Financial Stability Institute | BIS

FSI Briefs

No 7

Financial crime in times of Covid-19 – AML and cyber resilience measures

Juan Carlos Crisanto and Jermy Prenio

May 2020

FSI Briefs are written by staff members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), sometimes in cooperation with other experts. They are short notes on regulatory and supervisory subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS or the Basel-based standard-setting bodies.

Authorised by the Chairman of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2708-1117 (online)
ISBN 978-92-9259-384-1 (online)

Financial crime in times of Covid-19 – AML and cyber resilience measures[1]

Highlights

- *Criminals are exploiting vulnerabilities opened up by the Covid-19 lockdown, increasing the risks of cyber attacks, money laundering (ML) and terrorist financing (TF).*
- *Authorities worldwide have responded by drawing financial institutions' attention to these threats and by providing guidance on ways to improve cyber security and mitigate ML and TF risks.*
- *Financial authorities are warning financial institutions to be particularly watchful in relation to their IT networks and non-public data; third-party risk; and cyber security incident response plans; and to focus additional effort on staff training and awareness.*
- *Financial authorities also emphasise the need for financial institutions to be vigilant of new ML and TF risks and to continue meeting anti-money laundering (AML) and combating the financing of terrorism (CFT) requirements, while using the flexibility built into the AML/CFT risk-based framework, digital customer on-boarding and simplified due diligence processes.*
- *In both areas, the official guidance underscores the trade-offs between expecting financial institutions to enhance or adjust their cyber resilience and AML frameworks and, on the other hand, avoiding imposing an excessive burden that could hinder financial institutions in delivering key financial services.*

1. Introduction

A third of the world's population is in coronavirus lockdown.[2] An estimated 300 million office workers globally may be working from home,[3] including up to 90% of banking and insurance workers.[4] Most of these staff log into their firms' sites remotely, attending meetings using teleworking arrangements, and/or accessing non-public data online – sometimes via home computers and private devices. Since the customers of most financial institutions are also staying at home, doing financial transactions online has become not just a convenience but a necessity.

The lockdown increases the scope for criminals to exploit vulnerabilities and commit financial crime.[5] The increased online presence of virtually everyone has led to new, and in some cases more naïve, targets for online fraudsters. Work-from-home arrangements with remote access to corporate networks have significantly expanded the attack surface for cyber criminals. Money launderers can also take

[1] Juan Carlos Crisanto (juan-carlos.crisanto@bis.org) and Jermy Prenio (jermy.prenio@bis.org), Bank for International Settlements. The authors are grateful to David Whyte and Ruth Walters for helpful comments and insights and to Christina Paavola for administrative support.

[2] Further details available on the Business Insider website, www.businessinsider.com/countries-on-lockdown-coronavirus-italy-2020-3?r=DE&IR=T.

[3] Further details available on the Boston Consulting Group website, www.bcg.com/en-ch/publications/2020/covid-remote-work-cyber-security.aspx.

[4] See eg report in Risk.net, www.risk.net/comment/7511026/coronavirus-is-testing-op-risk-managers-to-the-limit.

[5] See eg post in Refinitiv by James Mirfin on the perfect storm: Covid-19 risk shaping digital transformation, www.refinitiv.com/perspectives/authors/james-mirfin-2/.

advantage of the increased need for financial institutions to identify and onboard their customers online. In normal times, cyber attacks and AML violations expose financial institutions to significant operational and reputational risks. In exceptional circumstances like the current one, those risks could be further exacerbated.

This note outlines official responses to the increasing levels of financial crime during the global lockdown. Section 2 highlights the financial crime seen so far during the current crisis. Section 3 summarises official approaches to strengthening financial institutions' cyber resilience. Section 4 describes the main AML measures taken by selected authorities worldwide. Section 5 concludes.

2. Financial crime during the pandemic crisis

Threats have evolved as a result of the coronavirus crisis. The International Criminal Police Organization (Interpol) recently issued a global threat assessment on crime and policing to its 194 member countries.[6] This highlighted a marked increase of cyber threats connected with malicious domains, malware and ransomware. For its part, the Financial Action Task Force (FATF (2020b)) points to an increase in ML and TF risks stemming from Covid-19-related crime, which could include (i) increased misuse of online financial services and virtual assets to move and conceal illicit funds; and (ii) possible corruption connected with governmental stimulus funds or international financial assistance.

