INTRODUCTION

As COVID-19 (Coronavirus disease 2019) continues to spread across countries, it is first and foremost a human tragedy and a medical crisis which requires collective action to mitigate its effects and find solutions on a global basis. With the situation becoming more acute in parts of the world, the efforts of the international community to tackle this pandemic should be applauded and supported.

In the current crisis environment, financial firms are focused on serving clients, customers and communities, and supporting the broader economy. This includes work on a variety of measures, such as activating continuity plans to safeguard operations during a period of heightened disruption. As part of this, the risks associated with financial crime continue to be a top priority for the global financial services industry, and the work to address those risks remains an essential part of financial institutions’ critical infrastructure.

Financial crime is a contributor to societal ill and a threat to both financial stability and financial inclusion and its mitigation and prevention is a vital issue. The COVID-19 crisis has raised a number of new challenges for financial crime risk management which should be tackled on a consistent, international basis. As such, we take this opportunity to discuss some key issues we believe policy makers at the G20 level and beyond – along with the international standard setting bodies, law enforcement and regulators – should consider when examining the response to the crisis in a holistic fashion. This should be part of the broader effort underway to ensure effective international cooperation across all areas of the pandemic response.

---


2 For further information on the wider work of the IIF in relation to financial services and the COVID-19 pandemic, please see: https://www.iif.com/COVID-19
Specifically, we outline herein examples of typologies many in the industry and law enforcement are currently seeing directly linked to the COVID-19 crisis in order to ensure collective awareness of new and emerging threats. We also consider operational issues for financial crime compliance and risk management which may arise from matters concerning the pandemic response. Lastly, we discuss how further work on a cross-border basis in the following areas will assist both in the current crisis setting and in the longer-term fight against financial crime:

1. **A collective international response**: Building on the good work already underway at the Financial Action Task Force (FATF)\(^3\), countries should ensure their response to the COVID-19 crisis is carefully coordinated internationally. The FATF should be supported in identifying challenges, good practices and policy responses to new threats and vulnerabilities to encourage the appropriate consistency globally and to ensure effective cooperation between the public and private sectors.

2. **Clear communication of priorities**: The pandemic has raised a number of new challenges for financial crime risk management and now more than ever there is a need for clear regulatory guidance on prioritization in line with the risk-based approach. This should take into account the necessary flexibility from changes to the system-wide crisis environment.\(^4\)

3. **The sharing of information**: While certainly not a new issue for effectiveness in the global anti-financial crime framework, the crisis has emphasized the need for sharing financial crime related information on a domestic and cross border basis within financial institutions, between financial institutions and between public authorities. The pandemic crisis has, in particular, shown the need for effective public/private sector mechanisms of cooperation between financial institutions, regulators and law enforcement to ensure new threats and updated priorities are communicated in an efficient and timely manner.\(^5\)

4. **The use of technological innovation**: The financial crime risk management space is one that can benefit from advancements in financial technology solutions. Their use, especially due to the need for more digital customer due diligence solutions in response to COVID-19 social distancing, should be encouraged on a consistent international basis across jurisdictions.\(^6\)

---


\(^3\) We note that the FATF has stated that regulators, supervisors, financial intelligence units, law enforcement authorities and other relevant agencies can provide support, guidance and assistance for the private sector on how national AML/CFT laws and regulations will be applied during the current crisis: FATF, Statement by the FATF President: COVID-19 and measures to combat illicit financing, April 1, 2020 (hereafter referenced as the “FATF COVID-19 Statement”).

\(^4\) We note the FATF has stated that supervisors, financial intelligence units and law enforcement agencies should continue to share information with the private sector to prioritize and address key ML risks, particularly those related to fraud, and TF risks linked to COVID-19: FATF, FATF COVID-19 Statement, April 1, 2020.

\(^5\) We note that the FATF has stated that line with the FATF Standards, it encourages the use of technology, including Fintech, Regtech and Supertech to the fullest extent possible. It also notes that digital/contactless payments and digital onboarding reduce the risk of spreading the virus: FATF, FATF COVID-19 Statement, April 1, 2020.
1. New and emerging risk issues for financial crime linked to the COVID-19 pandemic

It is a regrettable fact that the COVID-19 crisis has led to a rise in illicit financial activity associated with the pandemic. Criminals are exploiting the current environment of fear and anxiety through a range of methods to defraud victims of money and, in some cases, replace previously applied criminal methodologies displaced by the new environment of social distancing and self-isolation. Supply chains have also been disrupted, necessitating a pivot to new and potentially unfamiliar clients. Understanding how both the public and private sector are seeing new issues and new threats is critical to addressing them in a coherent fashion.

