



# Expected Changes in AML After COVID-19



E-Book



# Contents

Introduction.....	3
Ahsan Habib.....	4
Amlan Das.....	6
Andres Betancourt.....	8
Branka van der Linden.....	10
Ehi Eric Esoimeme.....	13
Gürcan Avcı.....	15
Imad Habre.....	17
Plamen Georgiev.....	19
Rezaul Karim .....	20
Sholane Sathu.....	22
Tarık Tombul.....	23

**Disclaimer:** "All articles published in this e-book are solely the authors' own opinions and do not reflect the official policy of the institutions they work for."

**\*Articles and authors are listed alphabetically.**

# Introduction



**Fatih Coskun**

Ceo at Sanction Scanner

**Dear Financial Crime Fighters,**

We are going through challenging days all over the world. It is our greatest wish that everything will return to normal quickly. For evil people, this type of crisis times is a blessing. Financial crimes can increase with coronavirus. When we examine the reports on attacks such as money laundering, counterfeiting, and phishing, these crime transactions have increased recently by using communication methods on coronavirus.

The current coronavirus pandemic (COVID-19) has created different challenges for the authorities in charge of Money Laundering and the Financing of Terrorism (ML/FT).

As usual, all companies must strive in the prevention and detection of these risks in a timely manner and carry out an analysis of the new ML / TF risks derived from the COVID-19 crisis.

In this e-book project, we have compiled the views of AML experts from all over the world about the "Expected Changes in the AML after COVID-19". As the Sanction Scanner, we wish to overcome the COVID-19 outbreak as soon as possible. We are ready to make sacrifices to support all parties that related AML during and after this pandemic. Do not hesitate to contact us.

Best Regards



## Ahsan Habib

Analyst, AML Quality Assurance at Scotiabank

### **Changes in CDD procedure may be the ‘new normal’ :**

As Coronavirus continues to disrupt business activity and social distancing becomes widespread, compliance professionals may have concerns over how this will impact their ability to comply with the money laundering regulations in a post-COVID world. From an AML and anti-fraud perspective, the COVID-19 pandemic and the related government lockdown of a broad range of business activity is unique because it is a health crisis creating a change in economic behavior across the globe.

Even when the crisis will be over, there may be situations where the business line professionals will not be able to meet their clients in person because the work arrangements in bank branches will not likely be the same as it was in the pre-COVID world. As we know, the three stages of Customer Due Diligence (CDD) are client identification (information gathering), risk assessment and verification (evidence gathering), any inability to meet the client face to face may impact a financial institution's ability to conduct an effective client risk assessment. This may lead to increased levels of caution, and Simplified CDD will be likely to continue.

Financial institutions will be in a dilemma as they need to onboard clients, get more business to get back on track after Q1 or Q2 (First/Second Quarter) subdued/frustrating performance and at the same time clients may not be willing to visit bank premises in person as they did before (in fear or due to drastic change in their financial capacity). Thus client screening and certified e-identification databases can be used, adverse media searches undertaken, and video-conferencing facilities deployed so that prospective client are still met. Take an example of document verification, using a camera on a high-end smartphone. It is possible to identify compromised, altered easily, or fake documents, as compared to an eyeball test in a branch.



Combine that with some of the anti-impersonation and anti-fraud tools that can be deployed, and you can have a very robust identity verification done remotely, along with real-time screening for regulatory risk against a database like. A risk-based approach will be adapted by Financial Institutions to conduct CDD, allowing the discretion to not necessarily sight certain documents in certain circumstances, depending on the reporting entity's assessment of ML/FT risk. As the situation evolves, we may expect to see a shift in focus and a re-prioritization of operational and conduct risks as Financial Institutions may come to terms with managing dispersed workforces.

**Recommended actions as a part of CDD :**

Financial institutions should refrain from relying entirely on automated processes to onboard customers. They should also take steps to understand the activity within 30 days of entering into a new relationship and continually reevaluate the kind of information they collect at any point in time. If needed, FIs may do periodic reviews on apparently high-risk clients in the increments of 60 days and make sure who is behind the wheel (Ultimate Beneficial Owner).