At the national level, law enforcement agencies have issued warnings related to these evolving threats. For instance, security officials in the United Kingdom and United States have issued a joint statement[7] urging individuals and organisations to maintain a heightened level of security and advising them about threats connected to email and message scams that appear to have come from trusted sources (eg the World Health Organisation) and offer medical supplies or treatment to fight the pandemic, or advertise fictitious solidarity initiatives. The statement paid particular attention to cybercriminal actions directed at exploiting vulnerabilities in software and remote working tools, including video conferencing software.[8] According to law enforcement agencies, the main aim of Covid-19-related cyber crime is to steal personal information, induce the download of malicious software, commit fraud or seek illegal gains.

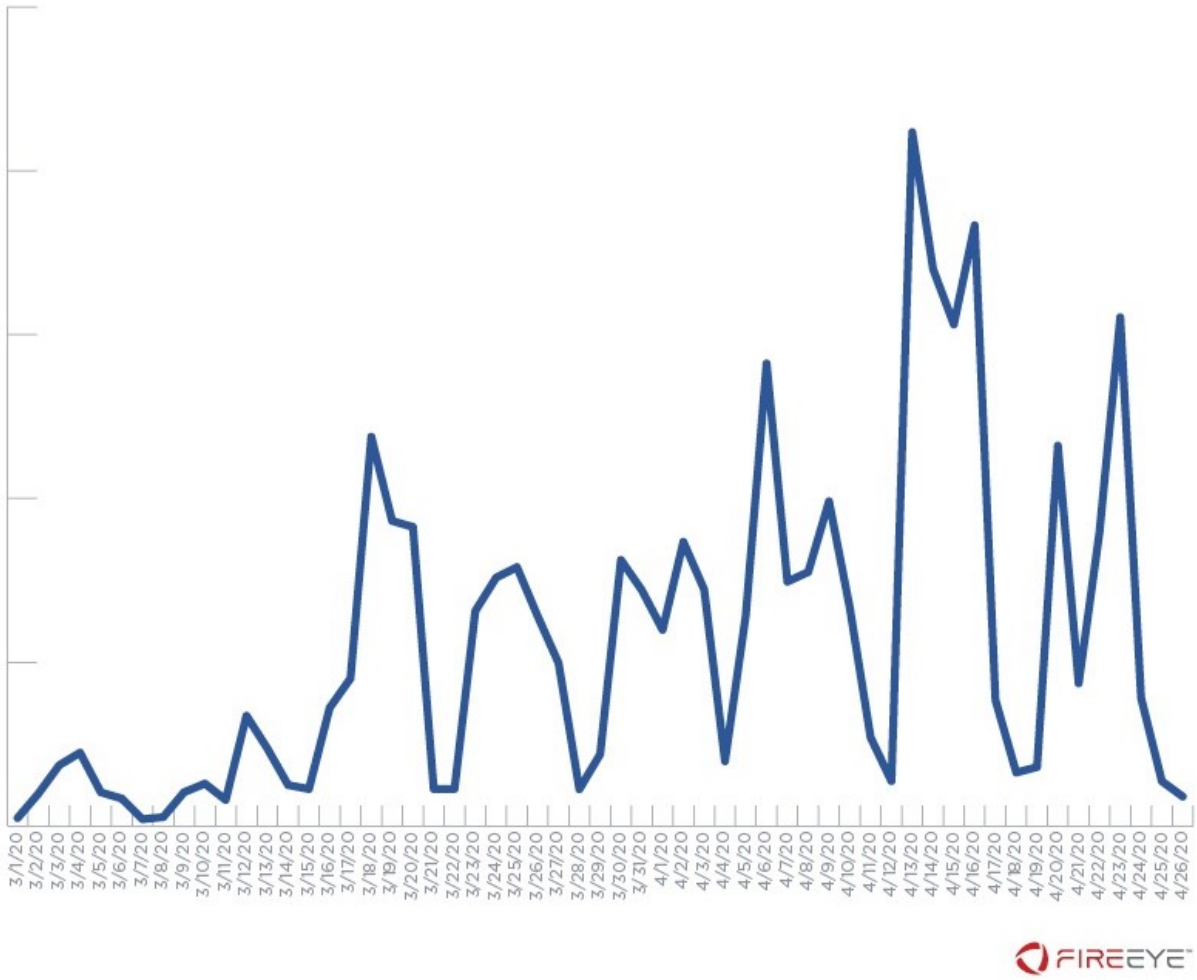
Data show that Covid-19-related cyber threats are increasing. For example, Carbon Black (2020), a cyber security company, noted that ransomware attacks had increased 148% in March 2020 over baseline levels in February 2020. Among the different sectors, the finance sector was the top target, with a 38% increase in cyberattacks against financial institutions. Similarly, the Financial Services Information Sharing and Analysis Center (2020) identified over 1,500 high-risk domains (ie those likely to have been set up by threat actors) created on or after 1 January 2020 containing both a Covid-19 and financial theme. Google (2020), meanwhile, reported 18 million daily malware or phishing emails related to Covid-19 in early April 2020, which was in addition to more than 240 million Covid-19-related daily spam messages. This is consistent with the findings of Mandiant Threat Intelligence that indicate coronavirus-themed malicious emails reached their highest observed volume on 13 April (Figure 1 provides a relative scale of the volume of coronavirus-themed malicious emails).

