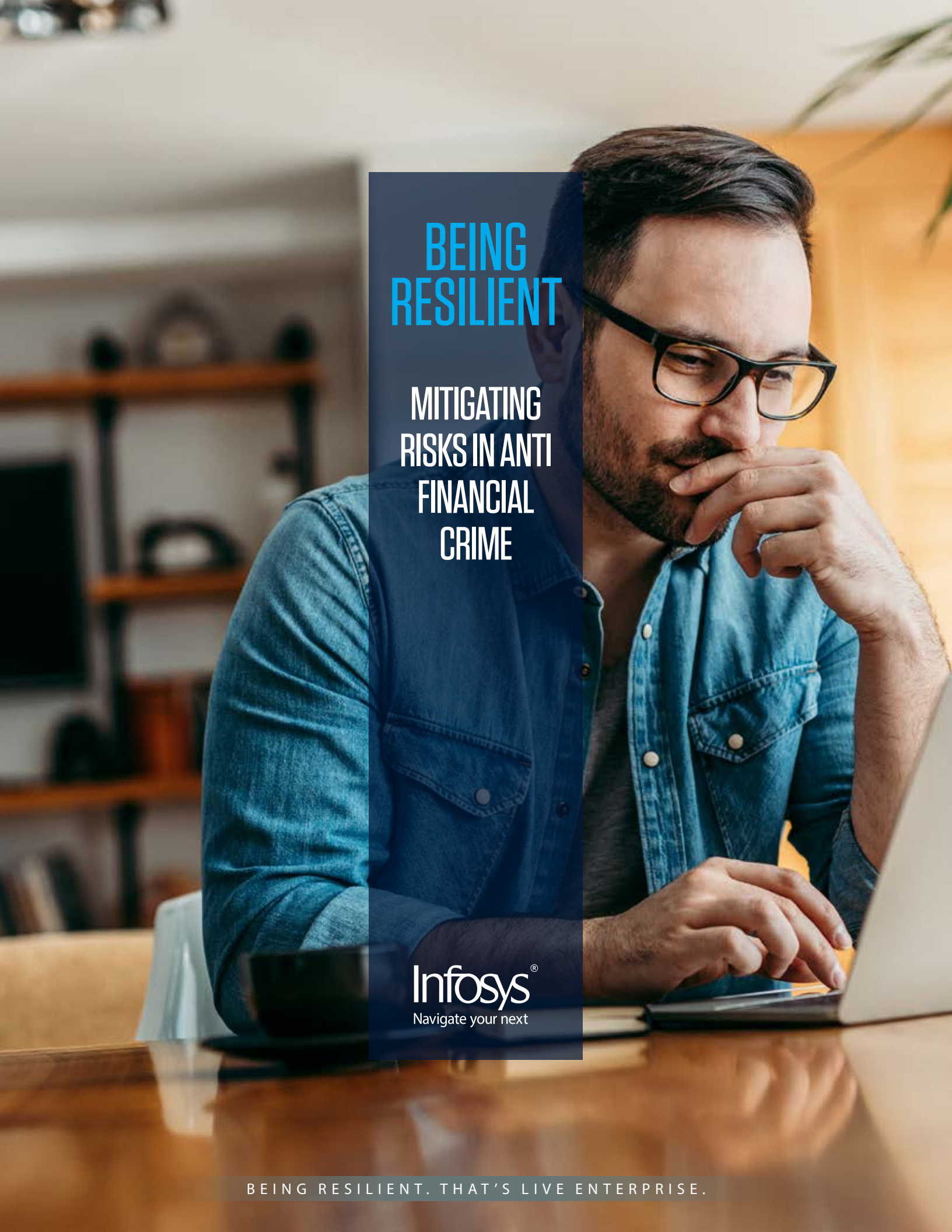


BEING RESILIENT

MITIGATING RISKS IN ANTI FINANCIAL CRIME

Infosys®
Navigate your next

BEING RESILIENT. THAT'S LIVE ENTERPRISE.

Introduction

Covid-19 (Corona) is an unprecedented calamity on human beings, society and the world in general. This pandemic has already taken more than hundred thousand lives and impacted human health across the globe.

