways – e.g. ISAs and pensions, whilst standard investment accounts do not have such limits.

Trade Finance

Typology	Frequency ranking (2022)
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	1
TP20 - Transfer of funds from a high crime/corruption environment to a low crime/corruption environment	=2
TP21 - Transfer of funds from a low crime/corruption environment to a high crime/corruption or low transparency environment	=2
TP25 - Use of falsified or phantom trade shipments	4
TP24 - Use of high value assets to transfer value	5
TP26 - Takeover of financial systems	6

- As with Corporate and Wholesale, organisations in Trade Finance identified the *use of complex corporate structures to conceal Ultimate Beneficial Owner* as the most prevalent typology. The nature of some trade transactions, which often involve many different parties for the purchase, sale, financing and shipment, all of which may have complex structures, may make them particularly susceptible to this typology
- It is interesting to note that organisations witnessed money laundering through *falsified or phantom trade shipments* less frequently than other typologies, given its uniqueness to Trade Finance products/services. It may be that criminals do not favour this method of laundering money; alternatively, it may be more prevalent than the results indicate, suggesting organisations do not have the controls to detect this risk
- Controls do not appear to be deployed according to the most prevalent risks for this sector. Despite its relatively lower frequency, *use of high value assets to transfer value* was the most effectively mitigated typology by Trade Finance organisations.

Improving prevention

The results from this year's survey have allowed us to identify the most prevalent risks in more detail at a sector level, and therefore draw more detailed insights about the ways in which money is laundered through different organisations.

We have also been able to identify how some aspects of criminal behaviour have changed over time, by comparing the prevalence of typologies in 2022 with our previous report.

Overall, the results tell us that there is still a relatively weak correlation between the prevalence of a typology and how effectively organisations mitigate them, suggesting that resources do not appear to be allocated proportionately to risk.

We recommend financial institutions take the following steps to be better equipped at detecting and mitigating the risk of money laundering in their organisation;

- **Conducting more precise risk assessments to identify the risks that are specific to the organisation**, rather than applying generic controls. As we have seen from the variation between frequency of typologies across different sectors, risks are heavily dependent upon the unique features of the products and services offered by an organisation. Controls must be much more targeted if they are to effectively protect an organisation from money laundering risk
- **Ensuring that the typologies relevant to products and services offered by organisations are understood** so that appropriate detective controls can be implemented to identify risks and preventative controls are in place to mitigate them
- **Demonstrating that controls are robust enough to prevent the risk of money laundering**. Recent regulatory fines have been applied even in instances where money laundering has not occurred, rather regulators are penalizing organisations that have insufficient controls in place. For example, the FCA fined Ghana International Bank £5.8m (GBP) in 2022 for breaches of the MLRs in relation to its corresponding banking activities, specifically around insufficient controls in helping to mitigate the risk of correspondent banking services[19]. Whilst there is clearly more to be done to improve the effectiveness of organisations' controls, resources to do so are finite, and it is never going to be possible to prevent all money laundering risks. Therefore, organisations should take a risk-based approach to mitigating the typologies that are most prevalent or impactful
- **Tightening the controls around the use of cryptocurrency** by more consistently identifying customers transacting with crypto exchanges, particularly where the value of transactions is incommensurate with their profile and putting in place controls to identify where mixers or 'off chain' transactions have been exercised. Cryptocurrencies by nature have a transparent ledger and so it ought to be possible to trace the history of the funds. Mixers distort this by swapping small amounts of cryptocurrencies between different users to disguise their origin. 'Off chain' transactions involve the sharing of virtual wallet details to share value between users without a record. FIs should put in place controls to try and identify where such obfuscation techniques have been employed to reduce the risk of facilitating financial crime
- **Recognising that for larger, more complex clients, KYC is even more critical** – as is clear from the Fowler Oldfield[20] case, identifying whether or not a business is expected to deal is cash does not go far enough to understand whether or not the value of cash it is dealing in is appropriate for the nature of its business. For these types of clients, detailed review by trained financial crime professionals is the only effective way to identify, measure and manage the risk appropriately
- **Be aware that prevalent pre-pandemic typologies may re-emerge** – *cash deposits through third party channels* and *use of high value dealers* were significantly more prevalent at the beginning of 2020. Whilst the reliance on transactions through physical outlets and businesses may have reduced their prevalence during COVID-19, there is no reason these typologies will not re-emerge given their prevalence in the past. Therefore, it is important FIs keep controls up to date to mitigate these risks
- **Money laundering through gambling outlets has seemingly reduced whilst some significant high-profile cases have come to light** – accordingly, FIs should be mindful that this typology may still be active and must be managed appropriately.