[6] The International Criminal Police Organization (2020b).

[7] United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the United Kingdom's National Cyber Security Centre (2020).

[8] See eg CERT-EU website https://media.cert.europa.eu/cert/moreclusteredition/en/securityboulevard-e65efcacb6cd9bf31080185461c6e720.20200404.en.html.

Figure 1: Malicious email detections with coronavirus theme, 1 March–26 April 2020



Source: Mandiant Threat Intelligence.

This situation has put enormous pressure on cyber resilience capabilities at financial institutions and their third-party technology service providers. The financial industry and the official sector have been making progress towards adopting a common cyber lexicon,[9] implementing a robust cyber security framework[10] and enhancing international cooperation.[11] However, not even the most extreme scenarios envisaged a global lockdown with such high levels of online activity over such a time span, and subject to the prevailing high degree of uncertainty.

Criminals also have ample scope to exploit gaps or weaknesses in AML defences in the financial system opened up by the pandemic crisis. As noted above, financial institutions have now resorted to remote onboarding and identity verification due to social distancing and office closures. This could create potential loopholes for money launderers, especially in cases where financial institutions may not be fully equipped to verify the identity of customers remotely. The need to devote additional resources to ensuring the effective operation of business continuity arrangements may mean that financial institutions are less

9 Financial Stability Board (2018).

10 Basel Committee on Banking Supervision (2018).

11 Domanski (2019).

able to monitor suspicious transactions. Authorities are in a similar situation. As a result of the crisis, many authorities are prioritising other prudential areas and therefore postponing AML onsite inspections or relying only on off-site monitoring. Some are also delaying AML reporting and other AML regulatory requirements in order to alleviate the resource pressure on both financial institutions and their own staff. Moreover, a number of jurisdictions have seen an increase in cash withdrawals during the crisis.[12] When the flow of cash goes into reverse as the situation stabilises, this could provide cover for ML activities.

3. Cyber resilience measures

In response to current and emerging cyber threats, Interpol has released international guidelines to curb illegal activities arising in the context of the Covid-19 crisis.[13] National agencies responsible for cyber security have given guidance and advice. For instance, the joint statement by the UK and US cyber security agencies includes a list of practical indicators that systems have been compromised, and encourages individuals and organisations to review their guidance on home working, mitigating malware and ransomware attacks, enterprise virtual private network (VPN) security and risk management, among other topics, to ensure that Covid-19-related challenges are addressed. Similarly, the Singapore Computer Emergency Response Team (SingCERT) recently published measures to strengthen the cyber security posture of organisations and their staff while teleworking.[14] For organisations, the SingCERT measures emphasise: (i) ensuring that remote access systems are updated with the latest patches, security configurations and anti-virus signatures; (ii) performing regular audits of privileged domains; (iii) providing regular reminders to employees about cyber threats and preventative tips so that their awareness is heightened; and (iv) putting in place cyber incident response and recovery plans that can be effectively implemented in view of the telecommuting circumstances.[15]