It has also given a massive jolt to the global economy. Consumption is declining. Industrial production is nosediving. Unemployment is increasing. GDPs of all major nations are falling. Interest rates are falling. Development projects are getting deferred. Stock markets are collapsing. And supply chains are getting shattered. Overall the global economy is staring at a big recession. This is the biggest challenge we are facing after the great depression of 1930s.

Being a key sector of the economy, Banking and Financial Services industry has been affected tremendously. Organizations are struggling to keep essential services up and running. Revenues are contracting. Cost reduction pressure is increasing. New forms of financial crimes such as fraud and cyber security are erupting. Workforce productivity has reduced due to remote working. At the same time, new workload is getting added to manage relief package activities On top of it, day by day regulators are giving new guidelines and regulatory compliance obligations are getting enforced.

These business challenges are having profound impact on technology side also.

This paper is excavating all these business and technology challenges in Anti Financial Crime (AFC) area and how the financial services industry is coping up and mitigating the risks, including short terms tactical measures and developing strategic roadmaps to make their systems and processes resilient to such debilitating events.

Impact on Anti Financial Crime

To address the current crisis, The Financial Task Action Force (FATF), The US Financial Crimes Enforcement Network (FinCEN), The European Banking Authority (EBA), The Australian Transaction Reports and Analysis Centre (AUSTRAC), The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and other regulators have released their guidance to be adopted without sacrificing the core standards that help fighting fraud, money laundering and terrorist financing.

In light of these developments, this paper analyzes the impact on Financial Crime from the perspective of

1) KYC-CDD

2) Transaction Monitoring

3) Sanctions/Watch List Screening

4) Fraud Risk Management

5) Compliance Policies and Procedures

1. Know Your Customer - Customer Due Diligence

The KYC/CDD process can be primarily considered as 2 phases, first is the onboarding and second is the review process which conducted throughout the customer relationship lifecycle.

The onboarding process has 3 sub-processes,

1) To collect information

2) To gather evidence for verification before setting up a relationship

3) To risk assess the customer.

The established processes are challenged either due to lock down or due to staff being in quarantine. This is causing onboarding delays of new customers.

For collecting information, they can leverage digital banking channels to collect evidence and use electronic verification mode wherever possible. FATF has recently published a separate guidance for the use of digital-ids to encourage digital onboarding. For example:

1) Using electronic copies. Scanned or photographed documents can be used. Also, 'Selfie' of customer can be used to compare the scanned or photographed copies of identification documents.

2) OCR (Optical character recognition) based document verification can be done.

Scanned or photographed copies of identification documents can be compared against customer's face by doing video calls. For example, RBI (Reserve Bank of India) has now allowed banks and NBFCs to have video KYC or Video based Customer Identification Process (v-CIP).

Risk-based approach is used for customer risk scoring. In the current turmoil, risk scores will have to be revisited which are associated with type of product, type of customer, purpose of account opening, occupation, country of registration. for example, Automotive and Tourism industries are badly impacted, so there is a possibility that a firm doing business in such industries deals not in line with the industry trend may be involved in money laundering activities. Let us say a new SME customer has started a business in tourism sector and wants to set up a relationship with Bank A. In normal circumstances this customer may be a low risk customer but post Covid-19 he will be classified as medium or high risk.

On the other hand, FIs may also have to consider revising the high risk associated with online/internet channels to avoid enhanced-CDD since in the scenario where lockdown is imposed customer onboarding will take place through digital channel. Also, reducing the count of enhanced CDDs will increase the workforce availability for critical activities. This will as per the guidance given by regulators.

Re-risk rating of some customers has to be done due to changes in risk assessment parameters or changes in risk tolerance. Related Party and Beneficial Owner information has to be re-examined as ownership changes may happen. This will also trigger re-risk rating. Periodic as well as event-driven risk review can be impacted due to roadblocks in collecting information of customers, as sufficient staff may not be available due to lockdown and self-quarantine.

2. Transaction Monitoring

It has been observed that people are modifying their financial behavior to respond to the pandemic. To mention few

1) withdrawing physical cash in panic.
2) using mobile apps for transactions, considering its safe.

