Financial Crime and Cyber Security Concerns in Times of Covid-19

DRAFT

ONLY FOR INPUTS, NOT TO BE QUOTED

Professor Shah Md Ahsan Habib, PhD, BIBM

Maruf Ahmed, President, ISSA Bangladesh

Md Foysal Hasan, Lecturer, BIBM

June, 27, 2020

Information Systems Security Association (ISSA)

Bangladesh Chapter

Segment-1: Criminals and Fraudsters Taking Advantage of Covid-19 Outbreaks and Economic and Financial Sector Disruption

As the Covid-19 pandemic continues[1] with economic destruction and financial disarray and there are growing widespread fears and uncertainties, the criminals are engaged in availing the opportunities[2] by taking advantage of the situation. Fraudsters seek not only to make a profit through exploiting public health issues, but also through spreading misinformation and creating confusion.[3]Financial sector is no exception that has been confronting growing instances of crimes and fraudulent activities in response to the Covid-19 outbreaks. There have been many reports on emerging financial crime risks related to the pandemic, including increased money laundering and cybercrime risk and exploitation of Covid-19 related fund disbursement processes and vulnerable customers (A&L Goodbody, 2020).

Though some policymakers are still searching for right kind of responses for containing the virus, social distancing and reduced mobility came up as the most effective ways till date, and policymakers are also engaged in supporting the economies with essential services. Alongside few others, financial service providers have been very active in maintaining essential services in an environment of unusual information network. As part of combating Covid-19 pandemic, there are constant efforts of exchanging information on the virus and preventive measures; economic and financial implications; and policy interventions. Sometimes, it seems as if there is as much misinformation as there is information, and financial institutions must consider whether they are immunizing themselves for the onslaught of crime designed to take advantage of the confusion (LaPorte, 2020).

In general, the risk of internal fraud increased due to remote working[4] and associated reduced oversight and challenge in banks and financial institutions (KPMG, 2020). While the world adapts to fight the pandemic, launderers are using this time to transfer illicit funds under minimal or no suspicion (Acamstoday, 2020). Due to social distancing measures, online and e-commence transactions increased significantly and seizing this opportunity, fraudsters equipped with the latest technology are perpetrating more sophisticated online transaction frauds and cyber-attacks

[1]As of today (June 22, 2020), there are over 90 lakh reported cases and about 4.7 lakh confirmed death in 215 countries and territories (Worldomer.info).

[2] "Scammers are opportunistic who feed on panic and fear; they command a sense of urgency and panic to extort money" (LaPorte, 2020).

[3] Fake charities; person-in-need scam; fake emails, texts, and phishing; misinformation and rumors, scams offering Covid-19 vaccine, cure, testing; investment scams; ATMs and POS related scams etc. have become wide spread (Bank of Blue Valley, 2020: https://www.bankbv.com/stories/fraud/latest-covid-19-scams).

[4]An estimated 300 million office workers globally may be working from home, including up to 90% of banking workers (Boston Consulting Group website, www.bcg.com; and Risk.net, www.risk.net).

(Covington, 2020). As expected during crisis, banks and financial institutions are also at the risk of confronting increased moral hazard in lending operations - a source of willful default during crisis. Covid-19 is also affecting the capabilities of the regulatory agencies and the banks to enforce anti-money laundering (ALM) and counter terrorist financing (CTF) obligations and measures (FATF, 2020a).

Economic and business disruptions and instability already have notable implications for the banking and financial industry. The crime risk and cyber security concerns became additional burden to the banks, financial institutions, stakeholders and the policy makers. Banks and financial institutions need to have effective risk management procedures and adequate internal control mechanisms to manage their financial crime risks. Practically, it is the duty of all banks and financial institutions to protect customers from the scams that may have remarkable negative implications. Extra-ordinary and innovative approaches might be required to address this sprouting risk in this unprecedented situation of multiple crises.[5]

The objective of this keynote paper is to facilitate an online discussion on the financial crime and cyber security issues that are evolving in the context of the Covid-19 pandemic for identifying right approach (es) and strategy (ies) for banks and financial institutions.

Reports on financial crimes and cyber security issues, scenario analyses, strategic approaches to money laundering, and policy and operational suggestions and forecasting by a number of publications and several scholarly articles have been extensively used to prepare the keynote paper. An opinion survey was conducted with some senior bank executives regarding cyber security and financial crime issues in the context of the country. Financial crimes and cyber security issues might be connected with any sector of an economy; however, the focus of this paper is the financial sector i.e. 'financial crime and cyber security issues associated with the financial sector'. This is a draft paper that attempted to come up with background information, data analyses, and relevant issues for discussion. It would be presented in a Webinar on June 27, 2020; and would be finalized with recommendations based on the discussions and inputs of that event.

Segment-2: Economic and Financial Recessions with Growing Crime and Fraudulent Activities

With the economic recession and rise in unemployment, cases of fraud and criminal activities are expected to rise. Witnessing and analyzing four major crises during last two decades, Deloitte (2020) observed increasing fraud phenomena and huge damages suffered by companies, institutions and states, and for this particular economic turmoil, expectations are not so different.

[5]Published recently in the Harvard Business Review, an article placed the existing and upcoming situation under the broad areas of Real Recession; Policy Recession and Financial Crisis (Carlsson-Szlezak et. al, 2020).

Maintaining the consistent trend, the increase in Covid-19 related crimes such as fraud, cybercrime, exploitation of government funds' distribution process are creating new sources of proceeds for the fraudsters (FATF, 2020b).