19 FCA Decision notice, FCA, https://www.fca.org.uk/publication/decision-notices/ghana-international-bank-plc.pdf
20 'Fowler Oldfield jury see CCTV footage of cash arriving', Telegraph & Argus, https://www.thetelegraphandargus.co.uk/news/20133036.watch-fowler-oldfield-jury-see-cctv-footage-cash-arriving/

Appendices

Appendix A - Top 10 Typologies

Typology Money laundering typology	**Typology description** Explanation of the typology	**Red flags** Warning signs that may indicate that the typology is being carried out	**Examples** Example of the typology being carried out	**Rank** Risk rank
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	Corporate structures are set up using a variety of corporate vehicles and multiple layers of ownership, often across several jurisdictions, in order to obscure the ultimate controller and beneficiary of the corporation's activities.	• Corporate structures have a level of complexity that does not make sense for the nature business, for example, use of trusts, Scottish partnerships, holding companies • Involvement of low-tax or low transparency jurisdictions in the ownership structure • Activities carried out on the corporation's accounts do not reflect those of a legitimate business or are inconsistent with its nature of business • Transactions are made with foreign jurisdictions which have no apparent connection to the corporation	An Australian drug trafficking organisation set up a transport company and used it to deposit funds generated through cannabis sales. They then transferred funds to a legitimate wage processing company who paid salaries of approx. $100k (AUD) to the criminal members of the organisation. See 'Case study 2' in FATF report 'Concealment of Beneficial Ownership'. A recent Global Witness report, 'Getting the UK's House In Order' suggests: • 336,224 companies in the UK state that they have no beneficial owner • 6,711 are controlled by beneficial owners who control more than 100 companies, who are likely to be nominees • 487 have circular ownership structures, implying they control themselves	1
TP1 - Cash or quasi-cash deposits (direct)	Large amounts of cash are deposited into an account. Alternatively, quasi-cash instruments such as travellers' cheques are used to make deposits. In some countries, bearer shares and/or bills of exchange are still permitted which may also enable this typology.	• The majority, if not all, of the deposits made into the account are made in cash or quasi-cash • The total cash or quasi-cash deposits on the account are significantly higher than customers of a similar type, for example, retail customers with a similar income and occupation, or corporate customers with a similar revenue and industry • Deposits are of a 'round' amount, for example, £1k • There is a sudden and unexplained increase in cash or quasi-cash deposits	**Example 1:** A recent fine against Standard Chartered Bank from the FCA highlighted that an individual was able to open an account in the UAE with $3m (AED) in cash, which had been brought into the branch in a suitcase. See FCA Decision Notice. **Example 2:** HSBC were found to have cashed $290m (USD) of travellers' cheques over a four-year period on behalf of a Japanese bank. The cheques were received in large blocks and were sequentially numbered. These were cashed on behalf of Japanese clients of the bank, purporting to be in the used car business, but had originally been purchased by Russian nationals. See US Senate Report 'U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History'.	2