It is important to note that due to the nature of how a financial institution monitors and detects criminal financial flows, the precise details differentiating COVID-19 related crime from other types of illicit activity is not yet fully clear from the current data; however, certain patterns are emerging. In particular, there has been a documented rise in the threat of cyber incidents as the operating infrastructure of companies around the world has shifted to accommodate telework and as personal online behavior changes in response to social distancing. This type of criminal activity can include phishing campaigns, the use of ransomware, growth in new types of mule accounts and the advance of malicious online applications targeting the vulnerable and the isolated. Fraud and counterfeiting schemes in particular have seen a significant uptick, with scams linked to the counterfeiting of COVID-19 related supplies including facemasks and other personal protection equipment and/or the sale of products falsely offering a virus cure.

Previously understood criminal typologies may also adapt in certain ways in the crisis environment. Methodologies for human smuggling and wildlife trafficking, for instance, may change with updated routes necessitated by border closures. Terrorist financiers may use the crisis to raise funds by moving into new COVID-19 linked criminal activity. Economic sanctions targets may seek to take advantage of disruptions and changes to supply chains to evade financial institutions’ compliance systems. Certain types of human exploitation could continue to shift online as social distancing carries on. Criminals may seek out struggling businesses to invest their illicit funds by more easily obtaining real estate sold out of desperation, acquiring cafes and restaurants that have gone bankrupt, or investing liquidity in small and medium sized enterprises (SME) which cannot obtain funds elsewhere.7

Concerns also persist around potential increases in systemic corruption, whereby COVID-19 related funds or aid packages are misappropriated or diverted locally or nationally, preying off the scarcity and demand for such resources. Lastly, financial activity patterns are changing and may vary country-by-country. There have been some examples of an accretion in cash withdrawals as the crisis has evolved; however – conversely – volumes of online payments and transfers to different regions have increased as fears of virus transmission through physical money grows in certain quarters. It will be important to decipher if a spike in virtual money movements include a movement of cash-based criminal activity online.8

---

7 As an example, please see the statement on these issues from the Regional Council of Darmstadt, Germany: https://rp-darmstadt.hessen.de/pressemitteilungen/rp-warn-vor-missbrauch-der-corona-pandemie-f%C3%8Crdvergaben.html

8 For instance, some increases in online payments and money transfers are legitimate changes in customer behavior owing to the crisis, such as increases in small remittance transfers to regions economically impacted by the pandemic or deposits arising from government support schemes. Others, however, may linked to illicit flows, insider trading and the proceeds of corruption. A review of differentiation in financial patterns will be important.
Law enforcement is playing a critical role in documenting and relaying these new sources and examples of criminal financial behavior related to the pandemic and there has already been much work undertaken in this regard. Interpol, for example, has been advising the international community on issues such as the rise in advance payment fraud related to COVID-19 supplies, the shift of associated illicit money-flows coinciding with the outbreak in more countries, and the layering techniques employed by criminals to launder the proceeds of crime. It also assists member countries to interrupt the flow of crime proceeds by providing swift alerts to banks. Europol has begun a weekly assessment on the impact of the COVID-19 pandemic on crime and terrorism in the European Union. National authorities in countries impacted by the virus are also documenting new typologies and endeavoring to update their regulated entities on new threats to assist in risk assessment.

As discussed in more detail in section three of this paper, it is vital that the public sector keep financial institutions informed of any impact seen from COVID-19 on the threat landscape; and vice-versa from the financial institution’s own organization and customer perspective. It is important for the private sector to have closer collaboration with law enforcement authorities and regulators in preventing/detecting such crimes and new or enhanced means of ensuring that clear connectivity domestically and internationally should be considered.