**Increased focus on cyber-hygiene and transaction laundering:**

More than ever, corporate offices will focus on their cyber hygiene, shore up their cyber defenses, and educate employees, at all levels, to the emerging risks. Bank financial crimes compliance professionals will be expected to remain cautious of business customers whose banking activity remained unchanged during the COVID-19 crisis and whose transaction patterns remain unchanged. For example, a restaurant that had little cash activity and normally receives mainly deposits averaging \$5,000 per week as their main source of revenue in the pre-COVID situation, but continued to maintain just a little below that \$5,000 per week despite government lockdown, should be scrutinized. More focus will be there on transaction laundering.

**Recommended step to mitigate risks of transaction laundering:**

Financial Institutions will be expected to work to amend their automated monitoring rules and triage alerts to ensure those linked to the most significant activity are addressed quickly. The actual account activities of clients should not deviate significantly from expected account activities.

**"The views/opinion expressed are explicitly of the Author. And are not necessarily reflective of his employer's standing or corporate policy"**



## Amlan Das

Senior Manager Anti-Money Laundering  
at Bandhan Bank

Alongside the multifaceted disruption worldwide, COVID-19 pandemic has changed the traditional way of money laundering. Financial fraud and exploitation scams are in focus.

### 1. Malicious cybercrimes:

- The Dark Web: Customer data viz. credit card details of many Banks are being compromised and put up for sale on the dark web.
- Phishing, business email compromise: With increased work-from-home activities using various digital tools, Ransomware attacks are on the rise. Scammers are utilizing the loopholes in the network to gain access to customer and transaction information.
- SMSs impersonating Government/regulatory bodies are in use to lure individuals into disclosing personal and account information.

### 2. Changes in banking transactions:

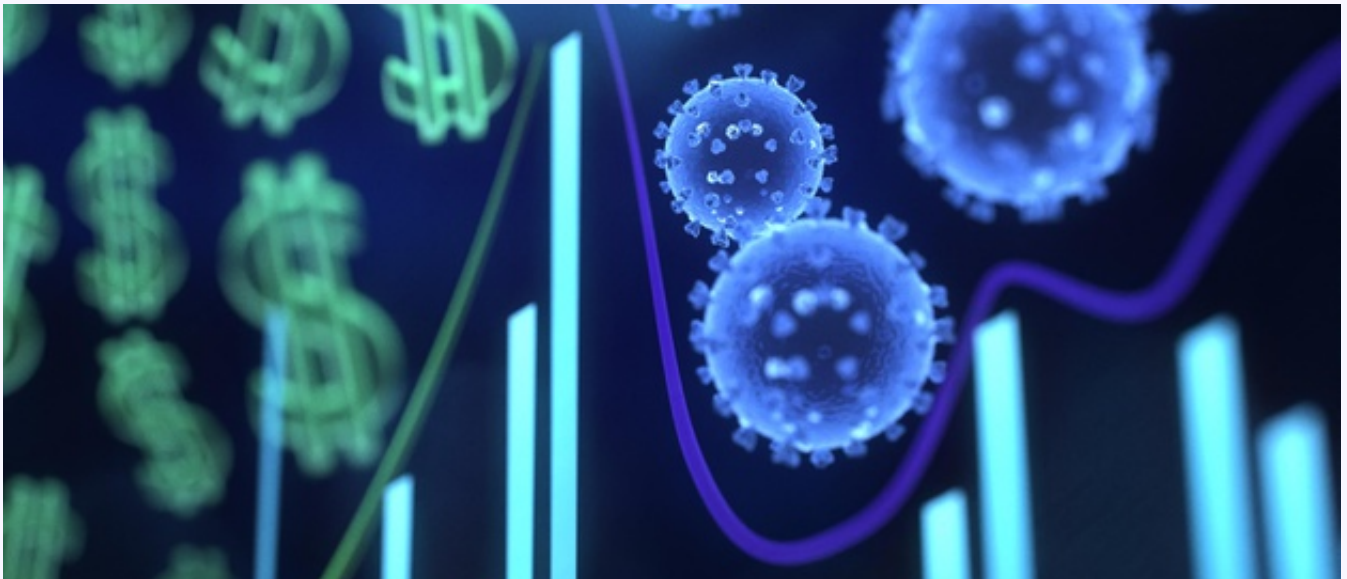
- Increased online transactions may lead to the disclosure of bank accounts, passwords, and other personal details to the suspects.
- People unaccustomed to the usage of digital platforms, make it vulnerable to fraud.
- Unorganized lending in developing countries may lead to the syndication of crimes.