Financial authorities are generally tackling cyber security risks as part of their efforts to ensure the continuity of critical financial services,[16] including through requirements to bolster firms' operational resilience or business continuity. Coelho and Prenio (2020) gave examples of authorities that have advised financial institutions to remain vigilant with respect to cyber threats and to proactively assess and test the capacity of existing infrastructure as part of their business continuity arrangements. Financial institutions' staff responsible for information or IT security are generally considered key or essential financial workers and are therefore expected to remain alert against cyber-criminal activities.[17] In the United States, the Cybersecurity and Infrastructure Security Agency – the country's cyber security agency – has identified as essential workers, among others, third-party staff supporting banks and other financial institutions

[12] See eg report in the Financial Times, www.ft.com/content/28b59b28-44ac-43ec-b0dd-c1f1eacfbeb0, and BIS Bulletin, no 3, www.bis.org/publ/bisbull03.pdf, which posits that the outbreak could in principle lead to both higher precautionary holdings of cash by consumers and a structural increase in the use of mobile, card and online payments.

[13] The International Criminal Police Organization (2020a).

[14] Singapore Computer Emergency Response Team (2020).

[15] See eg the Advisory issued by the Indian National Critical Information Infrastructure Protection Centre, https://nsdl.co.in/downloadables/pdf/17%20Circular%20-%20Cyber%20Security%20Advisory%20dated%20March%2025,2020.pdf.

[16] See eg FSB press release, www.fsb.org/2020/04/fsb-members-take-action-to-ensure-continuity-of-critical-financial-services-functions/.

[17] See eg statement by the PRA on key financial workers who are critical to the Covid-19 response, www.bankofengland.co.uk/news/2020/march/guidance-for-schools-colleges-and-local-authorities-on-maintaining-educational-provision.

responding to cyber incidents, and the Office of the Comptroller of the Currency (OCC (2020a)) has asked its supervised institutions to reflect this consideration in their business continuity approaches.

In addition, a number of authorities are taking complementary measures specifically targeted at the increasing levels of cyber criminality in the financial sector during the pandemic crisis.

Raising awareness through public statements about increasing levels of cyber crime

Several authorities have issued public statements asking supervised institutions to remain vigilant to the heightened risks connected with ML and TF;[18] and/or to remind employees to be alert for such criminal activities.[19] A few authorities have gone further and publicly outlined the types of cyber resilience measure undertaken in the context of Covid-19. An example of this approach is the April 2020 public joint statement by the Bank of Italy and the Institute for the Supervision of Insurance (IVASS) – the Italian insurance supervisor. This described how the two institutions are addressing Covid-19 cyber security challenges by focusing on (i) the vulnerabilities resulting from the more intensive use of teleworking; (ii) conducting reviews to gain insights on the characteristics of cyber threats in the context of Covid-19; and (iii) relying on information exchange mechanisms.

Providing guidance on the most relevant cyber resilience areas

Some authorities have provided guidance on the heightened risks to IT networks and non-public information. For instance, the New York State Department of Financial Services (DFS) (2020) highlighted (i) the importance of relying on secure VPN connections that will encrypt all data in transit; (ii) using multi-factor authentication protocols and updating them for key actions (eg security exceptions, wire transfers); (iii) applying robust security protocols to company-issued devices and strong controls to personal or home devices used to access corporate technological infrastructures; (iv) configuring corporate video and audioconferencing facilities in a way that limits unauthorised access; and (v) taking measures that prevent the loss of non-public data.

As part of its Covid-19 cyber guidance, the DFS has also asked their regulated entities to address third-party risks connected with the current exceptional circumstances. It expects regulated entities to coordinate with critical vendors to ascertain that they are adequately addressing the new risks and challenges posed by the pandemic crisis.