Typology Money laundering typology	**Typology description** Explanation of the typology	**Red flags** Warning signs that may indicate that the typology is being carried out	**Examples** Example of the typology being carried out	**Rank** Risk rank
TP3 - Direct cash deposits into another individual or entity's account	Cash is deposited into an individual or entity's account by a third party, who has not undergone identity and verification checks on the account, to obfuscate the identity of the depositor. Control of the account may have been unofficially granted to the third party by the named account holder or the account may have been set up using falsified documentation	• Individual depositing the funds is unwilling to provide an explanation for the source of funds • The funds are subsequently transferred to another account • A large number of smaller deposits are made on the account • Deposits are made a long distance from where the account was originally opened and/or the address registered on the account • Deposits are made from disparate locations	In the US, some banks restricted third party cash deposits on accounts following a FinCEN advisory notice about their misuse. For example, in 2013, 13 individuals based in California were prosecuted for illegally selling prescription drugs across the US, often delivered by mail. More than $3.5m (USD) in cash was deposited directly into their accounts by the purchasers of the drugs in branches all over the US. See US Department of the Treasury 'National Money Laundering Risk Assessment 2015'.	3
TP9 - Use of Money Services Businesses (MSBs)	MSBs, such as remittance providers, often have weaker identification and verification controls in place, which provides a greater level of anonymity and makes it easier to conceal the source and/or destination of funds. Customers may use these services as a means to place cash or cheques into the financial system, to pool funds abroad or to pay for illicit services. In some cases criminals may take control of an MSB, or an MSB owner may be complicit with criminal activity, allowing their services to be misused.	For customers utilising MSBs: • Frequent usage of MSBs with limited other activity on the account For accounts held by MSBs: • Structured transactions involving the same geographic areas, even if carried out by different customers • Multiple transactions between the same originator and beneficiary over a short period of time • Lack of ultimate originator and/or ultimate beneficiary information (and the jurisdictions in which they reside) on transactions processed through the MSB's account • MSB company turnover is in excess of comparable companies	**Example 1:** An FIU identified a series of unusual transactions made via a money remitter to South America. The transactions had been instructed by a number of different people through several branches of the remitter located within the same area of the country. Despite the majority of the individuals instructing the transactions having no prior criminal record, one was found to have a connection to a large drug trafficking organisation and it is likely that the beneficiaries of these transactions were involved in the same organisation. See 'Remittances to high-risk countries' case study in FATF report 'Money Laundering through Money Remittance and Currency Exchange Providers'. **Example 2:** A currency exchange company received deposits from criminals which were withdrawn as cash by mules for the purposes of paying illicit workers. SARs were filed by the banks that were used to deposit the illicit funds. The owner of the currency exchange company was later prosecuted and convicted. See Council of Europe report 'Use of Securities in money laundering schemes'.	4

Typology Money laundering typology	**Typology description** Explanation of the typology	**Red flags** Warning signs that may indicate that the typology is being carried out	**Examples** Example of the typology being carried out	**Rank** Risk rank
TP2 - Structured cash deposits	Cash is deposited into an account in a series of small transactions to attempt to evade detection	• The total cash deposits on the account are significantly higher than customers of a similar type, for example, retail customers with a similar income, or corporate customers with a similar revenue • Where a local 'deposit reporting threshold' is in place, deposits made are just below to this value • Value of transfers out of the account are significantly higher than the value of the individual deposits	The owner and sole director of a retail company made multiple cash deposits below the reporting threshold in Australia over a period of five years, totalling more than $2.5m (AUD). The proceeds were deposited into the company account before being transferred to the individual's personal account. See AUSTRAC article 'Offender convicted of structuring funds to launder money: $1m recovered'.	5
TP30 - Use of 'off the shelf' or shell companies	Criminals purchase an 'off the shelf' or shell company and deposit funds into the company bank account. The funds are later withdrawn as 'clean' funds, under the justification that they have been generated through legitimate business activity.	• Use of nominee directors • Funds are received or sent to a company account from an MSB account • Funds are withdrawn shortly after the account is set-up • Transaction counterparty is inconsistent with nature of the company, for example, industries are not aligned • A company bank account is set-up and quickly shut down following a deposit/ series of deposits	Israel's FIU received a SAR from a bank regarding an individual who held a student account with the bank. Despite being a student, the customer owned a private company which he used to purchase a controlling interest in a publicly traded shell company. He then proceeded to open a bank account under that company's name and shortly after, $2.5m (USD) was deposited into this account. See FATF report 'Money Laundering and Terrorist Financing in the Securities sector'.	6