2. Operational issues for financial crime risk management from the COVID-19 pandemic

Banks, insurance companies and other financial firms are proactively taking numerous measures to address the challenges stemming from COVID-19. As the IIF has noted, these measures can generally be grouped across three categories: firms are taking preventative measures to protect their employees and customers; firms have taken recovery measures when employees become infected; and firms are taking forward-looking actions to ensure the effectiveness of their contingency planning, to strengthen operational resilience and to support the broader economy. Financial firms are not alone, of course, in taking these actions, as organizations around the world are responding to the crisis. Any company-specific initiatives are overridden by government requirements that have been or may be put in place in specific jurisdictions.

As a major part of these endeavors, financial institutions globally continue to prioritize the operations of their financial crime risk management and compliance teams. However, the challenges outlined in section one of this paper in relation to new and emerging COVID-19 threat typologies, coupled with the realities of new ways of working, may present the need for further closer cooperation between financial

---

12 For example, the Financial Crimes Enforcement Network (FinCEN) in the United States has stated that financial institutions to remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters and has given examples on new typologies of which to be aware: https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions
institutions and the regulatory community on the coordination and interpretation of new risk coupled with ongoing assessments.

Recent official sector pronouncements on a national or regional basis have been helpful in this regard. For example, the European Banking Authority (EBA) called on competent authorities to support financial institutions’ ongoing efforts by sharing information on emerging money laundering and terrorist financing (ML/TF) risks, setting clear regulatory expectations and using supervisory tools flexibly.\(^4\) The Financial Crimes Enforcement Network (FinCEN) in the United States also published guidance on compliance with Bank Secrecy Act (BSA) obligations which, among other things, addresses flexibility in line with the risk-based approach under current circumstances.

As with any change to operations emanating from a crisis environment, not all patterns of work will remain the same and adaptation must occur to handle new challenges. In this environment, it will be critical to ensure the public sector define and oversee policy in a way that empowers financial institutions to implement the government’s vision. Clear and consistent guidance from the public sector that is implemented faithfully at the bank examiner level is crucial in this regard. The FATF recently issued a statement which called on regulators, supervisors, financial intelligence units, law enforcement authorities and other relevant agencies to provide support, guidance and assistance for the private sector on how national AML/CFT laws and regulations will be applied during the current crisis. We strongly agree that, as the FATF states, “such guidance can help give reassurance that the authorities share their understanding of challenges and risks involved in the current situation, and of the appropriate actions to take.”\(^{15}\)

A specific example of regulatory clarity that would assist in operations under the current crisis and during the rebuilding phase is explicit guidance to financial institutions on any measures that can be adopted to ensure legitimate non-governmental/intergovernmental organization (NGO/IGO) activity addressing the crisis is not negatively impacted.\(^6\) This would need to involve agreed guidance from both the local country governments where the aid is to be distributed, as well as the financial institution’s home country regulator that in these “non-equivalent” jurisdictions (from an AML/CFT regulatory perspective), special risk-based measures may be taken given the pandemic.

Though the general point on regulatory clarity for AML/CFT is much broader than the current crisis, it is amplified by the significantly increased risks arising from fluid circumstances that could lead to de-risking decisions. In addition, the large level of data currently flowing through the system based on new crime typologies and shifting consumer behavior emanating from the pandemic response can, inter alia, lead to increases in false positive monitoring results raising issues for the effectiveness and efficiency of compliance operations and highlighting commercial issues with continuing business. Clear regulatory guidance in line with the risk-based approach which takes into account the necessary flexibility from changes to the system-wide environment is important operationally going forward. This is particularly true when considering issues for smaller and emerging market banks, who may not have the resources or capacity to adapt as quickly or effectively to the new order.\(^{17}\)

\(^{14}\) European Banking Authority, *Statement on actions to mitigate financial crime risks in the COVID-19 pandemic*, March 31, 2020


\(^{16}\) We note that the FATF has stated that national authorities and financial institutions should apply a risk-based approach to ensure that legitimate NPO activity is not unnecessarily delayed, disrupted or discouraged. FATF, *FATF COVID-19 Statement*, April 1, 2020.

\(^{17}\) Indeed, some smaller banks and those in developing markets may not have the necessary capacity to respond to the array of challenges the COVID-19 response brings, including changed CDD policies, new crime typologies, and limitations on resources. Another issue is the capacity
3. **Issues and recommendations for collective action in combatting illicit financial flows during the COVID-19 pandemic and beyond**

The collective challenge of dealing with the pandemic’s human toll and addressing its ancillary economic and social effects is of paramount importance. In addition to considering operational challenges and new threat typologies in the context of pandemic-related financial crime matters, it is important that the crisis response also takes into account a number of issues which, when considering lessons learned from this crisis and past crises, would generally help to improve the overall environment in stopping illicit flows.

