MAYER | BROWN

FINANCIAL SERVICES | Financial Crime Compliance and Risk Management for Financial Institutions and Other Market Participants Amid the COVID-19 Outbreak

The COVID-19 outbreak presents serious challenges to financial institutions and other market participants. Among them is the need to maintain legal and compliance functions dedicated to detecting and preventing financial crimes in the midst of significant business, regulatory and market upheaval. Financial regulators around the world are issuing guidance that may better protect financial institutions and other market actors against financial crimes. Below, we highlight some of the available regulatory guidance and offer practical tips for identifying and mitigating financial crime risk during this unprecedented time.

The business and market disruption caused by the COVID-19 outbreak necessitates particular attention to potential financial crime and other misconduct, including potential misconduct (i) by insiders triggered by increased opportunities created by the crisis (e.g., insider trading on material non-public information relating to the crisis); (ii) by opportunistic fraudsters and criminals (e.g., social engineering and phishing that may prey upon current fear and uncertainty); or (iii) directly related to the crisis (e.g., financial crimes resulting from reductions in compliance monitoring and controls due to the crisis, potential misuse of bailout funds).

Financial regulators worldwide are warning that the COVID-19 pandemic may result in an increase in potential financial crime and other misconduct due to market disruptions, reduced staff, and other factors, as was the case during past global crises.[1] More specifically, the following authorities have responded to increased financial crime risks:

- On March 22, 2020, the U.S. Department of Justice ("DOJ") announced its first enforcement action against COVID-19-related fraud, after U.S. Attorney General William Barr directed the DOJ to "prioritize the detection, investigation and prosecution of illegal conduct related to the COVID-19 pandemic."[2]
- The Financial Crimes Enforcement Network ("FinCEN"), Financial Industry Regulatory Authority ("FINRA"), U.S. Securities and Exchange Commission ("SEC"), and Commodity Futures Trading Commission ("CFTC") have all advised financial institutions to be on high alert for a potential increase in "illicit financial activity" and have issued guidance that financial institutions can utilize to reduce instances of financial crime and misconduct.[3]
- FINRA has provided member firms with pandemic-related guidance and regulatory relief, advising member firms to maintain appropriate supervisory and cybersecurity practices.[4] FINRA also pointed member firms to prior guidance on pandemic preparedness.[5]
- FinCEN has warned financial institutions to remain alert about malicious and fraudulent transactions.[6] FinCEN reported that investor, imposter, and product scams are emerging during the COVID-19 pandemic and advised financial institutions to reference its prior guidance on financial crimes connected to natural disasters.[7]
- The SEC and CFTC warned potential investors about investment scams related to COVID-19. The guidance documents provided helpful tips on identifying fraudulent investment opportunities.[8]
- The European Banking Authority ("EBA") has highlighted fraud and other risks related to payment services during this period of "increased purchases on the internet" and reminded consumers of the EBA's and national regulators' key tips regarding the choice of financial products and services, which could also be relevant and applicable to other purchases in order to protect consumers.[9]
- The French Prudential Supervisory and Resolution Authority ("Autorité de contrôle prudentiel et de resolution or ACPR") and the French Autorité des Marchés Financiers ("AMF") warned the public about "the risks of scams in the context of the coronavirus outbreak and the downturn in financial markets". The two regulators reminded investors of the precautions and the vigilance measures to be taken "before any investment or subscription".[10]
- The European Securities and Markets Authority ("ESMA") and the AMF also issued recommendations and guidelines on compliance obligations which have a direct impact on financial misconduct during the COVID-19 crisis.[11] ESMA reminded market participants of the MiFID II call taping requirements, while also recognizing that recordings may become impracticable under present circumstances. It urged market participants to consider alternative steps that could mitigate the risks related to the lack of recording.
- The AMF echoed ESMA's call recording guidance and issued its own guidance advising regulated entities to be "watchful" of remote working situations during the COVID-19 crisis, especially in the case of potential "conflict[s] of interest (with other persons present when homeworking)" and "latency risks which may incur difficulties with the monitoring of real-time trading." The AMF invited market participants to contact it with potential difficulties with complying with regulatory obligations during this period, including difficulties relating to compliance obligations designed to prevent, detect and report potential financial misconduct.