3) It has also been observed surge in virtual currency usage.

4) Low business activities and hence less transaction volumes of some clients. For example, wire transfers have dropped by 25% since February.

5) There can be changes in customer's transaction patterns due to deferred or intermittent payments of loans accounts, credit card accounts, mortgages and auto loans. Salary deposits also can be irregular. This may have impact on segment-wise thresholds.

6) There can be spurt in dormant accounts. Non-profit Organizations (NPOs) play a vital role in delivering human assistance. But it is possible that money can be laundered through the existing or newly set up NPOs wherein the funds meant to help the needy is diverted for setting up terrorist infrastructure and buying of military equipment. Since this is a global pandemic, use of charities for terrorist financing has to be strictly monitored.

Similarly, it is also possible that NPOs can serve as a money laundering front for criminals holding illicit assets and use money mules to launder money. The money mules are individuals who are hired by criminals to facilitate the transformation of proceeds of crime. The criminal deposits money in mules' personal bank account through a newly established NPO. This money is then withdrawn as cash and can be deposited as bitcoin to be transferred to criminals' bitcoin wallet. In addition to such scenarios there may laundering attempts through setting up of shell firms supplying medical goods online (for example face masks) where even though the payment is made but there are no goods delivered. These shifts in transaction patterns are making it harder to AML investigators to discriminate between legitimate activity in a time of crisis and illegal transactions.The situation is becoming worse due to reduced productivity of investigators due to remote working. They cannot refer physical and historical documentation available at the workplaces. Plus, the banking industry is staring at forced attrition by lay-offs due to envisioned losses in the FIs' revenue. Also, the reduction in workforce productivity can result into piling up of alerts to be investigated. It can have impact on quality of investigation, and Financial Institutes will face risk of missing SLAs of CTR and SAR filing due to reduction in the workforce productivity. Compliance units will have to prioritize their activities to avoid these delays. All these circumstances are making investigators' job more challenging.

To deal with these challenges, financial Institutes must revisit red flags and the transaction monitoring rules and tune the thresholds to address the changes in customer behavior. For example, a mid-sized bank in the Midwestern U.S., is considering treating a much larger volume of digital payments as normal.

Use of automation technologies like RPA, Artificial Intelligence and Machine Learning will increase investigation throughput by reducing manual processing and by reducing false positives. But investigation quality and consistency will be maintained.

Also, there will be much emphasis on accessibility of IT systems and data from remote locations and effective controls to ensure the remote access is not abused. Banking industry is also expecting some reliefs from regulators in compliance.

Banking industry is also expecting some reliefs from regulators in compliance.

- FinCEN conveyed that FIs should alert the them of "any potential delays in their ability to file required BSA reports" due to the outbreak.
- FinCEN has suspended implementation of new rule on CTR (Currency Transaction Report) filing for sole proprietorships and organizations operating under a "doing business as" (DBA) name.

3. Sanctions / Watch-list Screening

Countries such as Iran are listed as Sanctioned countries by USA and some other countries. If any individual or an organization wants to help Iranian NGOs or government agencies on the basis of humanitarian grounds, these transactions will be creating an alert by default. So, the sanction screening mechanisms need to be adjusted properly to review such transactions.

White lists can be carefully updated for such sanctioned geographies to help charities for Covid-19 affected people.

Also, Adverse Media Screening can be increased.

4. Fraud Risk Management

Various regulatory bodies have warned about rise in fraudulent activities and changes in the types of frauds.

- The FATF has mentioned "Criminals are taking advantage of the Covid-19 pandemic to carry out financial fraud and exploitation scams". These are crimes related to fake medicines, fraudulent investment schemes, cybercrimes including phishing and fundraising for fake charities.
- FinCEN has asked FIs to be vigilant of the fraudulent and malicious transactions like

1. Imposter Scams (Fraudsters attempt to get donations, steal personal information, or distribute malware by impersonating government organizations, and organizations like WHO).

2. Investment Scams (Claiming that a publicly traded company's products or services can prevent, detect, or cure the covid-19).

