WHITE PAPER

Financial Crime Risks in Investment Management

May 2021

INSIGHT | INTELLIGENCE | INNOVATION

fiserv.

THEMIS

Financial crime risks in investment management

Introduction

Investment management is an industry in constant expansion, with PwC recently estimating an increase in total global assets under management from US$110 trillion in 2020 to US$145 trillion in 2025.[1] The industry is commonly split into two main strands - asset management and wealth management - the former defined by the United Kingdom's Joint Money Laundering Steering Group (JMLSG) as those activities that include "both discretionary and advisory management of segregated portfolios of assets (such as securities, derivatives, cash, property etc.) for the firm's customers"[2] and the latter as "the provision of investment services including advice, discretionary fund management and brokerage to private investors, ranging from the mass affluent to high and ultra-high net worth individuals"[3].

Because of this significant growth in assets under management, both financial crime risks and regulatory scrutiny are set to increase in the industry, even though it has not conventionally been used to transfer assets or value, and has therefore been exposed to lower inherent risks in comparison to other sectors. However, as criminals seek out new ways to exploit the financial system, they have found additional vulnerabilities in wealth and asset management, notably when clients have multiple accounts across different jurisdictions or when there is low visibility of beneficial owners of assets traded. As a result, it is more important than ever before for wealth and asset managers to fine-tune their financial crime risk management controls and develop a strong understanding of the inherent risks they face, as well as the emerging financial crime threats they may potentially be exposed to.

This paper seeks to examine financial crime risks in investment management, understand current regulatory frameworks and rules pertaining to the industry, and assess the challenges that investment managers face in terms of financial crime compliance. The analysis draws upon desktop research and relevant findings circulated among Themis and Fiserv contacts who operate in investment management. It focuses on the current financial crimes threatening firms in the sector, and on the challenges and opportunities associated with implementing the right steps required to mitigate threat exposure.

What financial crime risks are wealth and asset management firms exposed to?

Even though they operate in sectors of the financial industry that are exposed to a relatively lower risk of financial crime, asset managers and wealth managers must still be aware of and alert to diverse threats. According to a recent survey circulated by Themis and Fiserv among professionals working in compliance/financial crime functions in asset and wealth management, money laundering, fraud and cybercrime were cited as the top three financial crime threats to which the investment management industry is particularly exposed. As Figure 1 shows, respondents also

---

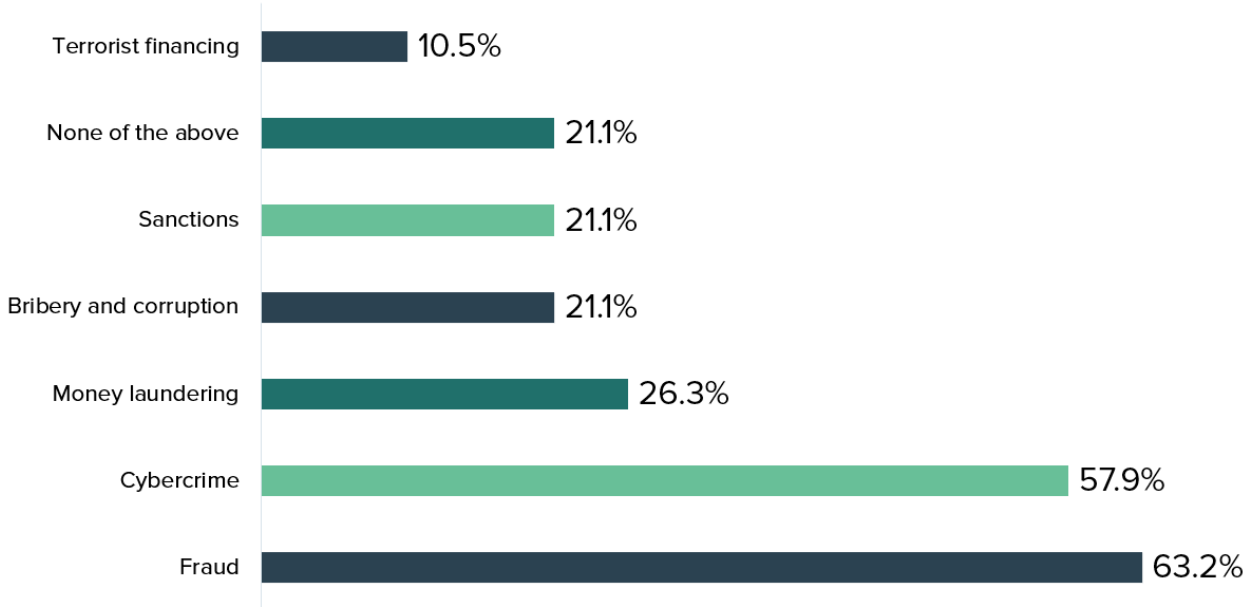
[1] PwC, "Global Assets under Management set to rise to $145.4 trillion by 2025" Available at: https://www.pwc.com/ng/en/press-room/global-assets-under-management-set-to-rise.html

