COVID-19 Crisis and Financial Crime Compliance:

Navigating Uncharted Territory

Banking & Financial Services

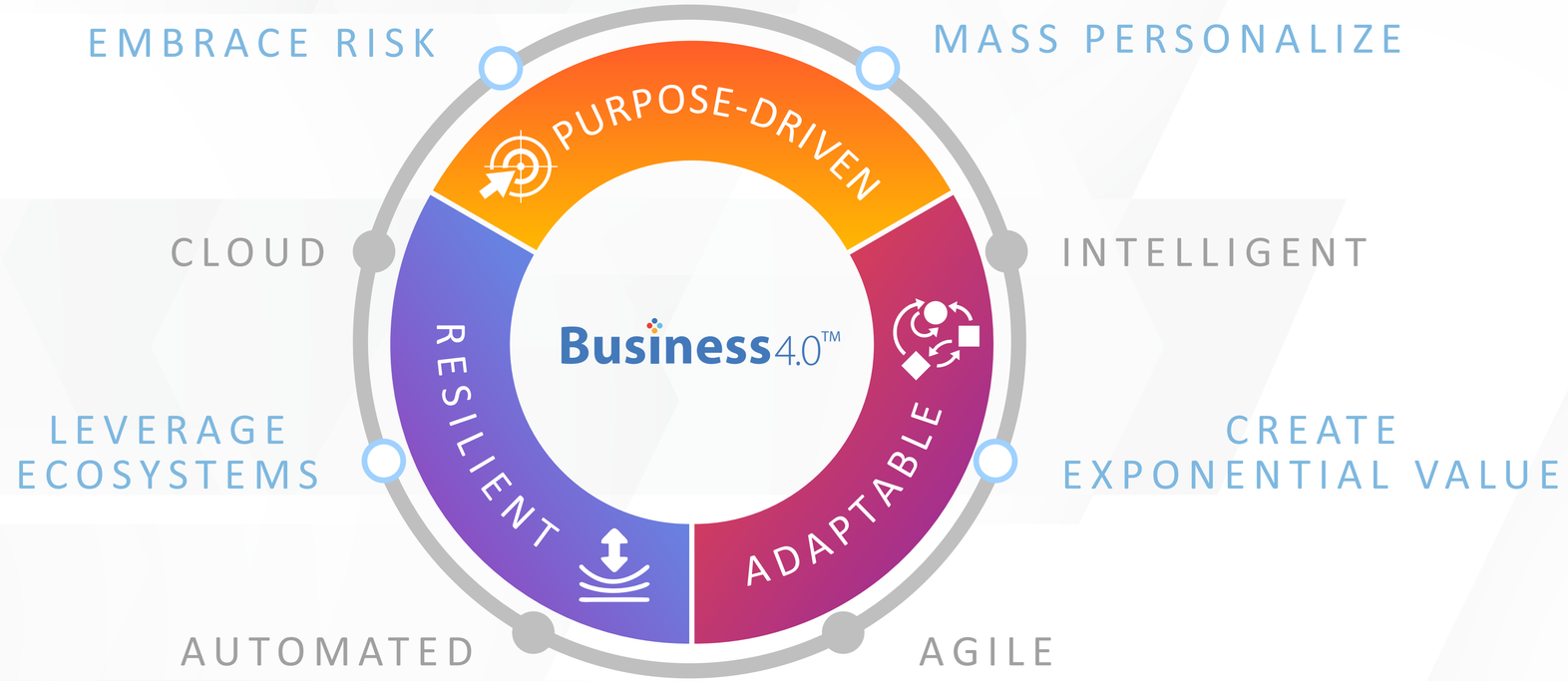
PURPOSE-DRIVEN

RESILIENT

ADAPTABLE

PURPOSE-DRIVEN, RESILIENT & ADAPTABLE

with Business 4.0™;



PURPOSE-DRIVEN

RESILIENT

ADAPTABLE

Abstract

As the world welcomed 2020 full of hopes for peace, progress and prosperity in the new decade, little did we know that an invisible microbe was already tormenting parts of China, and would invade the globe in a matter of weeks practically holding the world to ransom. Fact is indeed stranger than fiction. Life has changed. The world stands imprisoned, economies have stalled. Each individual, household, organization, industry, and government is trying to muster strength to endure this phase and return to normalcy. Amidst all this, we have learned to adjust to a new normal – staying at home, yet trying to live a normal life, by embracing everything digital. As painful a period as this is for all of us, there are criminals out there who are trying to take advantage of the crisis through scams, fraud, and money-laundering. How do we as individuals spot them, and how do banks prepare to stop such crimes that are generating new typologies in financial crime prevention? This white paper attempts to answer these questions.