Typology Money laundering typology	**Typology description** Explanation of the typology	**Red flags** Warning signs that may indicate that the typology is being carried out	**Examples** Example of the typology being carried out	**Rank** Risk rank
TP7 - Significant use of cryptocurrency or Non-Fungible Tokens	Cryptocurrencies are received as payment for criminal activity, taking advantage of its anonymity. Mixers may be utilised to further increase the anonymity. These illicit funds are then converted into fiat currency through a Virtual Currency Exchange (VCE). Similarly, Non-Fungible Tokens (NFTs) which act as digital ownership certificates, often purchased using cryptocurrency, are used as bearer negotiable instruments to enable illicit value to be transferred between two parties anonymously.	• Large or frequent deposits are made into the account from known VCEs • Transactions with VCEs make up the majority of the activity on the account • Deposits received from VCEs are often followed by cash withdrawals or electronic transfers of a similar value • Deposit values not commensurate with expected customer income and/or source of funds • NFT is purchased and then sold shortly after for a much higher value	**Example 1:** An organised crime group, operating in Europe, were originally laundering the proceeds of drug sales by structuring cash deposits into bank accounts and travelling to Colombia to withdraw the funds via credit cards linked to these accounts. They then switched tactics to convert their cash into cryptocurrencies instead so that it could be more easily transferred into Colombian bank accounts directly. See Europol article 'Illegal network used cryptocurrencies and credit cards to launder more than EUR 8m from drug trafficking'. **Example 2**: HMRC seized three NFTs after it was suspected that the owners were trying to conceal the proceeds of VAT fraud involving 250 suspected fake companies. Three people were arrested in connection with the case, accused of using different methods to hide their identities and defraud HMRC of £1.4m (GBP). See Guardian article 'HMRC seizes NFTs for the first time amid fraud inquiry'	7
TP15 - Appointment of nominees into key company positions	Individuals who do not control a company are appointed into key company position, for example, a 'director', to obscure the beneficial owner, who is actually responsible for the underlying activity of the company. These are also known as 'proxies' or 'white horses', in Czechia and Slovakia. Such individuals may be professional or non-professional facilitators. In the case of non-professional facilitators, they may or may not be aware that they are being appointed into these positions and sometimes they are coerced.	• Company appears to be registered at the address of a corporate service provider (CSP) or where there are many other companies registered • Company directors hold directorships in many of businesses	One CSP in New Zealand provided nominee directorship services for over 2,000 companies, 73 of which were involved in facilitating crime in foreign jurisdictions. The employee recruited to act as the nominee director had no prior involvement in the CSP services and so is unlikely to have been aware of the criminal activities being carried out. See FATF report 'Concealment of Beneficial Ownership'.	8

Typology Money laundering typology	**Typology description** Explanation of the typology	**Red flags** Warning signs that may indicate that the typology is being carried out	**Examples** Example of the typology being carried out	**Rank** Risk rank
TP20 - Transfer of funds from a high crime/ corruption environment to a low crime/corruption environment	Funds are generated in a high crime/corruption environment and transferred to a low crime/ corruption environment where they are used to purchase high value assets, for example, property, cars.	• Involvement of politically exposed persons on the account • Large cash withdrawals • Purchase of high value goods, for example, jewellery	The Vice President of Equatorial Guinea, who has been accused of corruption and embezzlement, transferred large amounts of money to Europe and the US in order to purchase high value property and cars. In 2018, he travelled on a government plane to Sao Paulo and was found to have ~$1.5m (USD) cash and ~$15m (USD) in luxury watches which were confiscated from him by the Brazilian authorities. See BBC article 'Teodorin Obiang: '$16m seized' from E Guinea leader's son'.	9
TP21 - Transfer of funds from a low crime/ corruption environment to a high crime/corruption or low transparency environment	Funds are transferred from a comparatively low crime/ corruption environment to a high crime/corruption or low transparency environment to distance them from their origin and the crime, and to enable them to be utilised more easily. This includes repatriating funds from the sale of illicit goods.	• Customer has no apparent personal connections or business interest in the jurisdictions transacted with • Funds are deposited to the account and then shortly afterwards a similar value is transferred abroad • Typical personal or business transactions are not present on the account • Jurisdiction is considered to be a tax haven	A criminal organisation involved in the production and distribution of marijuana in Costa del Sol and the export of cocaine from South America to Europe, laundered the proceeds from Europe to Argentina, where it was invested into the property market. See Europol article 'International Drug Trafficking Between South America and Europe Disrupted By Police: 48 Arrested'.	10