[2] Joint Money Laundering Steering Group, "Prevention of money laundering/combating terrorist financing - 2020 REVISED VERSION", June 2020 (amended July 2020), Available at: https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf

[3] *idem.*

highlighted that, over the previous 12 months, their firms had been directly exposed mainly to fraud (63.2%) and cybercrime (57.9%), two offences that often go hand in hand.

Figure 1: Has your organisation been exposed to any of the following financial crime threats over the past 12 months?



Additionally, 80.0% of respondents agreed that financial crime risks had increased as a result of the COVID-19 pandemic and associated circumstances. An increase in investment-related fraud in connection with the pandemic has also been reported by the Investment Association, which highlighted an upsurge in attempted fraud such as email phishing targeting investment management firms following the onset of the pandemic.[4] Common frauds see criminals using genuine investment companies' names and registration numbers, but their own contact information, to receive funds from unsuspecting clients, or bogus investments that are set up to look like legitimate companies.

Meanwhile, even though instances of money laundering in the investment management sector are typically fairly rare,[5] money laundering risks will increase when managers work with certain types of customers, such as offshore trusts or companies, politically exposed people (PEPs) or customers originating from/engaged in activities in higher-risk or sanctioned jurisdictions. For

[4] Andrew, T., "Investment managers see spike in Covid-19 related scam activity", Wealth Manager, 29 April 2020, Available at: https://citywire.co.uk/wealth-manager/news/investment-managers-see-spike-in-covid-19-related-scam-activity/a1351388

[5] Business Control Solutions, "Shifting sands: Financial Crime Risk Management for Wealth and Asset Managers", 2020, Available at: http://www.bcsconsulting.com/wp-content/uploads/2020/06/BCS_Snapshot_Shifting-sands-Financial-Crime-Risk-Management-for-Wealth-and-Asset-Managers.pdf

instance, according to the Wolfsberg Group[6], politically exposed people and high-net-worth customers represent a particular risk to wealth management firms, which can therefore be more exposed to bribery and corruption than asset managers. Indeed, the typical wealth manager deals with low volumes of high-value customers for which there should be a take-on process that involves a high level of understanding of the customer's needs and priorities, but also circumstances and source of funds.

The Wolfsberg Group and the Financial Action Task Force (FATF) note that geography and jurisdictional risks also require particular attention from asset and wealth managers. These risks are related to jurisdictions which continue to foster secrecy, corruption, and money laundering due to their attractive tax regimes, hidden beneficial ownership structures, lack of supervision or political instability. Sanctions risks also represent a strong liability for asset and wealth managers especially since sanctioned entities and individuals often gain access to the international financial system through third-party intermediaries.