Another area of focus is the adjustment of cyber security incident response plans to the pandemic environment. For example, the Abu Dhabi Global Market's (ADGM) Financial Services Regulatory Authority (FSRA) (2020) communicated to their financial institutions the importance of instituting incident response plans that are commensurate with the nature, scale and complexity of their business in the current context. This was intended to increase preparedness for identifying and mitigating operational and cyber risks, thus enhancing the financial sector's resilience so as to diminish the impact of possible cyber attacks. Incidentally, as part of its 2020 work programme, the FSB is currently consulting on a toolkit of effective practices to assist financial institutions before, during and after a cyber incident.[20]

Finally, several authorities are emphasising staff training and awareness at financial institutions. For example, the Financial Industry Regulatory Authority (FINRA (2020)), as part of its Covid-19 guidance

[18] See eg MAS media release on regulatory and supervisory measures to help FIs focus on supporting customers, www.mas.gov.sg/news/media-releases/2020/mas-takes-regulatory-and-supervisory-measures-to-help-fis-focus-on-supporting-customers.

[19] See eg New York State Department of Financial Services Guidance to regulated entities regarding cyber security awareness during Covid-19 pandemic, www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness.

[20] FSB (2020).

to members, recommends that firms train their staff on (i) how to connect securely to the office environment or office applications from a remote location; and (ii) potential scams, fraudulent communications and other criminal activities. In addition, FINRA emphasises the need for IT support staff or others involved in managing or supporting staff using the firm's systems to be alert and adequately trained to deal with fraudsters and social engineering schemes, such as bogus calls requesting password resets or fake reports of lost phones or equipment.

Information-sharing on Covid-19-related threats

Some authorities are using existing domestic channels to exchange information on Covid-19-related cyber threats with financial institutions and other trusted counterparts. Organisations such as the Bank of Italy and IVASS are using them to disseminate security bulletins, organise webinars on attack techniques and possible countermeasures, and facilitate training on the correct use of company devices and the strengthening of controls connected to remote work.

At the international level, the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures and the BIS's Cyber Resilience Coordination Centre (CRCC) are expected to play an important role in facilitating the exchange of information on Covid-19-related threats. The ECRB serves as a forum on systemic resilience against cyber risks. In recent weeks its members have agreed to share more cyber information and intelligence, with the aim of identifying cyber threats and exchanging best practice to prevent attacks.[21] For its part, the CRCC seeks to provide a structured and careful approach to knowledge-sharing and collaboration between central banks in the area of cyber resilience. A core service is to provide a secure collaboration platform for information-sharing on multilateral cyber threats.

4. AML Measures

The FATF has issued a statement[22] encouraging the official sector, financial institutions and other businesses to remain vigilant to current ML and TF risks while (i) using the flexibility built into the FATF's risk-based approach to address the challenges posed by the crisis; (ii) implementing responsible digital customer onboarding for the delivery of digital financial services to the fullest extent possible in the light of the lockdown and social distancing measures; (iii) working closely together, including by sharing relevant information; and (iv) offering effective mechanisms through which the industry can report Covid-19-related financial crime to authorities.

FATF (2020b) and our own research show that a number of national financial intelligence units (FIUs) and financial authorities worldwide have sought to draw attention to financial crime in the Covid-19 environment; emphasise the importance of continuing to meet AML/CFT requirements; and/or highlight the need to apply those requirements or supervisory tools in a way that achieves a balance between effectively mitigating ML and TF risks emerging in the Covid-19 environment while offering flexibility in the context of the pandemic crisis.

[21] Panetta (2020).

[22] FATF (2020a).

Issuing public statements drawing attention to Covid-19 ML and TF threats

All central banks and banking supervisory agencies issuing public statements related to Covid-19 ML and TF threats have drawn attention to the evolving risks in the pandemic crisis and/or the heightened importance of continuing to fight these crimes and meeting AML/CFT requirements.[23] Some financial authorities have specifically referred to the FATF statement. For instance, the Hong Kong Monetary Authority (HKMA) wrote to all authorised institutions making them aware of the FATF statement and highlighting the HKMA's expectations about emerging ML/TF risks, in particular the importance of remaining alert to criminal activities and detecting and reporting suspicious transactions.