### 3. Trafficking counterfeit medicines:

The pandemic has significantly increased online scams involving medical supplies, personal protective equipment, and essential items.

### 4. Fundraising for fake charities:

Fraudulent emails are being circulated for several fundraising activities. The victims are re-directed to make the payment using credit or debit cards, thereby leading to leakage of the information.



5. Criminals are utilizing the macroeconomic conditions and luring people to invest in fraudulent schemes promising high returns.
6. Ecommerce websites are used to sell smuggled items under the garb of genuine business transactions.
7. Other predicate crimes are on the rise, which includes online child sexual abuse, human trafficking, and exploitation of workers.

Change in crimes has led to the change in the regulatory framework, including an emphasis on the use of Fintech, Regtech & Supotech whilst remaining alert to new and emerging illicit finance risks. Regulators should guide the financial institutions to remain vigilant to detect suspicious financial and non-financial transactions/activity. STR reporting should be prioritized.

Countries receiving international aids should take additional precautions to ensure the funds are not diverted for other purposes. Countries and institutions with lower cybersecurity measures should strengthen their cybersecurity policy and framework. There should be continuous information sharing between private, public, and law enforcement authorities, enabling assessment of the new risks and adapt accordingly. However, there are high chances that the institutions may forego the risk associated with the conventional cash-intensive business and cross border funds flow.



## Andres Betancourt

Senior Audit Manager, AML/CTF and Sanctions  
at Scotiabank

AML is dynamic and fluid and impacted with factors globally, such as COVID-19. Illicit activity is on the rise as criminals, and organized crime groups are exploiting vulnerabilities opened up by the COVID-19 pandemic via new tactics like:

- advertising and selling counterfeit medical equipment, pharmaceuticals, food and vitamin supplements
- increase in wire fraud with transactions including terms such as donations, for the purpose of COVID, COVID-19, masks or ventilator purchases
- VPN Phishing attempts stating that required verification is needed for security tokens
- impersonation of representatives of public authorities and household decontamination services
- scams promoting test kits and assessment sites used to steal personal information to open fraudulent accounts, credit cards, and loans.

Areas of focus for prevention/detection of changing AML risks should center in transaction monitoring typologies and maintenance and validation of new rules tailored to identify :

- wire aggregation to new PPE companies and pharma companies,
- benefits payment or loans from the government to brand new legal entities with high velocity out activity after payments received (not used for actual business operations.)
- continued high volume activity of cash deposits for a cash-intensive business that is known to be affected by quarantine measures or mobility restrictions.

Emphasis on strong enhanced digital customer on-boarding controls ensuring KYC attributes and data are captured real-time and stored securely in core systems for robust transaction monitoring and client risk rating, aimed at reducing request for information and asking clients to visit branches.



- Focus on various components, such as, but not limited to: Enhanced scrutiny of all new individual/business accounts (receiving government subsidies or financial support) to ensure adequate KYC/CDD/EDD is complete to ensure fictitious companies are not created to claim fraudulent benefits.
- Ascertaining red flags are raised for new clients that do not have a long corporate history, lack of physical presence or that have been incorporated in High Risk or Off-shore Tax havens,
- Abuse of Not for Profit organizations and charities for "COVID" donations and support.

**"The views and opinions expressed are those of the authors and do not necessarily reflect the official policy or position of my employer."**





## Branka van der Linden

Head of AML Compliance at Megaserve  
Secretary of the Board Cyprus Integrity Forum

### COVID-19 more than just a health threat

When someone is involved in corporate services, they closely interact with law offices, banks, accounting, and audit firms. In this business environment, I get the impression even the birds on the trees are chirping what Money Laundering is. "Making dirty money appear clean." A practice of disguising the illicit origin of criminal proceeds. However, far fewer birds care or even comprehend what grave impact and damage money laundering causes. In the last thirty years in Europe, it seems like the AML Directives' evolution is disproportional to the growth of criminal ideas for laundering money. Criminals are more than one step ahead.