Third party relationships have also been linked to financial crime in the asset and wealth management sphere. For instance, in the Financial Conduct Authority (FCA)'s most recent thematic review of anti-money laundering and anti-bribery and corruption systems and controls in asset management, the UK regulator found that "most firms failed to demonstrate adequate systems and controls for assessing bribery and corruption risks in relation to dealing with and monitoring third party relationships, such as relationships with agents or introducers."[7]

Finally, cyberattacks against investment managers are on the rise, especially in light of the cybervulnerabilities associated with remote working conditions during the COVID-19 pandemic. New research from Digital Shadows highlighted that cybercriminals are increasingly setting their sights on asset and wealth management firms. One reason for this shift in focus by cybercriminals is the fact that "traditional financial institutions – primarily banks – are investing more heavily in mitigation in the wake of repeated cases of fraud, extortion, and theft at the hands of cybercriminals" - something which is not currently done by many investment managers.[8]

What inherent risk factors do the wealth and asset management sectors face?

Respondents to the Themis-Fiserv survey argued that client and geography risks are the main factors that make investment management vulnerable to financial crime. In particular, wealthy and powerful clients, including politically exposed persons (PEPs) and relatives or close associates (RCAs), represented the biggest risk for 55.0% of respondents, followed by clients who operate

[6] Wolfsberg Group, "Wolfsberg Group - Frequently Asked Questions (FAQs) - Source of Wealth and Source of Funds (Private Banking/Wealth Management)" Available at: https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20SoW%20and%20SoF%20FAQs%20August%202020%20%28FFP%29_1.pdf

[7] Financial Conduct Authority, "Anti-Money Laundering and Anti-Bribery and Corruption Systems and Controls: Asset Management and Platform Firms", October 2013, Available at: https://www.fca.org.uk/publication/thematic-reviews/tr13-09.pdf

[8] Security, "Asset management and wealth security threats in 2021", 21 January 2021, Available at: https://www.securitymagazine.com/articles/94399-asset-management-and-wealth-security-threats-in-2021

through offshore trusts and/or companies with complex business structure (50.0%) and those who operate in high-risk jurisdictions (50.0%).

These perceptions of inherent risk correspond with the Financial Conduct Authority's research about the main factors that increase the risk of money laundering, bribery, and corruption in investment management, which the UK watchdog reports to be the following:[9]

- Non face-to-face business, which can attract money launderers with stolen or fabricated identities;
- Customers with links to high-risk countries or sanctioned individuals;
- Wealthy and powerful clients, including politically exposed persons (PEPs);
- Offshore trusts, shell companies and complex ownership structures that conceal and distance beneficial owners from their funds;
- High value and or unexpected transactions;
- Payments to third parties without a clear business rationale, which could disguise the source or destination of laundered funds;
- Lack of resilient end-to-end digital systems, with vulnerabilities in this respect particularly highlighted during the COVID-19 pandemic.

Additional risks linked to the investment management industry include the culture of confidentiality that clients often expect from their wealth/asset managers, which can, however, translate into an unwarranted tolerance of secrecy that suits those with criminal intentions. Furthermore, although it helps investment managers understand their clients and their clients' transaction activity, the closeness of many investment manager-client relationships also sometimes means that investment managers let additional formal due diligence slip and certain new risks go unnoticed.

This vulnerability is particularly underlined by the Financial Action Task Force in connection with wealth management, a sector that, according to the international watchdog, "typically involves the provision of financial services in a managed relationship with clients who are often of high net worth", where it can be difficult to identify beneficial owners and where there is increased likelihood of concealment of funds or use of offshore trusts, and banking secrecy.[10]

What is the position of regulators?

Given the sector's growing inherent risks and recent scandals such as the Panama Papers, legislators, policy makers and regulators are increasing their oversight across the investment management industry internationally. The investment management community appears to be divided about whether regulators are communicating their expectations with regards to financial crime compliance clearly. As a matter of fact, a small majority (52.6%) of Themis-Fiserv survey respondents said that they were, indeed, communicating clearly, while the rest (47.3%) believed more regulatory guidance is needed.