Financial scams are among the common news in the media in recent years and the cases are increasing.[6] Financial scams and crimes have become so common that news of email scams, online scams, invoice fraud, cheque and bank draft scams, identify theft, etc. do not surprise us (Habib, et. al, 2018). Rather, a survey by Schaffer (2015), with ever higher dependence on e-banking, mobile payments, and the ability to do banking using social networks, found that risks would continue to menace financial institutions; and hacking attempts, losses, and prevention expenses are likely to increase with rise in mobile banking applications, vulnerabilities of financial call centers, and the increased sophistication of social engineering attacks. Practically, the dangers of cyber-crime have been there for many years; however, the increase in the population connected to the Internet and the time spent online, combined with the sense of anxiety and fear generated from the lockdown, have provided greater opportunities for cybercriminals to take advantage of the situation and has prompted a proliferation of e-crimes (UNICRI, 2020). Media reports and surveys have been coming up with the information of innovative scams.[7]

Even in normal times, there has been a growing recognition and concern of the threat that illicit financial flows pose to the integrity and stability of the global financial system. However, there are increasing evidences or sometimes skepticisms that the problem is growing and scopes are enhancing in the context of the Covid-19 situation (FATF, 2020a). The scale and scope of illicit financial flows could be increasing as authorities are distracted and overwhelmed by the unprecedented economic fallout, which is particularly true in developing countries commonly characterized by poor governance, weak regulatory oversight and relatively high corruption (Rowden, 2020). Observing the developments, several domestic and international regulators and watchdogs have issued warnings on money laundering risks, especially crimes associated with trade based money laundering (TBML) and money laundering associated with electronic payments and fund transfers.

Moral hazard is a common challenge during crisis.[8] During financial crises and uncertainties, certain unethical group of borrowers may take advantage of the situation and may not pay back banks' liabilities willfully. It is true that all Non-Performing Loans (NPL) cannot be tagged with

[6] "The Federal Trade Commission (FTC) recently noted that more than 650,570 cases of identity theft were reported in 2019, accounting for 20.3 percent of the 3.2 million fraud incidents that occurred that year: The most common form of identity theft was credit card fraud, with 270,000 cases reported in 2019. This is more than double the number recorded in 2017 and marked a 72.4 percent increase over 2018's figures" (PYMNTS.com, 2020).

[7] Victims notice deposits of several hundred dollars in their accounts and return the money in good faith, but the funds originally come from stolen credit cards. The scammers send funds to victims using those cards, then link their own to the Venmo account so the "returned" money will go to their own bank accounts (PYMNTS.com, 2020).

[8] Moral hazard mean a party has an incentive to take unusual risks in a desperate attempt to earn money or benefits; moral hazard played a big role during 2008 crisis (Investopedia, 2019).

financial crimes; however, there is growing body of literature that termed willful default as a criminal act (see e.g. Venkatesh, 2016). In the context of a number of banking sectors of developing countries, high percentage of NPLs has been among the key concerns and some of these are clearly the case of asset misappropriation. Though not always, in many instances these are the outcomes of financial frauds or crimes (Venkatesh, 2016; Lele, 2016). A PwC (2016) survey noted, in the context of some developing countries, the board, top management, influential groups and even the regulatory agencies were doing wrong or not doing enough to prevent financial crimes, and thus resulting in moral hazard and willful defaults. Moral hazard in the context of Covid-19 might be a critical source of financial crime if not handled properly.

There is no doubt that Covid-19 crisis accompanied several types and natures of crimes and fraudulent activities. However, cybercrimes, money laundering associated with international trade and electronic payment systems, and risks associated with willful default due to potential moral hazard appear to be particularly critical for the financial and banking sector.

Segment-3: Widespread Evidence of Growing Financial and Cyber Crimes Globally

In spite of notable increase in the use of technology in banks and financial services over the years, comprehensive digitalization of the financing services has remained a distant dream in the developing world. Visible improvements have mainly taken place in the areas of payment facilitation. Even then, money transfers through online wallets and online payments, including e-commerce transactions, were used moderately in most of the developing countries till the Covid-19 outbreaks. However, these have now become one of the feasible and popular ways to conduct transactions due to social distancing measures. Because a large part of the global population is not tech-savvy enough to handle the risks associated with these growing online transactions, they are becoming victims of social engineering and cyber frauds (Covington, 2020). An unprecedented volume of customers are digitally accessing their banks instead of visiting bank branches; and many are using digital banking services for the first time, implying that they may be unaware of personal security best practices which puts them at risk (PYMNTS.com, 2020). People even fall prey to very common types of scams.[9] There are reports[10] of cybercriminals taking advantage of

[9]There are a few common cons: fraudsters might claim a relative or friend is stuck in a foreign country and can only get home if one immediately wires funds to a random bank account; a bogus FBI or IRS list, paying fees will get that victim off the list; there are likely shell companies telling potential victims that they are working to find a virus cure and are just waiting on FDA approval would sell some restricted stock; an institution's brand might be used in an 'alert' to customers stating that their bank account has been temporarily suspended. The victim will receive a link that looks like their bank's login screen, encouraging them to login with their banking username and password. In reality, this screen allows criminals to collect the victim's personal banking information (LaPorte, 2020).

[10]Healthcare providers being attacked by ransomware such as Bitcoin ransomware 'Ryuk', which is wreaking havoc on the already stressed hospital information technology infrastructure and cashing in on the pandemic; cyberattacks on the depleted security systems of organizations due to limited staff presence and unpatched vulnerabilities; launching fake mobile apps, which claim to be providing information on Covid-19, aimed at stealing personal data or even rendering phones unbootable etc.(Acamstoday, 2020).

Covid-19 to scam the vulnerable section of population. Policy interventions and supportive measures of the policy makers have also been widely targeted.[11]

Countries[12] across the globe are reporting an increase in cybercrime during the pandemic. In some instances, quick adoption[13] of digitization resulted in complexities and cyber threats. Cyber-attacks have surged, ranging from phishing attempts to more sophisticated attacks on networks and information flows (KPMG, 2020).Cybercriminals are using malware such as viruses, worms, trojan horses, ransomware and spyware to invade, damage, steal or cancel personal data on personal computers; and stolen data can then be used for different malicious purposes, including accessing bank accounts and blackmailing the victims in exchange of ransoms.[14]Common cybercrime techniques such as phishing[15] have seen a spike and cause of threat for the bank clients and individuals (Europol, 2020). In January, Google registered 149k active phishing websites; in February, that number nearly doubled to 293k; in March, that number increased to 522k - a 350 percent increase since January (Google Report, 2020).[16] The situation in Bangladesh is not different.[17] Banks of the country have concerns on certain service areas[18] and quick adaptation of the technology in the changing situation.[19]

[11]For example, one such scam that is already occurring involves banks' moratorium on equated monthly installments. Borrowers are being contacted by scammers over the phone or by email and are being asked to reschedule a loan as a relief measure; this allows scammers to extract account details and siphon off funds in no time (Acamstoday, 2020).