We note that in most cases, these are not new issues when examining the effectiveness of financial crime risk management on a global basis. The communication of priorities, the sharing of information and unifying and modernizing the notion of technology are all critical elements to help place greater emphasis on bolstering the efforts of law enforcement with the help of the private sector, and ensuring legal and regulatory frameworks are enhanced to enable stakeholders to achieve improved outcomes - especially in circumstances like we are seeing now.\(^1\)

**a. A collective international response:** Action on the mitigation of financial crime flows across borders requires a collective response by the global community. This would eliminate one of the incentives criminals have to channel their operations through jurisdictions they know are less resilient than others. This remains particularly true under the current pandemic environment, where both the public and private sectors have seen an uptick in COVID-19 related financial crime across the world. Specific jurisdictional policy pronouncements are helpful, but further assistance would come from the regulatory and law enforcement community coordinating their actions in concert with the private sector on an international basis.

The FATF has correctly begun coordination across the FATF members, FATF-Style Regional Bodies and their observer organisations such as the United Nations (UN), International Monetary Fund (IMF), World Bank, the Organization for Economic Cooperation and Development (OECD), the Egmont Group and Europol on COVID-19 related ML/TF risks and potential policy responses. We understand this work is in part meant to encourage the public sector to work with the private sector to identify and monitor emerging risks; and for the public sector to engage with the private sector to communicate AML/CFT expectations.

This effort using the global FATF network to identify challenges, good practices and policy responses to new threats and vulnerabilities arising from the COVID-19 crisis should be encouraged as part of a broader effort by the FATF which, they emphasize, is meant to clarify how the risk-based approach of the FATF Standards provides for emerging threats and vulnerabilities to be managed effectively and in support of COVID-19 aid and containment efforts.\(^2\) The closer


efforts are aligned across jurisdictions, the better the collective response will be in addressing new threats arising is this area from the pandemic. 20

In addition to the international response, improved interagency collaboration at the national level should also be considered. The value of such collaboration has always been recognized, however, in times of crises such coordination becomes of paramount importance as the gravity of criminal activity takes on a larger magnitude. Financial Intelligence Units, customs agencies, law enforcement and anti-corruption commissions should come together sharing insights on recent trends and typologies.21 Connecting the dots would allow for more timely identification and communication of emerging financial crime trends emanating from COVID-19 vulnerabilities.

b. Clear communication and prioritization: As noted in section two of this paper, when dealing with operational considerations of the crisis, clear regulatory guidance in line with the risk-based approach which takes into account the necessary flexibility from changes to the system-wide pandemic environment is important.

Given the high-volume of new and emerging threats and changes to financial activity patterns noted in section one of this paper, it is important the regulatory community communicate AML/CFT priorities so resources at financial institutions can be directed to address key matters. It would also be beneficial if governments could prioritize certain filing requirement at this time – for example, the filing of currency transaction reports could possibly be deferred. We understand the criticality of quickly filing suspicious activity reports (SAR), particularly in light of COVID-19 related criminal activity, but we would also suggest that governments may consider deferring the filing of continuous activity reporting for a period and that financial institutions should apply the risk based approach and prioritization of the filing of SARs.

In addition, we strongly believe national adherence to the FATF Recommendations and implementation of findings from the FATF Mutual Evaluation Reports (MER) are of critical importance. However, given the current crisis, a level of forbearance may be needed in both the implementation of MER findings in the near term and in the process for upcoming evaluations (which we understand will be delayed until the crisis has abated) in order to help make resources available for the regulatory and law enforcement community, along with the private sector, in tackling issues concerning the pandemic.

Lastly, there should be clear regulatory communication by public sector authorities on timelines for implementation of new national and regional financial crime standards pending in 2020. If a delay in legislation or implementing regulations is envisioned due to the crisis, this should be clearly communication in a timely fashion. As financial institutions grapple with managing COVID-19 related compliance responsibilities, clarity on these types of regulatory and legislative expectations would provide greater comfort around legal liability issues and would allow better allocation of compliance resources.