[9] *FCA Thematic Review 2013.*
[10] Financial Action Task Force, "GUIDANCE FOR A RISK-BASED APPROACH - THE BANKING SECTOR", October 2014, Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

At the European Union (EU) level, the EU's recent 5th Anti-Money Laundering Directive (AMLD5) closed loopholes in member states that had lower requirements for enhanced due diligence (EDD) for high-risk customers, by setting clearer and more harmonised standards regarding due diligence. As a result, firms across the financial sector, including asset managers, must now consider additional high-risk factors when assessing the need for EDD. As per EU requirements, asset managers are also expected to update records relating to the beneficial ownership of corporate clients, record any difficulties in identifying beneficial ownership, and understand the control structure of their corporate customers.

Individual EU members have also made specific provisions that directly affect investment management. For instance, after Luxembourg's 2018 National Risk Assessment identified a high level of risk of money laundering and terrorist financing in the investment fund sector, the Commission de Surveillance du Secteur Financier (CSSF), the country's financial regulator, underlined that all Luxembourg funds and managers are now subject to AML/CFT supervision.[11]

Similarly, in the Netherlands, regulators have taken action to ensure stronger investigation, monitoring, and reporting of suspicious activity. Notably, in April 2020, the Dutch Authority for the Financial Markets (AFM) announced that it would conduct further investigation into monitoring and reporting of unusual transactions by investment institutions, which were as a result required to draw up transaction profiles for their clients, apply detection rules to identify suspicious transactions, and conduct timely and properly reporting to the Financial Investigative Unit by the end of 2020.[12]

Another example is that of the Central Bank of Ireland, which in September 2019 published the final version of its Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) Guidelines for the Financial Sector ("The Guidelines"), which require fund and asset management firms to follow an upfront and ongoing model of customer due diligence prior to any subscription for shares/units in Irish investment funds.

Now outside the European Union, the United Kingdom applies its own standards and regulations. Asset and wealth managers are subject to the Money Laundering Regulations 2017, which impose specific and stringent customer due diligence (CDD), EDD, transaction monitoring, and reporting obligations on these sectors. The JMLSG also provides detailed, specific and up-to-date sectoral guidance on the steps that asset and wealth managers must take to comply with these AML/CFT regulations.[13] The guidance document includes, for instance, a chapter devoted to risk assessment regarding the origin of the initial and ongoing source(s) of wealth and funds, particularly within a wealth management relationship, and a separate specific chapter on wealth management.

[11] Commission de Surveillance du Secteur Financier, 04 May 2020, Available at: https://www.cssf.lu/en/investment-fund-manager/

[12] De Koning, N., "AFM calls on investment funds and investment firms to improve transaction monitoring", Regulation Tomorrow, 20 April 2020, Available at: https://www.regulationtomorrow.com/the-netherlands/afm-calls-on-investment-funds-and-investment-firms-to-improve-transaction-monitoring/

[13] JMLSG, "Prevention of money laundering/combating terrorist financing".

The UK regulator, the Financial Conduct Authority (FCA), has also increased its emphasis on operational resilience in its Asset Management Supervision Strategy.[14] Recognising that asset managers are heavily reliant on robust and reliable technology, the regulator expects firms to manage technology and cyber risks appropriately, including through appropriate oversight of third party firms and intra-group service providers. Meanwhile, the Senior Managers and Certification Regime (SM&CR), which has been in force since March 2016 and applies to banks, building societies, credit unions and PRA-designated investment firms (Relevant Authorised Persons), has increased personal liability for Senior Managers who are now held responsible for any actions that can cause harm to their businesses, notably for instances of financial crime.

Finally, in the United States, an investment adviser may be subject to AML compliance requirements if it falls under another category of financial institution, such as a broker-dealer, but the investment adviser function alone is not currently subject to any federal AML compliance requirements. In 2015, an attempt to provide a set of AML requirements for the industry was made by the U.S. Treasury Department's FinCEN. Under the proposed rules, advisers that are registered with the Securities and Exchange Commission (SEC) must establish AML programmes and report suspicious activities related to money laundering and terrorist financing. So far, the requirements have not been approved. However, investment managers were included in the recent U.S. Corporate Transparency Act, which introduced new reporting requirements to FinCEN as of early 2021. Even so, mutual funds and private investment funds are still exempt from reporting ultimate beneficial ownership.