[12]For instance, in Italy, there are reported scams and frauds that came in the form of ads, emails, fake websites, but also through phone calls and messages (https://www.commissariatodips.it/da-sapere/per-i-cittadini-e-i-ragazzi/internet-rischi-e-minacce/index.html).

[13]The social distancing associated with the economic lockdowns meant that a great deal of in-person vetting of suppliers and hard copies of supply contracts have been shifted online, with many adopting electronic signatures, digitized documents and online payment portals for the first time, often before adequate protection (Rowden, 2020).

[14]https://www.ilmessaggero.it/italia/coronavirus_reati_truffe_online_ultime_notizie-5111692.html

[15]Phishing is the fraudulent practice of inducing individuals to reveal personal information, such as passwords and credit card numbers through fake websites or emails.

[16]Data gathered by Google and analyzed by Atlas VPN: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine/

[17] Bankers of Bangladesh identified phishing and spear phishing; social engineering; spam attack; DoS and DDoS attack; DNS attack, ransomware as the major types (Survey data).

[18] Customer's personally identifiable information (PII) may be stolen which would be very costly; risks associated with mobile apps are considered higher (Survey data).

[19] Due to huge number of bank's head office employees have no other way but to conduct office activities from home, it heightened dependency on exposed internet which causes risk of data breach; business meetings are conducted by using free tools/software (like zoom) and sharing valuable documents which may help fraudsters to conduct malicious activities (survey data).

Adoption of information technology without adequate preparation in the changed environment have created greater scopes for money laundering schemes (Asian Banking and Finance, 2020)[20]. Most of the leading regulators and several law enforcing agencies[21] have warned banks and financial institutions to be vigilant about any such situation (Kosnar, 2020). Reporting from FATF members, observers, and open sources indicates that criminals have attempted to profit from the Covid-19 pandemic through increased fraudulent activities associated with international trade (FATF, 2020). World Customs Organization (WCO) warned[22] and asked to exercise extreme caution when purchasing critical medical supplies from unknown sources, particularly online. There was a significant increase in seizures of counterfeit and unauthorized face masks and hand sanitizers during a collaborative enforcement effort by the WCO, Interpol, Europol, customs administrations, police forces and other law enforcement agencies. A series of operations, held from 3 to 10 March 2020, resulted in the seizure of 37,258 counterfeit medical devices, of which 34,137 were surgical masks (WCO, 2020).In the face of extraordinary demand for medicines and equipment to help contain the spread of the virus, many companies have struggled to identify legitimate suppliers. In one example, Europol (2020) investigated a transfer of 6.6 million euros from a European company to a supplier in Singapore selling alcohol gels and protective masks; the goods were allegedly never received. In another case, it was reported that an attempted purchase of 3.85 million masks resulted in a loss of 300,000 euros by an organization that also fell victim to a supply scam (Refinitive, 2020). These threats and vulnerabilities represent emerging money laundering and terrorist financing risks (FATF, 2020b).[23]

Europe's top banking regulator, EBA, asked banks to take additional measures while processing payments linked to trade transactions to establish whether unexpected flows particularly linked to customers or regions badly affected by the virus are of legitimate origin (GTR, 2020). TBML is especially vulnerable in this crisis as a result of unusual hyper fluctuation of markets as well as the prices of goods and commodities (ADS, 2020). Trade linked to medical supplies is already proving a fraud hotspot, and there is also an issue in global trade financing or passing invoices for medical supplies that are at over-inflated prices (ACAMS Today, 2020).

[20]For example, "so called 'money mule' activity is already identified as rapidly increasing, and criminals have been targeting individuals who might have lost their jobs recently with 'large salary working from home' job ads. These are designed to trick victims into using their personal bank accounts to funnel money illicitly obtained by criminals". (Asian Banking and Finance, 2020).

[21] Interpol and FBI warn of financial and frauds linked to Covid-19.

[22]Customs and law enforcement agencies in China, Germany, Indonesia, Uganda, Ukraine, United Kingdom, United States and Vietnam, to name but a few, have reported such seizures in March 2020 (WCO, 2020).

[23]"Criminals finding ways to bypass customer due diligence measures; Increased misuse of online financial services and virtual assets to move and conceal illicit funds; Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds; Increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds; Misuse and misappropriation of domestic and international financial aid and emergency funding; Criminals and terrorists exploiting Covid-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries" (FATF, 2020b).

There are indications[24]that massive levels of illicit financial flows[25] are going undetected through the global trading system (Rowden, 2020). GFI Report (2020) is particularly concerned with their impacts for developing countries, as things are projected to get worse for developing countries in the Covid-19 regime. According to Rowden (2020), even in normal times there have been common trends of trade mis-invoicing and other types of illicit financial flows to move wealth from low income to high income economies; and in the wake of the Covid-19 crisis, all of these dynamics are intensifying. Unemployment of migrant workers has resulted in fall in remittance inflows in a number of manpower exporting countries; and in some instances, even food insecurity and unemployment of a section of workers living abroad are also said to be a contributory factor for illicit fund flows from manpower exporting country to their host countries.