3. Product Scams (companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19).

4. Insider Trading.

- Action Fraud (UK's national reporting center for fraud and cybercrime)'s observations:
  - In March-2020, twenty-one reports were received, they were linked to the virus. Total losses were over £800,000. Ten reports were regarding fraudulent selling of face masks.
  - It also observed that fraudsters email potential victims and pretend to be from health related organizations like WHO or CDC (Centers for Disease Control and Prevention.
- Various check frauds related to COVID Relief have been detected by various agencies.

While regulators and government bodies are issuing guide lines, still fraudulent activities are increasing.

- The Guardian has reported 500+ corona virus related frauds and over 2,000 phishing attempts in March in UK.
- FTC (Federal Trade Commission, USA) has reported 1.1 MUSD and 1.28 MUSD fraud losses in online shopping and imposter scams from January 1 to April 1.

Financial Institutes need to revisit their mechanisms of fraud identification, prevention and reporting to address these frauds by reviewing internal systems, increasing audit trail, scrutinizing bail-out funds, maintaining consumer privacy & information security and maintaining critical functions and watching insider trades.

Almost all regulators, banks and Non-Banking Financial Institutes have issued advisories to customers to understand and prevent fraudulent activities. And some financial institutes have done some changes in their systems such as fine tuning fraud detection engines.

Tech companies are coming up with new programs to mitigate fraud risks. For example,

1) Amazon has removed a million products from its marketplace from those who either priced the items unfairly or made false claims.

2) Facebook and Instagram have already announced to ban ads and promotions of face masks on their platforms to stop people from exploiting the coronavirus emergency.

Some tech companies are offering free software products to address fraud risks. For example: Xelix AI (payment fraud identification), Fraud.net (email authentication tool), Shufti Pro (Id and face verifications tool)

Here are some other observations

- Use of machine learning to identify frauds will increase.
- Due to increase in digital payments, banks are tightening the scrutiny and equipping Fraud Identification systems to handle more transaction volume.
- Online retailers are tightening their fraud identification algorithms.
- FinCEN's has asked FIs to enter "COVID19" in Field 2 of the report (SAR) as applicable. So FIs have to configure their SAR filing systems.

5. Compliance Policies and Procedures

BCP planning in general at FIs had very low emphasis on pandemic situations. Many regulators also had muted or no guidance. Now, compliance functions of many Financial Institutes have published elaborate guidelines for remote working for their staff.

But now, nimbleness of processes to quickly adapt to new regulatory guidelines will be expected. At the same time, there has to be focus on avoiding any delays in SAR and CTR filings.