How can financial crime risks be mitigated in the industry?

A number of measures can be taken in order to mitigate the financial crime risks that asset and wealth management firms are exposed to. First, screening of public source information is essential in order to detect any adverse media that concerns prospective or current customers. Screening must be ongoing, and must be conducted alongside monitoring of transaction inflows and outflows.

If the initial customer screening raises suspicions, or if they are a high-net-worth individual or a politically exposed person, then performing enhanced due diligence on the client and any beneficial owners represents the best option for wealth and asset managers to ensure they are not unwittingly exposing themselves to financial crime. In situations of even higher risk, such as when alerts about potential connections with sanctioned countries or individuals are flagged, then firms should also perform enhanced due diligence.

Another important step is the implementation of automated financial crime risk management solutions to ensure that comprehensive and thorough checks can be carried out. In particular, firms should consider replacing internally developed bespoke systems, which may not be adequately scalable in light of the significant increase in transaction activity over recent years. Automated solutions have a greater capability to detect suspicious activity and transactions, such as excessive transfer, purchase or sale of funds, or flows that are not in line with the client's profile.

[14] Financial Conduct Authority, "Asset Management Portfolio Letter", 20 January 2020, Available at: https://www.fca.org.uk/publication/correspondence/asset-management-portfolio-letter.pdf

Finally, in order to counter the potentially damaging effects of the culture of confidentiality that permeates the industry, asset and wealth management firms should promote regular contact between the client manager and the client, creating a relationship based on trust but also on the ongoing monitoring of relevant activities and transactions.

Challenges associated with financial crime compliance in investment management

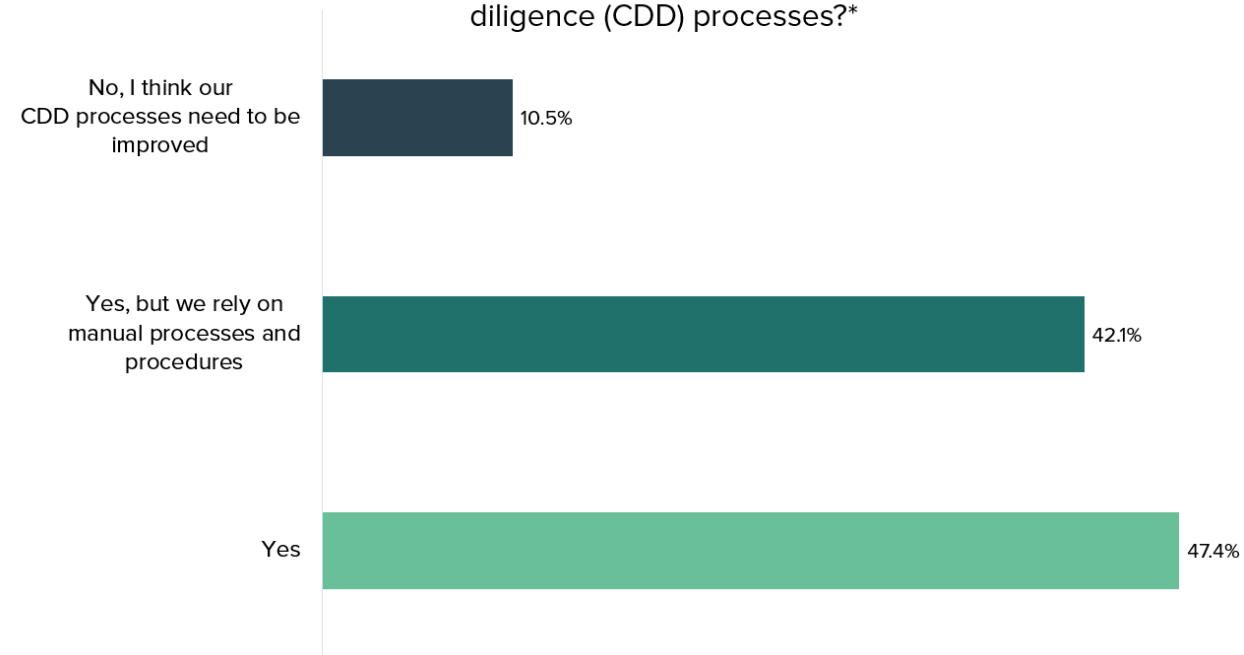
Due to the traditional consideration of wealth and asset management as "low risk" in terms of money laundering, firms may not deem it a top priority to have highly developed anti-money laundering (AML) systems in place. As a matter of fact, over the past decade, relatively few asset and wealth management firms have been subject to the attention of regulators on financial crime grounds.