Digital payments are growing[26]rapidly and increased digital payment and money laundering using technology has close association. For handling associated challenges, the growth in digital financial transaction requires a better understanding of how individuals are being identified and verified in the world of digital financial services (FATF, 2020a). However, quick adaption of digital payments in the Covid-19 scenario has become a challenge for understanding the dynamics and sometimes contributing to money laundering. Banks and financial institutions have recommended clients to conduct their transactions through non face-to-face instruments, which are inherently considered risky. In addition, migrant workers may resort to illegal fund transfer using online and mobile payment. ‘‘Therefore, if loopholes had not been found and addressed earlier (subject of Recommendation 15 of the Financial Action Task Force on New Technology), problems could arise. The irony is that the mitigation process for threats also relies on technology, like the efficient technology-based KYC-CDD procedures applied by financial institutions” (Finance Tribune, 2020).

Bank itself might be within the alleged money laundering circle when these financial institutions commonly face liquidity crunch and unusual business disruption. For overcoming the challenges, there might also be desperation on the part of banks and financial institutions.[27] Thus, banks might

[24]Global Financial Integrity (GFI) recently released its newest report (March, 2020), ‘Trade-Related Illicit Financial Flows in 135 Developing Countries: 2008-2017’, finding value gaps in reported international trade of a staggering USD8.7 trillion over the ten-year period, 2008-2017, and a gap of USD 817.6 billion in 2017 alone. The report also found high incidences of trade mis-invoicing as a percent of total trade (https://gfintegrity.org/new-gfi-report).

[25] Illicit fund flows, one associated area of TBML, are mainly accomplished mainly using trade mis-invoicing, tax evasion and the criminal smuggling of cash.

[26]Digital payment is increasing at an estimated 12.7% annually, and by 2022, an estimated 60 percent of world GDP would be digitalized (FATF, 2020b).

[27] The 2008 financial crisis is a good reference point when, former United Nations Office of Drugs and Crime Executive Director Antonio Maria Costa warned that ‘stupid and diabolic’ bank behavior as a result of the financial crisis allowed transnational mafia drug money to enter the financial system, estimated then at USD320 billion annually. ‘With the financial crisis, banks became desperate for cash, and one of the few sources of liquidity these days is the transnational mafia,” he claimed, based on intelligence from several jurisdictions (OCCR, 2020).

be vulnerable at this point and there may be 'classic' money laundering risks emerging as a result of Covid-19.

In this Covid-19 situation, borrowers may be exploiting moral hazard[28] to privatize the reward and socialize the risk. Moral hazard problem also relevant for bankers and may contribute in pulling credit risk. Policymakers around the world are using banking channel to help distribute various stimulus packages to companies in need of cash injection where fraud and credit risk might be critical challenges. In the changing circumstance, companies are facing cash crunch and sometimes are not in a position to pay back bank loans. In the process of the cash injection process, a minority of unscrupulous business owners may be tempted to capitalize on the support available and default on payments. It is not easy for banking institutions to distinguish between those that are actually in need of assistance and show propensity to recover and those that are trying to abuse the situation or simply fabricate information to get access to funds (Asian Banking and Finance, 2020).

With stimulus packages rolling out in most countries, corporate behaviors cannot come under comprehensive check; and there is a possibility that large businesses would be favored over small businesses. "Today some of the wealthiest people made their money by borrowing from the banks to buy their own company shares in order to inflate its price; and following this they then sold their shares for a profit on the market. Now some of them are asking for bailouts as their company starts to struggle to survive". Supporting criminal may even be more harmful for the economy (Econfix, 2020).

Segment-4: Global Measures and Initiatives to Identify and Address the Challenges- Regulatory and Policy Responses

Since the beginning of the Covid-19 destruction, there have been extensive highlights on increased risks around growing cybercrimes, frauds, fraudulent buying-selling, using trading of medical supplies for TBML, escalating illicit fund flows and social engineering scams. Against this backdrop, regulators, international bodies and organization, law enforcing agencies[29] and several other stallholders have provided warnings, alerts, directions and guidance on their expectations in managing financial crime risk and the associated fraudulent activities.

In the area of cybercrimes, cyber security experts and voluntary groups are mobilizing globally to provide threat intelligence and combat these attacks, and according to KPMG (2020), more than

[28] Nobel Prize winning economist Paul Krugman defined moral hazard as 'any situation in which one person makes the decision about how much risk to take, while someone else bears the cost if things go badly'.

[29] Interpol has also reported a rise in the number of websites selling fake protective products, including face masks, sub-standard hand sanitizers and unauthorized anti-viral medication; as many businesses adopt virtual working environments or permit new connections to their systems, the FBI has been alerted to an increase in the number of criminals trying to steal personal and intellectual property information (Refinitive, 2020).

ever, firms would need to shore up their cyber defenses and educate employees, at all levels. UK National Crime Agency has warned of an increase in spear-phishing attacks, and noted that organized criminals were using malicious mobile applications and websites to exploit the pandemic. FinCEN (2020) advised financial institutions to remain alert for schemes that seek to profit from the current crisis, noting a number of emerging trends.[30] FATF (2020a) very recently highlights the innovative ways in which financial institutions can deliver digital financial services and managing risks. As some employees are working from home[31], banks must undertake educative and informative programs to ensure that employees maintain sound cyber and information security practices (Freshfield, 2020). 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 efforts on staff training and awareness (Crisnato and Prenio, 2020). Campaign to educate customer is very essential at this vulnerable scenario.[32]

Central banks and regulatory authorities have become very active to emphasize the importance of maintaining effective systems and controls to ensure that the financial system is not abused for money laundering or terrorist financing purposes.[33]The European Banking Authority (EBA) issued a statement on actions to mitigate financial crimes during the Covid-19 pandemic, calling on competent authorities to support credit and financial institutions' ongoing AML/CFT efforts. Competent authorities are requested by the EBA to: "make clear that financial crime remains unacceptable even during the pandemic; continue to share information on emerging AML/CFT risks; set clear expectations on the steps financial institutions should take to mitigate those risks; consider how to adapt their supervisory tools to ensure ongoing compliance by credit and financial institutions with their AML/CFT obligations" (EBA, 2020a).