Best Practices in Managing Financial Crime During the COVID-19 Pandemic

Below are some best practices and tips for detecting and avoiding potential misconduct based on lessons learned from the 2008 financial crisis and recent guidance from the SEC, CFTC, FinCEN, FINRA, EBA, ESMA, ACPR and AMF.

Managing Risks of Internal Misconduct

Financial institutions should consider the following measures during and after the COVID-19 pandemic in order to reduce financial crimes, misconduct and potential regulatory violations by employees and other internal actors, such as vendors and independent contractors:

- Review internal systems. Review internal systems for potential gaps in supervision and crime detection due to social distancing, reduced staff, teleworking, or reorganization.
- Practice good governance. If derogations from ordinary compliance or operating standards (such as working remotely, lack of electronic recording of trader communications) are necessary due to extraordinary circumstances, make sure such decisions are made consistent with existing governance mechanisms (e.g., a board committee authorized for compliance supervision) instead of ad hoc decisions by each business line. Such decisions should be properly documented, with the rationale for the derogation justified, the duration of the derogation clearly articulated, and if possible, a specific plan made to address the derogation when circumstances change (e.g., spot checking).
- Maintain Audit Trails. Maintain proper audit trails and fulfill voice-recording obligations with available technological solutions under changed working conditions (e.g., remote working or with reduced technological capabilities), consistent with available regulator guidelines. Where exceptional circumstances do not allow for compliance, consider available alternatives (e.g., keeping contemporaneous written records) for limited periods.[12]
- Scrutinize bailout funds. Ensure any government bailout funds are only requested, received, and used in accordance with applicable law. Abide by any conditions imposed as a requirement to receive such funds. Where bailout funds are subject to terms, conditions or restrictions, ensure that compliance staff (who may already be subject to significant demands) have adequate bandwidth to learn and monitor the new obligations.
- Watch insider trades. Review internal activity for potential insider trading.[13] FinCEN has not provided details as of the date publication of the alert, but disclosed that it has already received reports regarding suspected COVID-19-related insider trading.[14]
- Maintain consumer privacy and information security. When working remotely, ensure that virtual private networks and other remote access systems are patched with available security updates, check that internal systems can only be accessed by those individuals who are supposed to have access, use multi-factor authentication, and educate and train employees on how to maintain consumer privacy and information security.[15]
- Maintain critical functions. The outbreak will undoubtedly force financial institutions to make difficult decisions about how best to allocate resources. It is critical to maintain high-priority compliance functions, such as sanctions and AML/CTF monitoring.

Detecting and Mitigating Financial Crimes by External Actors

While taking into account reduced resources, financial institutions and other market participants must remain alert for red flags related to potential imposter, investment, and product scams, including

benefits, charities, and potential cyber-related fraud related to the outbreak. Below are some red flags identified by the SEC, CFTC, FinCEN, and FINRA related to COVID-19 and natural disasters that financial institutions and other market participants should consider, along with additional factors (such as a customer's overall financial activity and the institution's risk profile), to determine whether a transaction may be suspicious.