The aforementioned 2013 FCA review found that money laundering risk assessments in the sector were sometimes not undertaken, not documented, lacked appropriate consideration of risks, were limited to one element of risk or were not used to inform control implementation. The FCA also found that risk assessments were conducted too infrequently in most firms. Indeed, approximately 40% of practitioners who responded to the Themis-Fiserv survey said that investment managers have an inadequate understanding of financial crime risks, and that this exposes the whole industry to financial crime. Additionally, a similar percentage of respondents argued that immature financial crime risk management frameworks across the investment management industry represent a hindrance to effective financial crime governance.

However, as highlighted in Figure 2, about 47% of survey respondents also reported that their investment firms have robust customer due diligence (CDD) processes that are able to identify financial crime risks at the onboarding stage and on a periodic basis during the business relationship. A further 42.1%, replied that, even though their CDD processes are strong, they still rely heavily on manual processes and procedures, which may be less effective at spotting red

flags.

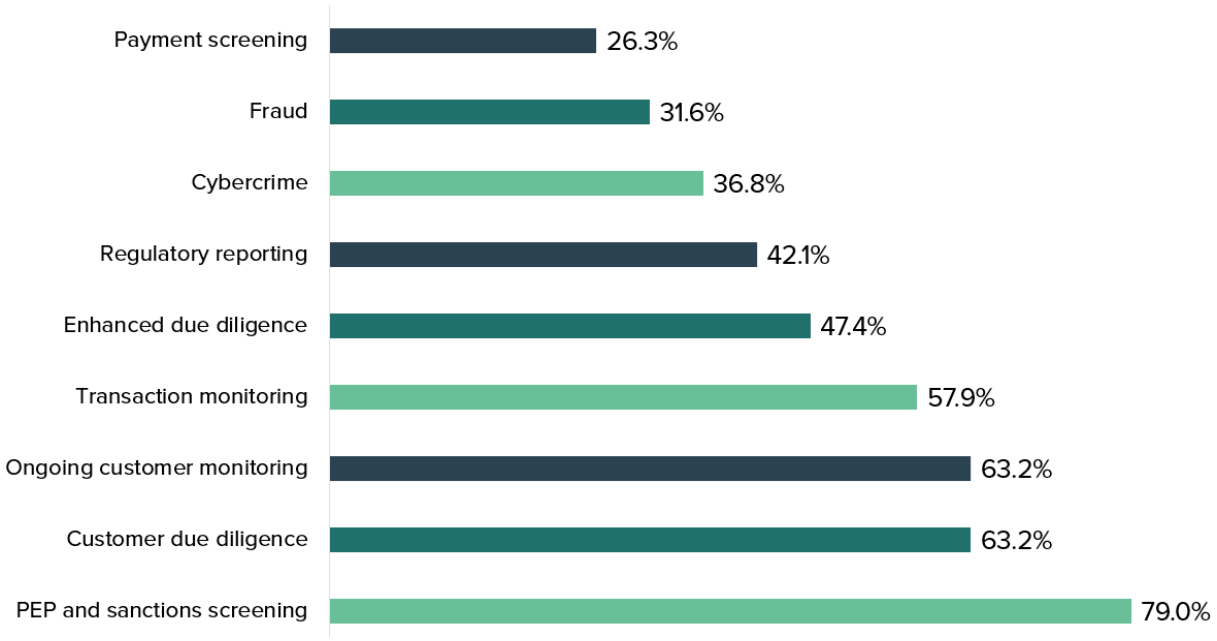
Figure 2: In your view, does your organisation have robust customer due diligence (CDD) processes?*



*That are able to identify financial crime risks at the onboarding stage and on a periodic basis during the business relationship?