It is well recognized that KYC (Know your Customer), CDD (Customer due diligence) and right red flags are crucial to handle money laundering risks in any situation. Already there are concerns and suggestions for greater scrutiny surveillance using newer red flags.[34]FATF issued 'Digital ID'

[30] "Like bad actors who pose as government officials to solicit donations, steal personal information, or distribute malware; investment scams involving false claims that products or services can prevent, detect, or cure the coronavirus; the sale of misbranded products that make unfounded health claims; and insider trading".

[31]As the huge jump in the number of staff at all levels of a bank needing remote access has created an initial challenge, like some staff may have lacked the hardware or software needed to access the bank's Virtual Private Network (VPN), leading to IT teams loosening some controls in the short term (KPMG, 2020).

[32]Several banks in the UK-including Barclays, HSBC, Lloyds Banking Group and Royal Bank of Scotland - have launched social media campaigns to educate customers about warning signs like unexpected password or personal banking information requests (PYMNTS.com, 2020).

[33]For example, the Central Bank of Ireland emphasizes that firms should remain up to date on the changing AML/CFT techniques and how they might change due to an economic downturn; this will involve in particular reviewing and, if necessary, updating AML/CFT risk assessments and transaction monitoring processes; paying particular attention to changing spending patterns, funds flows and a migration to online payments (A & L Goodbody, 2020).

[34] Red flags may include: recently incorporated companies with no or little track record in supplying medical or pharmaceutical products exporting; companies having a track record in supplying medical or pharmaceutical products

to assist governments, regulated entities and other relevant stakeholders in determining how digital ID systems can be used to conduct certain elements of CDD. In the digital ID context, the requirement that digital "source documents, data or information" must be "reliable", "independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results. The guidance clarifies that "non-face-to-face customer-identification and transactions that rely on reliable and independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk"(FATF, 2020a).

Operational efficiency, control and initiatives by the banks and financial institutions are at the core of handling credit related moral hazard and potential willful default scenario in the context of the Covid-19. However, regulatory and prudential guidelines might be useful to undertake due initiatives and approaches by the banks and financial institutions in the process of handling credit operations. EBA suggested measures to address the adverse systemic economic impact of the Covid-19 pandemic in the form of a general moratorium, payment holidays stemming from public measures or industry-wide payment relief initiatives taken by banks and financial institutions. In a statement on the application of the prudential framework regarding default and forbearance in light of Covid-19 measures, EBA (2020b) suggests that "in the process of moratoria or determining the modified schedule of payments or credit assessment for potentials borrowers, individual assessments should be done in a careful manner, which does not entail any automatism in the classification; and should institutions face a substantial number of individual assessments, they should prioritize the analysis, using their risk-based approach." "Initial assessment should focus on those individual exposures most likely to have had a significant impact and can initially be done at the portfolio level, if need be. Any assessment will furthermore need to be done on a consistent basis based on reliable information." And for the purposes of supervisory reporting, as suggested by EBA, the definition of forbearance is designed to be reported when banks offer specific measures to help a specific borrower who is experiencing or likely to experience temporary financial difficulties with their repayment obligations.

For handling financial crime, regulatory and policy approach may not be very concrete or certain. In the wake of the Covid-19 situation, on the one side, there are growing concerns of misusing digital, market and trade transactions that demand tough and stringent measures; while on the other side certain transactions and activities need smoothness and relaxation to address exiting health

where there has been a recent change in the controlling structure and where the said controlling structure cannot be properly identified or appear unusually complex; a company shipping medical and/or pharmaceutical products to a country and there is no planned cargo flight or vessel in the specified shipping period/route; trade documents that include vague description of the goods and/or their nature; price of goods and/or shipment that appear manifestly or abnormally high; and a company receiving shipment of medical and/or pharmaceutical products has no economic or lawful justification for this transaction (ADS, 2020).

and economic challenges.[35] Thus, in spite of adequate symptoms of the growing financial crimes and warnings on the part of the national authorities[36], some of the necessary policy interventions have contributed in the escalation of crime risks[37]. On the one side, international organizations have asked to undertake utmost care in financial facilitation and sought to unify the global approach against financial crime and also address sanctions, money laundering and terrorist financing concerns during the pandemic; and on the other side, there are guidance on digital onboarding and simplification of due-diligence procedures. For example, while it is logical to encourage the use of digital payment platforms by raising limits on mobile money transactions; this might be luring for the fraudsters. As in many other global economies, the Bangladesh Financial Intelligence Unit (BFIU) issued instructions for relaxed and smooth delivery of stimulus packages for much needed quick economic recovery, while on the other hand, it issued warning to the banks to be alert on the potential risks of financial crime. The recent declaration of the government of Bangladesh regarding 50 percent penalty reflects the country's concern on falsification of invoicing. Practically, identifying a balanced-stand and installing risk based approach are challenging tasks for the policy makers at this situation.

Segment-5: Identifying Approaches and Preparedness of banks and financial institutions to handle financial crimes and Cyber Security Concerns

Adopting right kind of approach, close monitoring and preparedness measures are crucial at this unprecedented and difficult time, though it is not easy to follow stringent measures in facilitating certain transactions associated with health[38] and other emergency services. The fear and chaos caused by the pandemic has provided a very good platform for launderers and fraudsters to flourish until banks and financial institutions develop a defense mechanism (Acamastoday, 2020). To address the financial risks in this covid-19 situation, a combination of trusted data and a risk-based

[35]FATF statement also reminds financial institutions to use a risk-based approach to ensure that legitimate non-profit relief work is not hampered so that aid can be delivered to its intended recipients (A & L Goodbody, 2020).

[36]For example, several USA agencies have warned of financial crimes associated with Covid-19; UK National Crime Agency has warned of an increase in spear-phishing attacks, and noted that organized criminals were using malicious mobile applications and websites to exploit the pandemic; Canada's Financial Transactions and Reports Analysis Centre has instructed banks to focus more on flagging and reporting suspicious activity during the crisis (Moneylaudneirng.com).