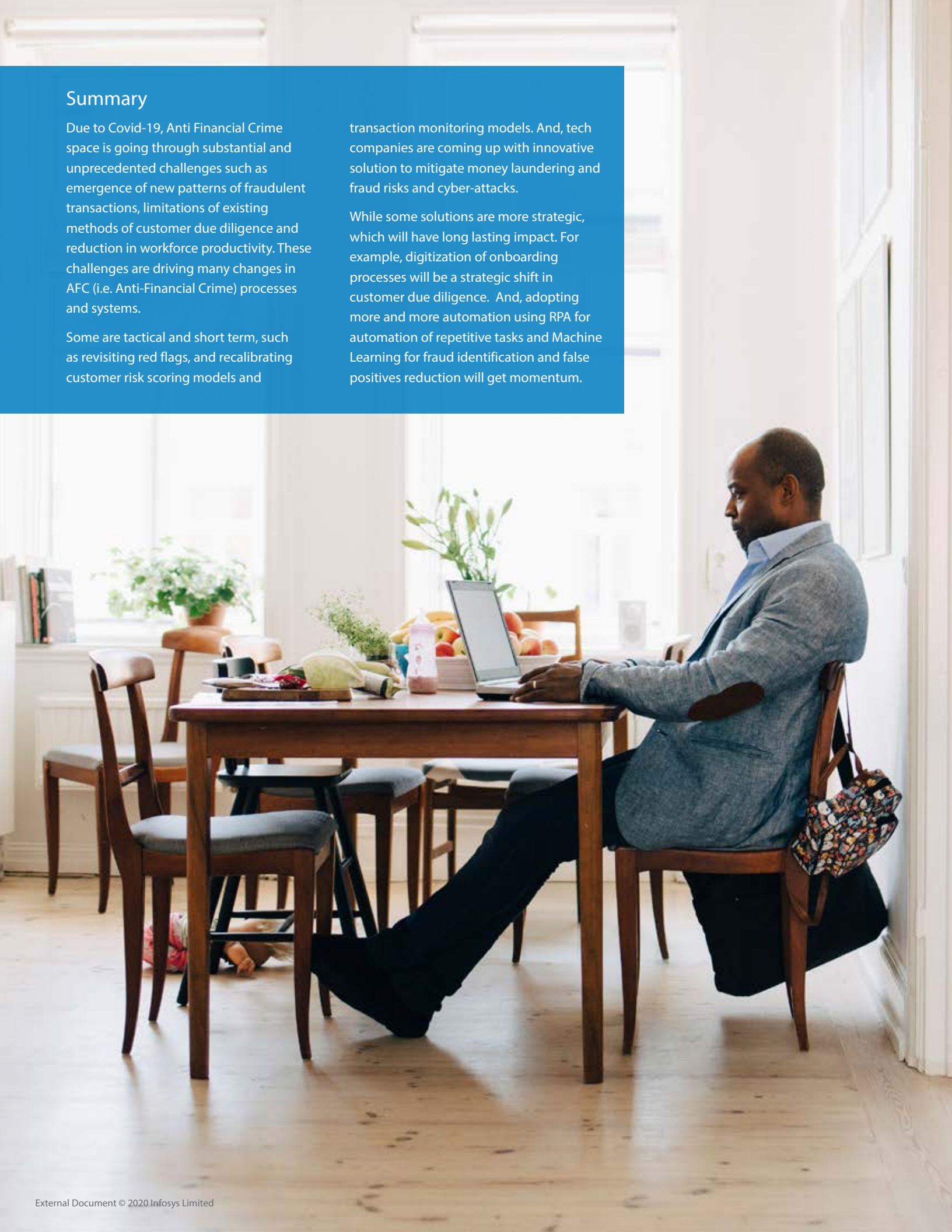
Stress testing of managing compliance operations effectively with minimum bandwidth and reduced resources availability will be done frequently. Testing of pandemic preparedness will emerge as new normal for compliance functions.

Summary

Due to Covid-19, Anti Financial Crime space is going through substantial and unprecedented challenges such as emergence of new patterns of fraudulent transactions, limitations of existing methods of customer due diligence and reduction in workforce productivity. These challenges are driving many changes in AFC (i.e. Anti-Financial Crime) processes and systems.

Some are tactical and short term, such as revisiting red flags, and recalibrating customer risk scoring models and transaction monitoring models. And, tech companies are coming up with innovative solution to mitigate money laundering and fraud risks and cyber-attacks.

While some solutions are more strategic, which will have long lasting impact. For example, digitization of onboarding processes will be a strategic shift in customer due diligence. And, adopting more and more automation using RPA for automation of repetitive tasks and Machine Learning for fraud identification and false positives reduction will get momentum.