- False identity scams
    - Impersonation of government agencies such as the Centers for Disease Control and Prevention, international organizations such as the World Health Organization, or healthcare organizations.
    - Transactions where the payee organization's name is similar to, but not exactly the same as, those of reputable charities.
    - Payments to websites that are virtually identical to legitimate charities and relief organizations. These fraudulent websites often end with a ".com" or a ".net", while most legitimate charities' websites end in ".org."
- "Cure all" and other fraudulent cures
    - Promotions that falsely claim that the products or services of publicly traded companies can prevent, detect, or cure coronavirus, especially if the claims involve microcap stocks.
    - Trades or investments that involve: urgency; vague, unverifiable credentials; testimonials; free gifts; or claims of special insider knowledge or insights, promises of unusually large returns, guarantees, surefire trading signals, or low costs to open accounts.
    - Sale of unapproved or misbranded products that make false health claims pertaining to COVID-19. Such schemes are currently active: a website fraudulently claiming to offer "World Health Organization (WHO) vaccine kits" is the subject of the DOJ's first COVID-19-related enforcement action.[16]
    - Fraudulent marketing of COVID-19-related supplies, such as certain facemasks.
- COVID-Relief check fraud
    - Deposits of multiple emergency assistance checks or electronic funds transfers into the same bank account, particularly when the amounts of the checks are the same or approximately the same.
    - Cashing of multiple emergency assistance checks by the same individual.
    - Deposits of one or more emergency assistance checks, when the accountholder is a retail business and the payee/endorser is an individual other than the accountholder.
    - Opening of a new account with an emergency assistance check, where the name of the potential accountholder is different from that of the depositor of the check.
- Other Suspicious COVID-19-related transactions
    - The use of money transfer services for charitable collections.
    - Crowdfunding platforms that have limited policies and procedures in place to protect customer funds and identification. Information security units may have access to information that may help in the detection and reporting of such activity.
    - FinCEN encourages financial institutions to enter "COVID19" in Field 2 of the suspicious activity report (SAR) template if a financial institution identifies suspicious transactions linked to COVID-19, in addition to any other types of suspicious activity being reported.

Other Mayer Brown COVID-19-Related Regulatory Updates:

- Broker-dealers can find a full discussion of FINRA's Regulatory Notice 20-08 in our Legal Update COVID-19: FINRA Addresses U.S. Broker-Dealer Preparedness and Regulatory Relief in Regulatory 20-80.
- Additional tips for investment managers dealing with COVID-19 are available in our Legal Update Investment Management Survival Tips in the COVID-19 Environment.
- Firms registered with the CFTC can find information on the CFTC's regulatory relief in our Legal Update CFTC Issues Additional COVID-19 Relief For Remote Derivatives Trading.
- EU financial institutions are invited to review our Legal Update COVID-19: Compliance and Operational Risks for Financial Institutions: EU Financial Authorities Provide Initial Guidance.

And for additional resources, please visit our COVID-19 Portal.

Authors

- Nicolette Kost De Sèvres
- Alex C. Lakatos
- Brad A. Resnikoff
- Joydeep Sengupta
- Kerri Elizabeth Webb

---

[1] Helpfully, the Federal Reserve ("Fed") has suspended routine examinations and extended deadlines to resolve noncritical outstanding supervisory findings in order to permit institutions under its supervision to most efficiently deploy resources during this public health crisis. *Federal Reserve, Federal Reserve Statement on Supervisory Activities* (Mar. 24, 2020), available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200324a1.pdf.

[2] *See* DOJ, *Justice Department Files Its First Enforcement Action Against COVID-19 Fraud* (Mar. 22, 2020), available at https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud.

[3] *See* e.g., *FinCEN, The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity* (Mar. 16, 2020), available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions; FINRA Regulatory Notice 20-08 (Mar. 9, 2020), available at https://www.finra.org/rules-guidance/notices/20-08; SEC, *Look Out for Coronavirus-Related Investment Scams – Investor Alert* (Feb. 4, 2020), available at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus; CFTC, *Coronavirus: COVID-19 Customer Advisory*, available at https://www.cftc.gov/coronavirus.

[4] FINRA, *supra* note 3.

[5] FINRA Regulatory Notice 09-59 (Oct. 2009), https://www.finra.org/sites/default/files/NoticeDocument/p120207.pdf.

[6] FINRA, *supra* note 3.

[7] FIN-2017-A007- Advisory to Financial Institutions Regarding Disaster-Related Fraud (Oct. 31, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf.

[8] SEC, *supra* note 4; CFTC, *supra* note 3.