[37]EBA issued a statement emphasizing the need for a flexible approach to anti-money laundering and counterterrorist financing supervision for certain situation. Asian regulators have focused on balancing the need for commercial efficiency with the need to address a heightened risk of financial crime. The Philippines relaxed certain regulatory obligations related to AML and know-your-customer requirements. Regulators in Australia and New Zealand underscored their expectations that financial institutions continue to meet their AML and counterterrorist financing obligations, especially those pertaining to the monitoring of suspicious transactions, but also relaxed reporting deadlines and KYC requirements. Securities and Exchange Board of India focused on easing access to funds while noting the need for vigilant cybersecurity measures (Moneylaundering.com)

[38]The mean percentage of companies in the healthcare sector carrying out due diligence at only 50%, which is 7% below the total for all sectors surveyed in a newly released report by Refinitive (Refinitive, 2020).

approach would be needed (Refinitive, 2020). For banks and financial institutions this risk may be transformed into an opportunity by undertaking right approaches and measures.[39]

Despite emergency and funding need, compromising with KYC and CDD may be expensive. Banks and financial institutions need to ensure effective risk procedures, strong communication, due compliances and adequate internal control mechanisms to manage their financial crime risk at this unprecedented time.[40] Control and surveillance by the banks and financial institutions at all levels is necessary for ensuring market and transaction level integrity.[41]Undated information and identification of red flags are essential to handle the ongoing challenges. Training of the staff and collaboration is a necessity.[42] It is important to understand that these crimes are not just a nuisance to customers; rather, these are going to affect profits and reputations of banks and financial institutions.

On the way to address the situation, solutions of financial crime and cyber threats are coming up, using risk-based approach and extensive use of information technology. The FATF is encouraging "the fullest possible use of responsible digital customer onboarding and delivery of digital financial services" during the crisis. FATF (2020b) suggested for "domestic coordination to assess the impact of Covid-19 on AML/CFT risks and systems; strengthened communication with the private sector; encouraging the full use of a risk-based approach to customer due diligence; and supporting electronic and digital payment options" as strategy to handle financial crime risks by banks and financial institutions. Information sharing and collaboration have been suggested commonly in several solution frameworks. For addressing the challenge of illicit capital flows, more support is needed in many developing countries in the form of improved interagency collaboration between financial intelligence units, customs agencies, law enforcement and anti-corruption commissions (Rowden, 2020). Driving on technology based solutions, Poole (2020) recommended for realignments[43] that include strengthening suspicious activity report investigation and enhancing

[39]"Banks and financial institutions have been faced with the compelling need to move work operations online, and while this presents a unique opportunity to explore the digital onboarding of clients, trusted and secure solutions must be adopted in order avoid cyber security threats and identity fraud" (Acamastoday, 2020).

[40]"Unprecedented times call for innovative solutions, and looking at improving the communication channels between AML and fraud to provide vital intelligence could prove hugely beneficial in tackling the increase in crime during these challenging times" (PwC, 2020).

[41]"It is warranted for financial institutions to deploy strict transaction and communications surveillance to safeguard market integrity" (Levy, 2020).

[42]"It is also helpful to train staff and customers to maintain healthy skepticism surrounding new companies addressing the pandemic; partnering up and networking are another essential issues to address" (LaPorte, 2020).

[43]As most client interactions for banking are now happening through online channels, anti-money laundering (AML) procedures need to be changed. The risk perception of banks should also be changed accordingly as bad actors will introduce newer forms of suspicious activities into the system.

automation[44]; fine-tuning adverse media screening[45]; new scenario building for transaction monitoring[46]; stricter Insider-trading detection through AI-based models[47];finding newer acceptable ways to perform KYC updates[48]; enriching fraud scenarios with the latest event information[49]; and deploying adequate staff for handling cyber threat[50]. Technology focused solution and artificial intelligence (AI)[51] probably is the right approach for the banking strategy in the corona regime. Some of these suggested measures seem to be very sophisticated that involve major transformation and costs. Such major changes may not be a short term option for most of the banks and financial institutions of the developing countries; however, those would be useful from a long term perspective. And, the reality is "digital transformation will not regress or slow once the pandemic is under control; and financial institutions and other businesses that are required to meet AML/CFT compliance requirements cannot afford to ignore this trend" (Accuity, 2020).

Based on the scenario analyses and suggestions, banks and financial institutions need to identify broad areas (box-5.1) to handle existing crime and cyber security concerns. Management approach for addressing the ongoing scenario would need special risk approach, and adjustment and accommodation (box-5.2).

[44] "It is time to work hard to introduce cognitive robotic process automation based solution." (Poole, 2020)

[45] "With Covid-19 introducing new sets of financial crime typologies, FIs face increased false positive alerts as well as true positive misses. Therefore, FIs need to review their media screening and introduce necessary changes to stay effective. In short, FIs must redefine screening typologies for drawing insights" (Poole, 2020)

[46] "Banks need to review TM scenarios and introduce artificial intelligence (AI)-based detection wherever possible to take care of any new anomalies or pattern changes automatically."(Poole, 2020)

[47]"A more rigorous trader and employee communication surveillance."(Poole, 2020)

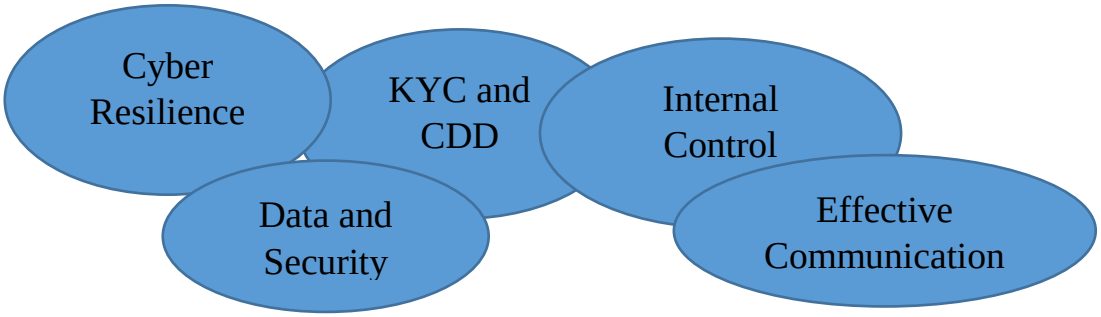
[48] "FIs need to develop a robust mechanism using unconventional channels wherever possible, such as online data collection for collecting customer data."(Poole, 2020)