20 We also note Financial Stability Board (FSB) has prioritized international cooperation and the sharing of information in the broader policy response to the crisis: https://www.fsb.org/work-of-the-fsb/addressing-financial-stability-risks-of-covid-19/
21 In particular, AML/CFT authorities should also work with data protection authorities nationally and regionally to ensure to ensure the compatibility of AML/CFT requirements with data protection and privacy rules and other similar provisions (e.g. data security / localization) as laid out under FATF Recommendation 2.
c. **Cross-border and domestic information sharing:** A key component of the collective response to COVID-19 related financial crime issues is effective and operable sharing of critical financial crime data across borders and domestically enterprise-wide, between entities in different group enterprises, between enterprises and governments, and between governments – in both directions. Without adequate insights by banks, law enforcement, and intelligence agencies into the funding of these activities, efforts to stop criminals from inflicting further damage globally will be increasingly inhibited. Given that the impact of the virus on each successive “hot spot” jurisdiction seems to be following a similar pattern, the ability to share information on lessons learned across borders is particularly important.

This issue, however, certainly isn’t unique to the COVID-19 crisis. Working to find information sharing gateways for cross-border exchange and addressing the legal and regulatory barriers which prevent the sharing of data will greatly assist overall in more effective risk assessment and the mitigation of illicit financial flows.  


d. **Public/private sector cooperation:** As noted in section one of this paper, it is important for the private sector to have closer collaboration with the law enforcement authorities and regulators in preventing/detecting COVID-19 related crimes and a new or enhanced means of ensuring that clear connectivity on a global basis should be considered.

Specifically, national or regional authorities should ensure a mechanism is in place for feedback to be shared from the public sector to the private sector on new threat typologies or geographic indicators and, where allowable, tactical level information on specific cases. Where formal public-private partnerships are in place already in jurisdictions, analysis should be undertaken as to their effectiveness in this crisis situation to ensure the continued good functioning of the operational information sharing environment in light of the pandemic response.


e. **The use of technological innovation:** As outlined in previous IIF papers on the subject, the financial crime risk management space is one that can benefit from advancements in financial technology solutions. From machine learning and data analytics to digital identity, it is clear that the potential to change the day-to-day approach to these matters is significant.  

Given the need for social distancing under the current global pandemic, regional and national authorities, along with the international standard setting bodies, should examine how new methods of technological innovation could support due diligence measures, customer onboarding and customer maintenance. The FATF recently stated that they support the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible in this area. However, there is significant need to ensure that officials across the regulatory community consistently

---


24 IIF, Digital IDs in Financial Services Part 1: Embedding in AML Frameworks, August 2019: https://www.iif.com/Portals/0/Files/content/Innovation/08272019_if_digital_id_part_1.pdf


embrace the use of innovation. Policy makers and regulators should enable and support domestic and international dialogues on the topic, be open to new concepts and techniques, support technological solutions to scale and avoid any approach that is too prescriptive.

Digital ID is a pertinent example of identifying people remotely for both onboarding and the conducting of transactions while also mitigating ML/TF risks and its use should be encouraged. Some of the accommodations for Know Your Customer (KYC) practices that are being made for economic relief programs during the pandemic where ID is no longer presented physically - such as scanning and video conferencing to present ID - show the limitations of other types of remote customer due diligence (CDD) measures.

However, in jurisdictions where digital ID is not allowed or available, other options for CDD should be leveraged in a way that ensures the current crisis doesn’t exclude the vulnerable in society from access to the financial system due to social distancing rules. This is particularly important where new aid or loan programs developed in response to the current crisis may not be accessible due to established CDD requirements which slow down or prevent access to legitimate relief funds.

Lastly, we note that in some cases digital measures have been considered for both the first and second lines of defence in maintaining an effective financial crime compliance and risk management system during the COVID-19 response. However, provisions and proposals have often not been made for the third line of defence relating to activities of the internal audit function, other than by government supervisors/regulators that assess AML/CFT policies and practices on a regular basis. Digital solutions in this area should also be considered.

---

27 We note that the FATF has called on countries to explore using digital identity, as appropriate, to aid financial transactions while managing ML/TF risks during the COVID-19 crisis. FATF, FATF COVID-19 Statement, April 1, 2020.