[9] *See* EBA, *Statement on consumer and payment issues in light of COVID19*, (Mar. 25, 2020), available at https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20provides%20clarity%20to%20banks%20and%20consumers%20on%20the%20application%20of%20the%20prudential%20framework%20in%20light%20of%20COVID-19%20measures/Statement%20on%20consumer%20protection%20and%20payments%20in%20the%20COVID19%20crisis.pdf; EBA, *Key tips to protect yourself when choosing online or mobile banking services* available at https://eba.europa.eu/sites/default/documents/files/document_library/0.%20EBA_Factsheet%20for%20consumers_Final_New_0.pdf

[10] *See* ACPR, AMF, *L'AMF et l'ACPR mettent en garde le public contre les risques d'arnaques dans le contexte de l'épidémie de coronavirus [The AMF and the ACPR warn the public about scams in the context of the coronavirus outbreak]* (Mar. 26, 2020) available at https://acpr.banque-france.fr/sites/default/files/medias/documents/20200326_communique_presse_acpr_amf_vigilance_arnaques_coronavirus.pdf

[11] *See* e.g., *AMF, Market activities continuity during the coronavirus pandemic– the AMF states its expectations*, (Mar. 19, 2020), available at https://www.amf-france.org/en/news-publications/news/market-activities-continuity-during-coronavirus-pandemic-amf-states-its-expectations; ESMA, *ESMA Clarifies Position On Call Taping Under MiFID II* (Mar. 20, 2020), available at https://www.esma.europa.eu/press-news/esma-news/esma-clarifies-position-call-taping-under-mifid-ii.

[12] See Mayer Brown COVID-19 Essential Business Team, *Who or What Is an "Essential" Business or Service That May Be Exempt from Shelter in Place or Stay at Home Orders?* (Mar. 22, 2020), available at https://www.covid19.law/category/financial-regulatory/.

[13] For more information, please see Michael N. Levy et al, *Profiting Off Pandemic: The SEC Issues a Sharp Reminder About Companies' Obligations Regarding Insider Trading and MNPI, Mayer Brown* (Mar. 24, 2020), available at https://www.covid19.law/2020/03/profiting-off-pandemic-the-sec-issues-a-sharp-reminder-about-companies-obligations-regarding-insider-trading-and-mnpi/.

[14] iIn addition, multiple advocacy groups have filed complaints with the DOJ, SEC, and Senate Select Committee on Ethics against senators that sold stock in the weeks before the market crash, alleging

that these senators may have used classified intelligence briefings as stock tips. *See, e.g.,* Citizens for Responsibility and Ethics in Washington, *CREW Files Ethics Complaints Against Burr and Loeffler* (Mar. 20, 2020), available at https://www.citizensforethics.org/press-release/crew-files-ethics-complaints-burr-loeffler/; Common Cause, *DOJ, SEC & Ethics Complaints Filed Against Senators Burr, Feinstein, Loeffler & Inhofe for Possible Insider Trading & STOCK Act Violations* (Mar. 20, 2020), available at https://www.commoncause.org/press-release/doj-sec-ethics-complaints-filed-against-senators-burr-feinstein-loeffler-inhofe-for-possible-insider-trading-stock-act-violations/.

[15] For more information on the cybersecurity risks posed by remote working and reduced staff during the pandemic, see the Mayer Brown COVID-19 Response Team's blog post "Managing Cybersecurity and Privacy Risks Through COVID-19" (Mar. 23, 2020), https://www.covid19.law/2020/03/managing-cybersecurity-and-privacy-risks-through-covid-19/?utm_source=Mayer+Brown+LLP+-+COVID-19+Response+Blog&utm_campaign=660716f4ab-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_ba01bdbc9d-660716f4ab-78806881. See the Department of Homeland Security's March 19, 2020 *Memorandum on Identification of Essential Critical Infrastructure Workers During COVID-19 Response* for more details, available at https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce.

[16] See DOJ, *supra* note 2.