It is, therefore, clear that lack of automation is still a particular challenge in the investment management industry. Figure 3 shows that this concerns around half of the Themis-Fiserv survey respondents, as only 52.6% said they have automated mechanisms in place to detect and disrupt different forms of financial crime, while another 47.3% reported that, although they have AFC frameworks in place, these are mostly manual. Amongst those who rely on automation, most do so for PEP and sanctions screening (79.0%), followed by customer due diligence and ongoing customer monitoring (63.2%).

Figure 3: If you use automated financial crime risk management solutions, which of the following areas do these cover?



Consequences of getting it wrong

Inadequate implementation of appropriate anti-financial crime measures leaves the sector exposed to potential penalties from regulators, customer loss, reputational damage and personal liability of senior management. As summarised in Figure 4, according to Themis-Fiserv survey respondents, the most worrying consequence of inadequate regulatory compliance is the increased risk of financial crime, followed by regulatory fines and reputational costs. For instance, in March 2021, the Latvian Financial and Capital Market Commission (FCMC) imposed a fine on ABLV Asset Management for breaches of anti-money laundering and counter-terrorism financing laws, and requested the firm to implement further measures to tighten its internal control systems.[15]

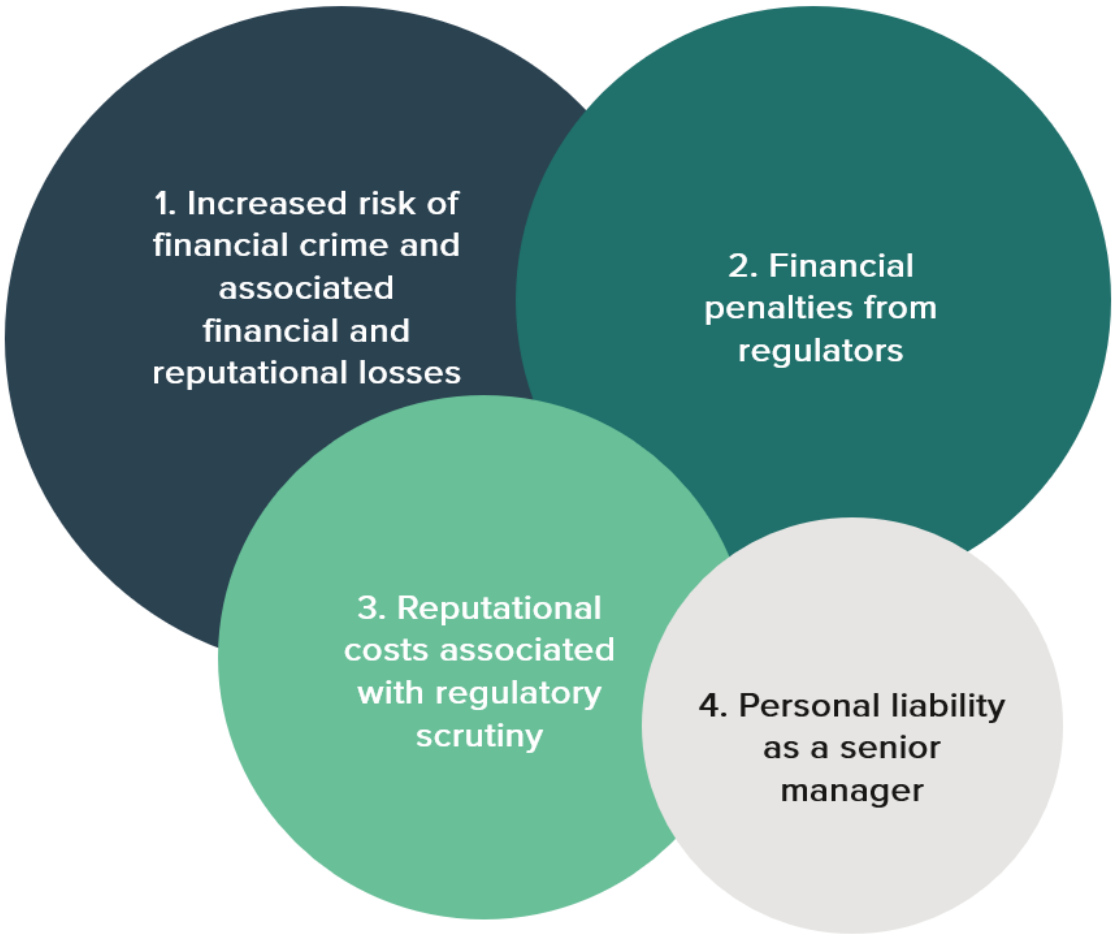
Similarly, a lack of appropriate cybersecurity measures rendered the Australian hedge fund Levitas vulnerable to a sophisticated phishing scam, which involved attackers using an executive's email account to initiate and approve cash transfer requests amounting to AU$8 million by sending fake invoices to the fund's trustee and third party administrator. Aside from the financial loss, the fund suffered from the loss of its key investor, which redeemed its assets in the aftermath of the hack, forcing Levitas to close.[16]