Emphasising the flexibility built into the AML/CFT risk-based framework and providing guidance on its application

Some financial authorities have also issued public statements that, due to the pandemic crisis, it is necessary to apply the AML/CFT requirements and/or the corresponding supervisory tools flexibly, in particular with respect to reporting requirements.[24] For example, the HKMA has indicated that it is using its supervisory tools flexibly in this period and reiterated that its risk-based approach to AML/CFT supervision does not require or expect a "zero failure" outcome.[25]

A number of authorities worldwide have provided guidance on the way the AML/CFT risk-based framework will be applied flexibly in the Covid-19 context. In the United States, the Financial Crimes Enforcement Network (FINCEN) has provided for certain regulatory relief under the risk-based approach to the AML/CFT requirements, including exempting firms from requirements to (re)verify beneficial ownership for new loans extended to existing customers under the Coronavirus Aid, Relief, and Economic Security (CARES) Act Paycheck Protection Program.[26] The OCC (2020b) has publicly expressed support for the FINCEN's approach and stated that, when evaluating banks' AML/CFT compliance programmes, it will consider the actions taken by banks to protect and assist employees, customers and others in response to the Covid-19 pandemic, including accepting reasonable delays in reporting filings and other risk management processes.

Authorities have also emphasised that financial institutions should continue to provide essential financial services, while at the same time seeking to mitigate ML risks by using the various tools at their disposal. One such tool is machine learning, to which financial institutions have recently turned for improved ML detection. Under normal circumstances, machine learning can dramatically improve ML detection rates, thus cutting the workload of AML staff.[27] But the Covid-19 crisis has changed the behaviour of retail and corporate clients, which could drastically reduce the effectiveness of machine learning techniques, particularly those trained on past patterns of behaviour.[28] Other tools may face similar challenges.

[23] See eg statement from the Danish Financial Supervisory Authority, www.dfsa.dk/News/Press-releases/2020/Fighting_money_laundering_covid19.

[24] See eg press release issued by the European Banking Authority, https://eba.europa.eu/eba-provides-additional-clarity-on-measures-mitigate-impact-covid-19-eu-banking-sector.

[25] HKMA (2020).

[26] FINCEN (2020).

[27] See Coelho et al (2019).

[28] See eg report in Risk.net, www.risk.net/risk-management/7520706/covid-19-frazzles-ai-fraud-systems.

Providing guidance on digital customer on-boarding and simplified due diligence

Some authorities have been echoing FATF's call to use financial technology to manage some of the customer due diligence issues presented by Covid-19. In this regard, Luxembourg's Commission de Surveillance du Secteur Financier (CSSF (2020)) has encouraged professionals under its AML/CFT supervision to use digital ID systems with technology, processes, governance and other safeguards that assure an appropriate level of trustworthiness in line with relevant FATF Guidance (eg on digital identity). In the light of these requirements, the CSSF considers that live video-chats could provide appropriate safeguards to verify a customer's identity.

Other authorities have opted to allow simplified due diligence approaches. For instance, the Swiss Financial Market Supervisory Authority (FINMA (2020)) decided to "grant a facilitation" in the application of due diligence requirements for new business relationships entered into before 1 July 2020. In particular, it has extended the 30-day period for confirming the authenticity of identification documents to 90 days. During this period, a new business relationship can be entered into with sufficient information regarding the contracting parties and a simple copy of the identification document provided that, on the basis of a risk-based assessment, the application of this flexibility is deemed appropriate.[29]

Working closely with the financial sector

Supervisors, FIUs and law enforcement agencies are using their existing channels to share ML/TF risks linked to Covid-19 with financial institutions and other private sector entities. For example, the HKMA (2020) is supporting a public-private partnership to share ML/TF information linked to Covid-19 and related typologies, particularly those related to fraud linked to Covid-19. In addition, authorities have started to set up mechanisms by which victims, financial institutions and other businesses can report Covid-19-related fraud. In this regard, FINCEN (2020) has established a specific online contact mechanism so that financial institutions can communicate any Covid-19-related concerns while adhering to their AML/CFT obligations.