References

1. https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html
2. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
3. https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions
4. https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20provides%20additional%20clarity%20on%20measures%20to%20mitigate%20the%20impact%20of%20COVID-19%20on%20the%20EU%20banking%20sector/Statement%20on%20actions%20to%20mitigate%20financial%20crime%20risks%20in%20the%20COVID-19%20pandemic.pdf
5. https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/kyc-requirements-covid-19
6. https://www.tookitaki.ai/news-views/money-laundering-amid-covid-19-what-regulators-across-globe-say/
7. https://www.acfcs.org/in-second-pandemic-statement-fincen-tackles-stimulus-aml-tangles-creates-new-covid-19-compliance-conundrum-contact-mechanism/
8. https://www.ballardspahr.com/alertspublications/legalalerts/2020-03-16-fincen-warns-about-covid-19-scams-and-requests-enhanced-comm-from-fin-institutions
9. https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/AMLCFT-Supervisor-Guidance-COVID-19-Alert.pdf?revision=2bf0b10b-c2a8-4e10-84ba-f413a1672e4c&la=en
10. https://www.icaew.com/insights/viewpoints-on-the-news/2020/mar-2020/aml-responsibilities-taking-on-clients-during-covid-19
11. https://economictimes.indiatimes.com/news/economy/policy/in-a-first-rbi-allows-kyc-process-on-mobile-video/articleshow/73183868.cms
12. https://brightlinelaw.co.uk/covid-19-consequences-for-anti-money-laundering/
13. https://www.moneylaundering.com/news/covid-19-outbreak-prompts-financial-institutions-to-adjust-transactions-monitoring-sources/
14. https://www.niceactimize.com/blog/aml-financial-crime-resilience-during-covid-19-we-still-have-a-job-to-do-640/
15. https://blogs.thomsonreuters.com/answerson/covid-19-obliges-banks-to-tweak-anti-laundering-alert-management-communicate-with-regulators-experts/
16. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/media/2020/apr/Oliver_Wyman_Compliance_and_COVID-19_paper.pdf
17. https://fcced.com/coronavirus-aml-transaction-monitoring-54201400/
18. https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_iran.aspx
19. https://www.riskscreen.com/kyc360/news/fatf-encourages-technology-use-to-address-covid-19-challenges/
20. https://www.riskscreen.com/kyc360/article/another-kind-of-outbreak-covid-19-as-financial-crime-threat/
21. https://www.actionfraud.police.uk/covid19
22. https://complyadvantage.com/knowledgebase/corona-virus-transaction-monitoring/
23. https://www.moneylaunderingnews.com/
24. https://www.ballardspahr.com/alertspublications/legalalerts/2020-03-16-fincen-warns-about-covid-19-scams-and-requests-enhanced-comm-from-fin-institutions
25. https://gulfnews.com/business/banking/covid-19-uae-central-bank-warns-about-fraud-attempts-linked-to-coronavirus-scare-1.1585548428870
26. https://www.theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m
27. https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints-040220.pdf
28. https://www.whitecase.com/sites/default/files/2020-04/mitigating-risk-of-fraud-during-the-covid-19-crisis.pdf
29. https://www.mayerbrown.com/en/perspectives-events/publications/2020/04/financial-crime-compliance-and-risk-management-for-financial-institutions-and-other-market-participants-amid-the-covid19-outbreak
30. https://www.usatoday.com/story/tech/columnist/2020/04/04/coronavirus-scams-going-viral-attacking-computers-and-smartphones/2939240001/
31. https://www.telegraph.co.uk/technology/2020/03/17/tech-giant-team-battle-coronavirus-fraud-fake-news/
32. https://telanganatoday.com/tech-giants-join-hands-to-fight-corona-misinformation-fraud
33. https://www.theverge.com/2020/3/16/21182726/coronavirus-covid-19-facebook-google-twitter-youtube-joint-effort-misinformation-fraud
34. https://www.forbes.com/sites/ronshevlin/2020/03/23/a-list-of-fintech-firms-providing-free-technology-to-banks-during-the-coronavirus-crisis/#6f7c1f4c1b5e.
35. https://www.ispartnersllc.com/blog/coronavirus-covid-19-remote-auditing-compliance/
36. https://www.acacompliancegroup.com/blog/guidance-business-continuity-and-disaster-recovery-planning-coronavirus-disease-2019-covid-19
37. https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial

About the Authors

Amit Khullar

Amit is Senior Industry Principal with more than 20 years of experience in large transformation and consulting initiatives for banking and financial services clients. He is global head of Risk and Compliance consultancy practice of Infosys Financial Services unit.

Ketan More

Ketan is Principal Consultant with more than 20 years of experience in banking related IT. He heads Infosys AML CoE and has vast experience in AML, Anti-Fraud Operations and Data Analytics.

Naveen Srivastava

Naveen is Principal Consultant with 19 years of experience in banking, financial and IT enabled services. He is leading Infosys Oracle FCCM (Mantas) Practice with primary focus on compliance services viz. KYC, AML, ECM etc. He is responsible for building strategic initiatives around the practice and manages pre-sales and delivery for various Mantas engagements.

For more information, contact askus@infosys.com

Infosys®
Navigate your next