Every coin has two sides. Where the world has portrayed COVID-19 as a global pandemic, for criminals, it poses as a money-laundering opportunity. The current need for advancement of AML compliance and control methods has created a distressing environment for the financial institutes and regulators globally.

The Financial Action Task Force ("FATF") has interpreted the current pandemic as a potential for criminal exploitation prominently in the financial domain. The FATF has further identified the possible opportunities for criminals to exploit the vulnerabilities of the system.

Let us look at the few.

**Relaxation** in the financial sector in terms of regulations allows perpetrators to launder illegal funds. In respect to the current social distancing needs, financial institutions are inclined to offer relaxation to their customers in terms of AML /CFT requirements such as customer onboarding and due diligence. But, this relaxation further creates a vulnerability in the system that can be exploited by the offenders. The level field is suddenly truly global.

Leveraging online financial services and virtual assets for moving illicit funds is growing in popularity. The necessary ingredients, such as anonymity and speed, are virtual nests for money launderers and fraudsters.

Misuse of financial aid, emergency funding, and fake charities for cross-border movement is a close second. The mushroom phenomena of new health materials providers and producers of COVID-19 related emergency aid is devastating.

Therefore, the AML/CFT compliance and controls need to be more robust than ever to combat this threat. The increasing possibility of cybercrime, fundraising for fake charities, and medical scams bear witness to the need for vigorous compliance and control. The question remains, what spreads faster COVID-19 or Money Laundering;

Looking at the new way we do business, a new system that allows the safety of employees persists to the rules of the pandemic is flexible for the customers, and, most importantly, is robust enough to prevent money laundering is an obvious necessity. This unprecedented change may become a difficulty for most institutions, but it is imperative to implement this change to combat the potential increase in financial crime.

Financial institutions are bound to face numerous problems, such as the massive increase in online transactions, which makes it challenging to track unauthorized funds transfer. While the financial conduct authorities further emphasize the need for advanced AML compliance in its business plan of 2020/21, the inescapable fact is that it will become even a more significant concern post-COVID-19.

For instance, the KYC operations do incur considerable pressure as governments worldwide offer their support in terms of loans and finance. Identification of dissolved businesses and dormant accounts add to this pressure.

The inevitable economic downturn followed by massive unemployment becomes another excellent opportunity for criminals. As a result, people may become more susceptible to corruption, and organized crime is expected to thrive, especially in developing nations. The financial institutes, regulators, and compliance teams are in a dilemma posed by the intensification of organized crime post-pandemic. What must we do?



This pandemic indeed is a wake-up call to re-examine the way we live, the way we wash hands, and the way we do business.

We should look at developing an implementation and accountability system for the plethora of guidance that is already in the market.

We can positively engage the private sector to provide solutions for effective and efficient information flow. We must undeniably admit the severity of the communication gap between institutions such as Tax Offices, Registrar of Companies, Social Insurance services, and other governmental and semi-governmental institutions, and bridge that gap, swiftly. Above all, to eradicate the problem, we must appeal to the personal ethics of every individual in our society and make awareness and education the first line of defense.



## Ehi Eric Esoimeme

Anti-Money Laundering Consultant  
at E-FOUR AND AAF

The COVID-19 outbreak highlights the importance of application programming interfaces (APIs) and artificial intelligence-enabled systems during the customer onboarding process. Traditional rule-based Know Your Customer (KYC) technology necessitates significant dependence on manual efforts, particularly in the alert investigation stage, which can be time-consuming, labor-intensive, costly, and error-prone. In order to overcome these considerable and lingering challenges, it has now become imperative that financial institutions leverage new-age smart technology solutions.

KYC API offers a single source for information and documentation to support due diligence and help financial institutions focus on decision-making rather than time-consuming and repetitive manual research activities. With KYC API, organizations can access information from a wide swath of sources from public records, private records, and governments. These include phone records, credit bureaus, DMV information, arrest records, utilities, court records, and business data, which can be accessed via APIs during the customer onboarding process.

KYC API will help an organization streamline the collection of financial counterparty KYC data and due diligence documentation, and maintain a holistic view of a counterparty using accurate intelligence that's updated regularly and confirmed by primary sources to ensure quality. Before using an organization's KYC API for digital identities, electronic or digital identity verification, or trust services, firms should be satisfied that information supplied by the provider is considered to be sufficiently extensive, reliable, accurate, independent of the customer, and capable of providing an appropriate level of assurance that the person claiming a particular identity is, in fact, that person.