[15] KYC360, "FCMC fines ABLV Asset Management for breaches of AML/CTPF laws", 19 March 2021, Available at: https://www.riskscreen.com/kyc360/news/fcmc-fines-ablv-asset-management-with-eur-57217-for-breaches-of-aml-ctpf-laws/

[16] CastleHallDiligence, "Cyber Attack: A Fake Zoom Link Kills a Hedge Fund", Available at: https://www.castlehalldiligence.com/blog/cyber-attack-a-fake-zoom-link-kills-a-hedge-fund

Surprisingly, despite the development of increasingly stringent senior management accountability regimes, personal liability of senior managers ranked last in terms of priority by the majority of Themis-Fiserv survey respondents (63.1%). However, recent examples of legal and reputational consequences directly affecting senior managers highlight the consequences that they can face, even if not directly personally implicated, if appropriate anti-financial crime frameworks are not implemented. For instance, in January 2021, two former chief executives of the private bank Julius Baer were formally reprimanded by the Swiss regulator, Finma, for their serious shortcomings in compliance measures related to the handling of dirty money from Venezuela's state-owned company Petroleos de Venezuela, resulting in extensive reputational damage for both the individuals and their organisation.

Figure 4: What do you see as the main risks associated with inadequate regulatory compliance? (Ranked in order of importance 1 to 4)



Conclusion

After a long period relatively far from both the regulatory and criminal spotlight, asset and wealth management firms are of growing interest to criminals, who are exploiting lucrative new avenues, and regulators, who are working hard to find innovative ways to stop them. However, years of

basic or lax anti-financial crime controls mean that additional effort and investment is required if firms are to keep up with regulators' expectations and be resilient to financial crime.

The Themis-Fiserv survey highlighted how, despite an overall confidence in CDD processes, investment management firms were relatively exposed to financial crime risks due to a lack of adequate understanding among senior managers and the prevalence of immature risk management frameworks.

As a result, asset and wealth management firms must ensure that they have taken all the appropriate steps to mitigate the risks to which they could be exposed. In particular, appropriate know-your-customer processes prior to entering into a business relationship, ongoing screening and transaction monitoring, and enhanced due diligence when dealing with high-risk customers, are all crucial measures that form the basis of any effective anti-financial crime framework. Failure to implement these leads not only to customer and stakeholder loss, but also to reputational damage, personal liability and hefty fines from regulators.

Authors

Maria Nizzero
Associate Director of Analysis
Think Tank
Themis
maria.nizzero@themisservices.co.uk

Andrew Davies
Vice President, Global Market Strategy
Financial Crime Risk Management
Fiserv
andrew.davies@fiserv.com