5. Concluding remarks

The Covid-19 crisis provides a favourable environment for financial crime. Authorities worldwide have responded with statements and by providing guidance to financial institutions, particularly on mitigating cyber attacks and ML/TF risks. In both areas, authorities have highlighted the need for (i) drawing attention to these crimes so that financial institutions and the general public are better informed; (ii) extra vigilance with respect to increasing and evolving risks; and (iii) active sharing of information between the public and private sectors, and within and between jurisdictions. Also, the guidance issued underscores the trade-offs between expecting financial institutions to enhance or adjust their cyber resilience and AML frameworks and, on the other hand, avoiding imposing an excessive burden that could hinder financial institutions in delivering key financial services.

[29] See also BAFIN information on new developments and key points, www.bafin.de/EN/Aufsicht/CoronaVirus/CoronaVirus_node_en.html.

References

Abu Dhabi Global Market's Financial Services Regulatory Authority (2020): "Heightened risk of cyber-attacks amidst the COVID-19 pandemic", Notice No: FSRA/FCPU/04/2020, 30 March.

Bank of Italy and the Institute for the Supervision of Insurance (2020): "Cyber security in times of Covid-19, Bank of Italy and IVASS' coordination group for cyber security", 17 April.

Basel Committee on Banking Supervision (2018): "Cyber-resilience: range of practices", December.

Carbon Black (2020): "Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted", 15 April.

Coelho, R and J Prenio (2020): "Covid-19 and operational resilience: addressing financial institutions' operational challenges in a pandemic scenario", *FSI Briefs*, no 2, April.

Coelho, R, M De Simoni and J Prenio (2019): "Suptech applications for anti-money laundering", *FSI Insights on policy implementation*, no 18, 29 August.

Commission de Surveillance du Secteur Financier (2020): "Financial crime and AML/CFT implications during the COVID-19 pandemic", 10 April.

Domanski, D (2019): "Cyber security: finding responses to global threats", speech delivered at the G7 2019 Conference on Cybersecurity, Paris, 10 May.

Financial Action Task Force (2020a): "Statement by the FATF President: Covid-19 and measures to combat illicit financing", 1 April.

——— (2020b): "Covid-19-related money laundering and terrorist financing risks and policy responses", 4 May.

Financial Crimes Enforcement Network (2020): "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic", press release, 3 April.

Financial Industry Regulatory Authority (2020): "Cybersecurity Alert: Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19)", Information Notice, 26 March.

Financial Services Information Sharing and Analysis Center (2020): "High risk domains with a Covid-19 and financial theme", 16 April.

Financial Stability Board (2018): "Cyber lexicon", 12 November.

——— (2020): "Effective practices for cyber incident response and recovery: a consultative document", 20 April.

Google (2020): "Protecting businesses against cyber threats during COVID-19 and beyond", 16 April.

Hong Kong Monetary Authority (2020): "Coronavirus disease (COVID-19) and Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) measures", 7 April.

New York State Department of Financial Services (2020): "Guidance to DFS' Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic", 13 April.

Office of the Comptroller of the Currency (2020a): "Pandemic Planning – Essential Critical Infrastructure Workers in the Financial Services Sector", OCC Bulletin 2020-23, 25 March.

——— (2020b): "Bank Secrecy Act/Anti-Money Laundering: OCC Supports FinCEN's Regulatory Relief and Risk-Based Approach for Financial Institution Compliance in Response to COVID-19", OCC Bulletin 2020-34, 7 April.

Panetta, F (2020): "Beyond monetary policy – protecting the continuity and safety of payments during the coronavirus crisis", *The ECB Blog*, 28 April.

Singapore Computer Emergency Response Team (2020): "Tips for Staying Cyber-Safe While Telecommuting", 5 April.

Swiss Financial Market Supervisory Authority (2020): "Exemptions for Supervised Institutions due to the Covid-19 Crisis", 14 April.

The International Criminal Police Organization (2020a): "Covid-19 Pandemic, Guidelines for Law Enforcement Agencies", 26 March.

——— (2020b): "Preventing crime and protecting police: INTERPOL's COVID-19 global threat assessment", 6 April.

United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the United Kingdom's National Cyber Security Centre (2020): "Joint Alert (AA20-099A), COVID-19 Exploited by Malicious Cyber Actors", 8 April.