[49] "As newer forms of frauds are gaining prominence, FIs need to enrich their fraud event repository so Covid-19-induced frauds are not missed; AI-based detection models will be quite handy for making unsupervised adjustments in flawed indicators."(Poole, 2020)

[50] "Cybersecurity and data breach prevention are nonnegotiable under all circumstances. Any frugality in terms of staffing this function will only attract hefty financial and reputational losses. Therefore, IT support should receive top staffing priority". (Poole, 2020)

[51]"AI-powered AML systems provide many advantages over an existing rule-based system. This includes being able to dramatically reduce false positives. The AI technology can be strategically placed between the AML rule-based system and the investigator, which allows companies to gain a rapid return of investment. Overall, the average investigation time is dramatically reduced from between 45 to 90 days, to seconds" (Global Banking and Finance Review, June 2020).

Box 5.1: Key Broad areas to be Targeted to handle Financial Crime and Cyber Security Concerns



Box5.2: Preparedness Measures to Handle Financial Crime and Cyber Attacks

Enterprise Risk Management Framework for Review and Adjustment

Reviewing Risks	✓ Identifying high risk customer segment ✓ Minimizing asymmetric information with customer ✓ Real time customer profiling behavioral analysis ✓ Familiarizing new fraud typologies on financial crimes
Reviewing Systems	✓ Fine-tuning to adverse media screening ✓ New scenarios and model building for screening ✓ Advanced analytics to monitor complex transactions ✓ Installing strategic Communication Network
Reviewing Compliance	✓ Compliance capabilities for Covid-19 related regulations ✓ Quick adjustment mechanism with policy intervention ✓ Reviewing Internal Compliance System for adjustment ✓ Strengthening SAR Investigation and Reporting
Reviewing Control	✓ Introducing dynamic and responsive control ✓ Improving regulatory compliance and governance ✓ Introducing stricter employee and borrower surveillance ✓ Integrating board with crime resolution process

Note: Authors' preparation (draws heavily on Acamstoday, 2020).

As measure and risk-based approach, the banking industry should rely on the integrated approach i.e. Enterprise Risk Management (ERM)[52] where board and top management have critical role to

[52].....is a structured approach that aligns strategy, processes, people, technology and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces; it is a forward looking approach to manage all key business risks and opportunities (Deloach, 2000).

play to handle crime and security risk management efforts in this crisis situation.[53]Four key areas should strongly come under review: risks; systems, compliance, and controls.

It is crucial that banks must outline internal vulnerability associated with the systems and products. Based on a bank's business model, where do points of entry for fraudsters and criminals exist? What segments of customers are particularly vulnerable to falling victim to scammers? Financial institutions must build controls around the vulnerabilities in their models.

Economic stimulus packages are targeted mainly for the affected clients of banks and financial institutions, and clients having financial strength and who are unaffected should not be facilitated. What strategies might work to attain that? Strategic communications are critical for addressing moral hazard problems associated with these facilitation that might cost credit quality of banks. It is important to identify what kind of feasible strategy and communication network would help handling credit risk and moral hazard challenges in this situation?

Is internal control mechanism of the bank responding to the emerging financial crimes? What are the areas- products and clients, where the banks need to heighten due diligence? Is the changing and evolving compliance and transaction monitoring under control of the management? Regardless of the strategy, it is important to stay compliant. Should the banks need extra care with customers who claim to have additional cash flows due to the pandemic?

Banks' employees must be updated with correct and valuable information, and kept away from misinformation and confusion. This might be part of strategic communication of banks. Training, education and awareness are critical at this moment. What are the critical information that the customers and employees need to protect themselves and the system from the fraudsters? Partnering with key agencies and professionals would be helpful to draw best possible practices and undertake counter measures against financial crime and cyber security concerns.

Alongside identifying crime risks, the time has come to gear up for the institutionalization of the changes and adjustments to attain both short-term and long term goals for handling financial crimes. Some technology adoption and digitization are very much possible as part of the ongoing adjustment process. However, ultimately it is about digitalization that may help transforming the financial crime and efficiency dynamics of banks and financial institutions. Adoption of technology might be the sources of several financial crime risks; however, embracing the technology can beget the best solution for handling financial crime by the banks and financial institutions.

[53] In spite of the importance of ERM that received renewed focus following the 2006-08 global financial crisis, it did not receive due impetus with its integrated and preparedness approach in banks; Global Risk Report 2019 explained why ERM should be the future of banks! (World Economic Forum, 2019).

References

A & L Goodbody (2020) COVID-19: Financial Crime Risk – Regulatory expectations: https://www.algoodbody.com/insights-publications/covid-19-financial-crime-risk-regulatory-expectations

Acamstoday (2020) COVID-19: The Lurking Financial Crime Threat for FIs, JUNE 3, 2020: https://www.acamstoday.org/covid-19-the-lurking-financial-crime-threat-for-fis/

Accuity (2020) How COVID-19 is Changing KYC and AML Technology in APAC: https://accuity.com/accuity-insights-blog/how-covid19-is-changing-kyc-and-aml-technology-in-apac/

ADS (2020) AML/CFT Risks during COVID-19 – Trade Based Money Laundering 15 April 2020 https://www.ads.mu/article/aml-cft-risks-during-covid-19-trade-based-money-laundering/

Asian Banking and Finance (2020) COVID-19 and the implications for fraud, credit risk and money laundering, APR 29, 2020: https://asianbankingandfinance.net/solution-center/protecting-and-defending-financial-institutions-financial-crime-and-cyber-attacks/co

Covington (2020) "FinCEN Issues COVID-19-Related Guidance on SAR Filings, Heightened Risk of Disaster Fraud," Covington, March 16, 2020, https://www.covfinancialservices.com

Crijantor, Juan Carlos and JermiPrenio (2020) Financial Crimes in Times of Covid-19: AML and Cyber Resilience Measures, FSI Brief, No-7, Financial Stability Institute, May, FSI.