Appendix B - References

Typology	Reference
TP16 - Use of complex corporate structures to conceal Ultimate Beneficial Owner (UBO)	**1.** 'Concealment of Beneficial Ownership', FATF, https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf **2.** 'Getting the UK's House In Order', Global Witness, https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/getting-ukshouse-order/
TP1 - Cash or quasi-cash deposits (direct)	**1.** 'Decision Note: Standard Chartered Bank', FCA, https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls **2.** 'U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History', US Senate, https://www.hsgac.senate.gov/imo/media/doc/PSI%20REPORT-HSBC%20CASE%20HISTORY%20(9.6).pdf
TP3 - Direct cash deposits into another individual or entity's account	**1.** 'Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML', FinCEN, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a005 **2.** 'National Money Laundering Risk Assessment 2015', US Department of the Treasury, https://home.treasury.gov/system/files/246/National-Money-Laundering-Risk-Assessment-06-12-2015.pdf **3.** US Immigrations and Customs Office, Cornerstone Report, Vol 11: No. 1, https://www.ice.gov/sites/default/files/documents/Report/2015/cornerstone11-1.pdf
TP9 - Use of Money Services Businesses (MSBs)	**1.** 'Money service business guidance for money laundering supervision', HM Revenue & Customs, https://www.gov.uk/government/publications/anti-money-laundering-guidance-for-money-service-businesses **2.** 'Money Service Businesses', JMLSG, https://www.jmlsg.org.uk/guidance/previous-guidance/ **3.** 'Money Laundering through Money Remittance and Currency Exchange Providers', FATF, https://www.fatf-gafi.org/fr/publications/methodesettendances/documents/moneylaunderingthroughmoneyremittanceandcurrencyexchangeproviders.html?hf=10&b=0&s=desc(fatf_releasedate) **4.** 'Money Service Businesses in the UK: Improving the Conditions for Effective Financial Crime Supervision and Investigations', Royal United Services Institute (RUSI), https://rusi.org/explore-our-research/publications/occasional-papers/money-service-businesses-uk-improving-conditions-effective-financial-crime-supervision-and
TP2 - Structured cash deposits	**1.** 'Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering', Europol, https://www.europol.europa.eu/publications-events/publications/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering **2.** 'Offender convicted of structuring funds to launder money: $1 million recovered', AUSTRAC, https://ngm.com.au/money-laundering-lawyers/money-laundering-austrac/

Typology	Reference
TP30 - Use of ‘off the shelf’ or shell companies	**1.** ‘Money Laundering and Terrorist Financing in the Securities Sector, FATF, https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf
TP7 - Significant use of cryptocurrency or Non-Fungible Tokens	**1.** ‘Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking’, Europol, https://www.europol.europa.eu/media-press/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking **2.** ‘Two criminal groups dismantled for laundering EUR 25 through smurfing and cryptocurrencies’, Europol, https://www.europol.europa.eu/media-press/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies **3.** ‘HMRC seizes NFTs for first time amid fraud inquiry’, The Guardian, https://www.theguardian.com/technology/2022/feb/14/hmrc-seizes-nfts-for-first-time-amid-fraud-inquiry
TP15 - Appointment of nominees into key company positions	**1.** ‘Concealment of Beneficial Ownership’, FATF, https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf **2.** ‘Death in Vienna’, OCCRP, https://www.occrp.org/en/troikalaundromat/death-in-vienna **3.** The term ‘white horse’ is explained in the following article: ‘Panama Papers: The Czech Republic’, OCCRP, https://www.occrp.org/en/panamapapers/the-czech-republic/
TP20 - Transfer of funds from a high crime/corruption environment to a low crime/corruption environment	**1.** ‘Teodorin Obiang: ‘$16m seized’ from E Guinea leader’s son’, BBC News, https://www.bbc.co.uk/news/world-africa-45546655
TP21 - Transfer of funds from a low crime/corruption environment to a high crime/corruption or low transparency environment	**1.** ‘International Drug Trafficking Between South America and Europe Disrupted By Police: 48 Arrested’, Europol, https://www.europol.europa.eu/media-press/newsroom/news/international-drug-trafficking-between-south-america-and-europe-disrupted-police-48-arrested **2.** ‘EU Drug Markets Report’, Europol, https://www.europol.europa.eu/publications-documents/eu-drug-markets-report-2016

We set out to build the world's most trusted consulting firm – creating lasting impact for clients and pioneering a positive, people-first way of working. We work with everyone from FTSE 100 names to bright new start-ups, in every sector. We have hubs in Europe, the US, Asia and Australia, and we can work all around the world – from a wind farm in Wyoming to a boardroom in Berlin.

Find us wherever there's a challenge to be tackled and an impact to be made.

We'd love to hear from you enquiries@baringa.com
Or visit baringa.com

For further information, please contact:

Cat Morris
Partner, Financial Crime
cat.morris@baringa.com

Christopher Nott
Partner, Finance, Risk and Compliance
christopher.nott@baringa.com

Richard Elliot-Cooke
Director, Financial Crime
richard.elliot-cooke@baringa.com

Olivia Goldberg
Senior Manager, Financial Crime
olivia.goldberg@baringa.com