Artificial Intelligence can be used to analyze API's dataflows. Artificial intelligence (AI) allows IT systems to imitate cognitive capabilities of the human brain in such a way that it could perform a wide range of tasks starting from thinking to learning, reasoning and problem-solving. Artificial Intelligence comprises various branches such as machine learning and natural language processing. Machine learning refers to the ability for software to learn and to become more accurate in its outcomes. Machine learning technology can take in large amount of data from public sources and connect it to customer information.



Once the information has been digested, it will match the information to each entity and look for any anomalies within the data that needs to be corrected. Natural language processing is a text processing engine that assigns topics/themes to incoming news automatically and provides a surveillance service for clients. Natural language processing breaks down search results by extracting useful information such as client identities, products and processes that can be impacted by regulatory change, thereby keeping the bank and the client up-to-date with regulatory changes.

In using the KYC API and Artificial Intelligence to verify a customer's identity, firms should ensure that they are able to demonstrate that they have both verified that the customer (or beneficial owner) exists, and satisfied themselves that the applicant seeking the business relationship is, in fact, that customer (or beneficial owner).





## Gürcan Avci

Head of Regulatory Intelligence  
at Sanction Scanner

### **We need hygiene regulations against money laundering**

The help of non-bureaucratic government institutions to the economy in the corona crisis was good. We should all pay attention to a few things so that criminals do not take advantage of this situation.

Staying away, wearing a mask for mouth and nose protection, and regularly washing your hands has become the new standard of hygiene in public life. However, we should all be more careful about new money laundering opportunities for criminals in the current pandemic.

States have provided billions of dollars of support to help businesses stand up and help when the coronavirus spreads. Companies were able to apply for loans quickly and without a large check. The default risk is covered only by the states, i.e., the taxpayer. From the benefits of non-bureaucratic institutions, criminals will have the opportunity to collect money that wasn't for them. For example, through mailbox companies: only companies on paper are valid for loans showing an emergency that is not available or non-refundable.

Where a lot of money is spent with little checking, there are more dangerous money laundering opportunities.

### **Gateway for criminals**

The Financial Action Task Force ("FATF"), the most important international body for combating money laundering, as well as financing terrorism and weapons of mass destruction, describes such machinations in a recently published report. The FATF strongly warns that criminals use the pandemic for financial fraud and make use of the new, often bulging pots. For example, a simplified money laundering check for lending can be a gateway for criminals.

FATF warns that criminals are involved in the existing COVID-19 pandemic and are increasingly using uncertainty between citizens and companies for fraudulent purposes. Crimes in this topic include fraudulent offers for protective masks and other medicinal products and fictitious calls for donations in connection with alleged aid actions. Others try to collect sensitive information for subsequent crimes, for example, questioning personal data by phone or e-mail, or questioning for urgent financial aid. With this data, they can redirect payments, go shopping with third-party credit cards, or sell their identities to other criminals.



Criminals also use pretext to install malware on private computers or mobile devices to access personal data where they can act like authority health workers and then trigger payments. Ideally, only banks and government agencies are not required to prevent such damage on your own account. Therefore, we must be careful and strictly follow the rules of fighting money laundering. **Only in this way, the criminal machinations will be blocked in the bud.** Finally, as well as washing our hands, we all need to take a closer look at who we entrust personal information and maintain a certain level of data hygiene.



## Imad Habre

AML, Compliance and Risk Management Professional  
at IBL Bank

### **COVID-19, putting business continuity planning into practice**

One of the most “Underrated” topics in the financial world is business continuity planning. As humans, we tend to think that we are invincible and that worst-case scenarios will remain scenarios.

Enter COVID-19. This tiny virus exposed weaknesses in countries, organizations, and institutions alike. It put our contingency planning into practice and highlighted the gaps that need to be tackled head-on. As an AML professional and a banker, I couldn't but notice the weaknesses in the majority of financial institutions while facing this virus.