Carlsson-Szlezak, Philipp, Martin Reeves and Paul Swartz (2020) What Coronavirus Could Mean for the Global Economy, Harvard Business Review, March 2020, Published on HBR, ORG.

Deloitte (2020) Banking fraud, AML and KYC compliance in the era of COVID-19 23 April 2020: https://www2.deloitte.com/ro/en/pages/business-continuity/articles

Deloach, J.W. (2000) Enterprise-Wide Risk Management: Strategies for Linking Risk and Opportunity, Financial Times/Prentice Hall, London

EBA (2020) "EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic," European Banking Authority, March 31, 2020, file:///C:/Users/d40831837/

EBA (2020a) EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic, March 31: https://www.cmvm.pt/pt/Comunicados/Comunicados/Documents/EBA

EBA (2020b) Statement on the application of the prudential framework regarding Default, Forbearance and IFRS9 in light of COVID19 measures, March 25: https://eba.europa.eu/sites/default

Econfix (2020) Moral Hazard and Covid-19: https://blog.elearneconomics.com/moral-hazard-and-covid-19/

Europol (2020) European Union Terrorism Situation and Trend Report 2020, June: https://www.europol.europa.eu/activities-services/main-reports

FATF (2020a) Digital Identity, March: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

FATF (2020b) Covid-19-related Money Laundering and Terrorist Financing Risks and Policy Responses, May: https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

Finance Tribune (2020) Perspective: Coronavirus and Money Laundering Concerns: https://financialtribune.com/articles/business-and-markets/102791/perspective-coronavirus-and-money-laundering-concerns

FinCen (2020) Concerns related to the Coronavirus Disease and to Remain Alert to Related Illicit Financial Activity: https://www.fincen.gov/news/news-releases/financial-crimes-enforcement

Freshfields Bruckhaus Derringer (2020) COVID-19 and Compliance Risks for Financial Institutions: http://knowledge.freshfields.com/en/Global/r/4167/covid-19_and_compliance_risks

Global Banking and Finance Review (2020), How artificial intelligence technology can prevent money laundering during covid-19: https://www.globalbankingandfinance.com/how-artificial-intelligence-technology-can-prevent-money-laundering-during-covid-19/

GTR or Global Tarde Review (2020) Regulators issue money laundering warning as criminals adapt to Covid-19 / 01-04-20 / by John Basquill: https://www.gtreview.com/news/europe/regulators-issue-money-laundering-warning-as-criminals-adapt-to-covid-19/

Investopedia (2020) How did moral hazard contribute to the 2008 financial crisis?:https://www.investopedia.com/ask/answers/050515/how-did-moral-hazard-contribute-financial-crisis-2008.asp

Kosnar, Michael (2020) "FBI warns of 'money mule' schemes exploiting COVID-19 pandemic," NBC News, April 9, 2020, https://www.nbcnews.com/news/us-news/fbi-warns-money-mule-schemes-exploiting-covid-19-pandemic-n1180581

KPMG (2020) Covid-19 Insight-Emerging Risks: https://home.kpmg/xx/en/home/insights/2020/04/covid-19-insights-emerging-risks.html

Levy, Michael N. Richard M. Rosenfeld and Matthew Rossi, "Profiting off Pandemic: The SEC Issues a Sharp Reminder About Companies', March 24, 2020, https://www.covid19.law/2020/03/

Moneylaundering.com-Silas Bartels, Larissa Bernardes, Laura Cruz and LeilyFaridzadeh (2020) Legal Brief: Global Financial Community Acts Against COVID-19, April 15, 2020: https://www.moneylaundering.com/news/legal-brief-global-financial-community-acts-against-covid-19/

Organized Crime and Corruption Reporting (OCCR) Project, "Financial Crisis Benefits Crime," March 20, 2009, https://www.occrp.org/index.php/en/ccwatch/cc-watch-indepth/239-financial-crisis-benefits-crime.

Poole, Ben (2020) "EBA seeking to mitigate financial crime risks during COVID-19," CTMfile, April 2, 2020, https://ctmfile.com/story/eba-seeking-to-mitigate-financial-crime-risks-during-covid-19

PwC (2020) Covid-19: Increased financial crime risk, Man 11 May, 2020: https://www.pwc.com/im/en/media-room/insights/covid-19-financial-crime-risk.html

PYMNTS.com (2020) Preventing Financial Crime-Playbook, May: https://www.pymnts.com/fraud-prevention/2020/preventing-financial-crime-covid-19-pandemic/

Refinitive (2020) The Covid-19 financial crime risks: https://www.refinitiv.com/perspectives/financial-crime/the-covid-19-financial-crime-risks/

Rowden, Rick (2020) Covid-19 and Illicit Financial Flows: What's to Come, May 6, 2020: https://gfintegrity.org/covid-19-and-illicit-financial-flows-whats-to-come/

Security Intelligence (2020) Cyber Security in the Wake of Covid-19: https://securityintelligence.com/how-cybercriminals-use-money-mule-accounts-to-profit-from-online-fraud/

UNICRI (2020) Cyber-crime during the COVID-19 Pandemic,Turin, 11 May 2020. byAdilRadoini: http://www.unicri.it/news/article/covid19_cyber_crime

World Economic Forum (2019) Global Risk Report 2019: https://www.weforum.org/agenda/2019/11/why-enterprise-risk-management-is-the-future-for-banks/

WCO (2020) Covid-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment, March 23: http://www.wcoomd.org/en