#### **AML and Compliance departments were not ready due to several reasons:**

- They lack the remote AML technological infrastructure as most systems are directly linked to core banking systems, and very few invested in APIs (application program interface).
- They never practiced Business Continuity Plans or prepared for such scenarios.
- Many FIs still rely on physical documentation and hard copies.
- Red flags and AML typologies rapidly shifted towards fraud and elderly abuse

**However harsh the reality is, we should embrace the changes and challenges for the post-COVID-19 period as follows:**

- “Walk the talk”, put those Business Continuity Plans into practice and adjust and update where necessary

- Start investing in remote AML technology for sanctions screening and AML monitoring systems
- Invest in cloud technology, OCR scanning, and other technological advancements to stop relying on physical documentation.
- Update Risk-Based Approach frameworks as it will be very useful in times of remote access and limited working hours.
- Refresh and frequently update AML typologies to include newly emerging financial crime trends.
- Don't be static.



Indeed, we are living exciting times and in the words of Charles Darwin, “It is not the strongest of the species that survives, nor the most intelligent; it is the one most adaptable to change.”



## **Plamen Georgiev**

Chief Legal Advisor/General Counsel at Alsas

The unexpected and rapidly spreading COVID-19 pandemic (caused by unknown by the end of 2019 type of coronavirus, also known as “SARS-CoV-2”) has affected almost any sphere of life and business. This entirely new and unprecedented situation has led to new forms of illegal activities as criminals quickly adapted to opportunities arising from the crisis. As a consequence, newly-generated “dirty” money are on their way to be “cleaned”. So, the crisis allowed money launderers to practice their “skills” in various new schemes of concealing origin of the illicit proceeds. In the following paragraph I will share with you my personal opinion and expectations how would change the AML regime after COVID-19.

Although global restrictions such as lockdowns, quarantines, curfews have been imposed because of the pandemic, the criminal world hasn’t taken “a break and chill”. All obliged persons/entities under the articles of the national AML legislations should not ignore the risks of money laundering in their business spheres and all of them are to continue monitor clients on a daily basis. As business relationships and financial transactions have been extremely digitized, I expect global AML standards to become more demanding in CDD, especially non-face-to-face identification of clients.

In addition, FinTech companies have already expanding the financial sector services providing new payment methods, I think we could expect new legal requirements in this area too. We could predict new regulations to be imposed on all business fields defined as “high risk” (according to national risk assessments of money laundering and terrorism financing) in their progress of digitization. It’s not only businesses, it’s life digitalization being started. COVID-19 pandemic has just accelerated these processes. So, it’s up to any of us working in the AML/CFT to be well-prepared to face the challenges of the new reality.





## Rezaul Karim

Anti-Money laundering Specialist | CDD Analyst  
at HSBC

### Coronavirus: The Good, The Bad & The Ugly:

Due to the outbreak of coronavirus, millions of people have locked themselves inside their house not because they are well conscious and responsible citizens; rather, they are forced to. The world has seen a lot of dark sides of the economic impact in the coronavirus, but as life continues, many people who are blessed to have a stable job are now exploring the bright side of coronavirus by giving a new dimension to the familial bonds by working from home. The Financial industry also has seen a fewer number of AML cases & fines from regulators as COVID-19 completely disrupted demand of illicit drug trafficking and successive money laundering measures.

The other aspect, the terrifying one, substantially marginalized people for whom 'No work means no pay' continuing the social distancing against the invisible virus is nearly impossible. Also, within the month of locked down, millions are jobless and consequentially already ran out of savings. The persistent locked down has impacted the economy, with Businesses cutting jobs as demands of non-essential goods & services have been drastically reduced. Study shows that an increase in the number of job cuts and subsequent unemployment can lead to a growth of unprecedented criminal activities. The world has already witnessed the far-reaching crisis and likely to see unprecedented pressure than usual in fighting financial crimes.

### Emerging trends in Pandemic & Afterward:

Following are a few emerging trends that will be prevailing in post COVID world as well:

- Regulators around the world will be more flexible in encouraging banks to provide financial services in digital space so that customers can obtain desired financial services by maintaining social distance

- A huge number of AML reporting backlogs like to increase in the Banks due to a shortage of staff & challenges in working from home.
- KYC compliance will reach its new heights as Banks will adopt the E-KYC approach to digitally on-board customers & the Due diligence approach will be more simplified as per the Risk-based approach FATF allows.
- Fraudsters will be more involved in money mule scheme, cybercrime and the world is going to see abuse of financial support / stimulus package in developing countries.
- Banks likely to face challenges in the supervision of AML obligations as criminals will attempt to bypass CDD measures in the context of health emergency in COVID Times.

### **Challenges in AML / KYC Compliance:**

AML/KYC compliance has seen its intensity and discussed worldwide only since last decade, the profession itself is comparatively new, even the most experts working in the field lack real pandemic or a skyrocketing unemployment experience to completely understand pandemic fraud behaviour profiling. The fraud schemes are capitalizing the coronavirus anxiety and insecurities to mass people, hence institutions must detect potentially suspicious activity and monitor emerging trends that may target them and their customers in pandemic and afterward. Financial institutions need to re-assess vulnerabilities in exposed areas, increase awareness, re-assess & develop compliance strategy to minimize the impact.

Needless to mention, the outbreak has disrupted access to traditional banking channels, likewise traditional money laundering measures are shifted to other schemes in the pandemic. AML professionals all around the world must rethink and redesign the AML monitoring system since only system based traditional behavioural monitoring system keeps financial institutions at a disadvantaged position and subsequently makes more vulnerable.



## Sholane Sathu

Managing Director: Navigate Compliance

The financial crime regulatory landscape is in a constant state of evolution amidst political interventions, global events and the sophistication of criminal activity and networks. The COVID-19 pandemic has led to unprecedented global challenges, human suffering and economic disruption which has generated various government responses, ranging from social assistance and tax relief measures, to enforced confinement measures and travel restrictions. While unintended, these measures have provided new opportunities for criminals and terrorists to generate and launder illicit proceeds while on the other hand has brought to light gaps inherent in the management of financial crime risks and is likely to influence the way we manage risks going forward.

The key themes that are likely to dominate the financial crime landscape in a post COVID world may include the following;

- The rise in digital onboarding,
- The need for an integrated financial crime risk assessment,
- A heightened focus on effectiveness testing and outcomes-based monitoring,
- Greater focus on client desirability balanced with the need to promote financial inclusion,
- The rise of global sanctions,
- Improved compliance business continuity planning.

The COVID-19 pandemic has certainly given us time reflect on the things that we can do differently to enable our organisations while finding new and innovative ways to manage financial crime risks.



## Tarik Tombul

Board Member at ODED,  
CEO at PayTR

We know that cases of fraud and cybercrime have increased in times of global economic turmoil from previous experiences and reports on this subject. In these periods, the crimes of money laundering and financing of terrorism increase in a similar way.

### **So what happened in COVID-19, what crimes increased, what were the measures taken?**

Public institutions, financial institutions, private sector, and individuals turned to work remotely during the lockdown period. This home office working model led to the disregard of some business processes. As a result of this, it led criminals to bypass some processes in their favor. Especially in the pandemic period, new businesses emerged in the medical products and disinfectant product categories. Front companies started to make fictive transactions by establishing new businesses for money laundering.

Fraud cases increased, especially frauds realized by seizing the information of consumers through social engineering and phishing increased, sales of counterfeit products increased, and likewise, frauds emerged through requests for donations and aid were also increased. In addition, the operational delays were experienced in suspicious transaction reports due to the home office working model.

### **What will happen after COVID-19:**

The behavior of consumers and businesses has changed. Companies must revise their AML programs taking these changes into account. Companies must put in place action mechanisms that will enable them to quickly monitor new behaviors. AML and Fraud monitoring programs, which detect new types of behavior and update their rules and scenario, will become more popular. In addition, business continuity plans will become much more important.

# Thank You

to all of our authors for supporting our ebook project by sharing their opinions on "Expected Changes in AML After COVID-19". We also thank all our esteemed readers who have read our e-book. We wish everyone healthy days.

## Contact Us



27 Old Gloucester Street, London, United Kingdom, WC1N 3AX  
+44 20 4577 0427



Yıldız Technical University - Yıldız Technopark  
C1 - No:106-2, Istanbul, Turkey  
+90 (212) 963 01 84



info@sanctionsscanner.com