Uncertainty Feeds Fear, Fear Creates Panic, Panic Fuels Irrationality

With the exception of essential services, everything is under lockdown putting livelihoods at stake and creating a lot of stress for people. Individual, organizational and societal behavior tends to diverge from the normal during stressful periods – fear and irrationality make people susceptible to Ponzi schemes and phishing. Additionally, governments are directing banks to advance funds to people who have lost their income to help tide over the crisis. In the prevailing scenario, banks may not be able to perform adequate due diligence on the authenticity of people/entities identified to receive the largesse increasing the possibility of the funds being handed over to those with mala fide intentions.

Technology has helped people stay positive in so many ways through this difficult period. From staying connected, to working from home yet seamlessly collaborating with colleagues, ordering essentials online, and staying updated on every bit of information available on the killer virus, technology has played a big role in retaining a semblance of normalcy during the lockdown. However, it is also technology that is being leveraged to swindle unsuspecting users by luring them to click on links that look benign but aren't – like COVID-19 precaution tips or sale of anti-virals. With a majority of the workforce across industries under lockdown and working remotely, the risk of being targets of cybercrime increases substantially. COVID-19 is the perfect storm that has made individuals, organizations, and societies vulnerable to the myriad cybercrimes.

Racketeering and counterfeit goods

With the world under lockdown and supply chains severely strained, racketeering and counterfeit goods rule the roost. Toilet paper, sanitizers and masks are being sold at unimaginable prices. Counterfeit 3M and N95 masks, medicines, sanitizers and many more such items are being sold through digital channels.

Fraud, cybercrime and social engineering

Several governments have announced relief packages worth billions as a part of the measures to help citizens and businesses in the wake of the pandemic. Such rescue packages and big payouts will provide a strong impetus to cybercriminals. Thousands of Coronavirus themed websites have sprung up. Fake mails mentioning World Health Organization, and government grants are being widely used by criminals to access personally identifiable information (PII) or extort money. Several charities have emerged for collecting donations to fund treatment and research around Novel Coronavirus; but many of them are a front for transforming ill-gotten money into legitimate wealth. In addition, such charities are recruiting hapless employment seekers into the ring who serve as the 'money mules' or conduits for moving these funds. Fraudulent investment opportunities promising juicy returns are also mushrooming preying on the fears of virus-impacted income uncertainties and duping innocent people of their money.

Dealing with the COVID-19 Crisis

Banks and financial institutions are racing against time to mitigate twin risks – the increased risk of missing real frauds and money-laundering cases due to the overwhelming volume of false alerts and the possibility of regulatory violation due to reduced staff strength or constraints caused by staff working remotely.

Emergencies such as the COVID-19 crisis just happen – no model can predict when they will occur or how deep and widespread the impact will be. However, what banks are witnessing now, in terms of drastic changes in customer behavior, can lay the foundation for a stronger framework for financial crime compliance.

New detection models for disaster scenarios

New detection models need to be designed for unpredictable circumstances including natural disasters. The models must have the capability to distinguish between legitimate crisis-driven changes in customer behavior and the illegitimate ones. The prevailing crisis will generate a lot of data on behavioral change specific to customer segments, demographics, and industries. This data can be fed into the existing detection models resulting in a more robust detection engine that incorporates scenarios that can be activated during disasters and pandemics. This will help avoid abnormal spikes in false alerts due to changed customer behavior in turn facilitating better risk management and reducing pressure on bank personnel.

New financial crime typologies for FCC frameworks

The Financial Crimes Enforcement Network (FinCEN) has released an advisory directing banks to remain alert for fraudulent transactions. FinCEN has also advised banks to adopt the typologies related to charities and benefits fraud, imposter scams, investment scams, and product frauds (covering fake or unapproved medical products being sold during COVID-19). FinCEN is also encouraging banks to mention 'COVID19' in SAR reports in cases where suspicious transactions are found linked to the Coronavirus crisis.[1] To comply with the FinCEN advisory, banks must incorporate new typologies that are emerging from the current crisis into their financial crime compliance (FCC) frameworks. The FCC detection engines should be enhanced with rules built for all such new categories of financial crimes. In addition, banks must define standard operating procedures to investigate such crimes. These new categories of crimes must be incorporated into management information systems so that the top management can take suitable actions including off-boarding of customers as appropriate.

1 Financial Crimes Enforcement Network (FinCEN), The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity, Mar 2020, Retrieved April 2020, https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions

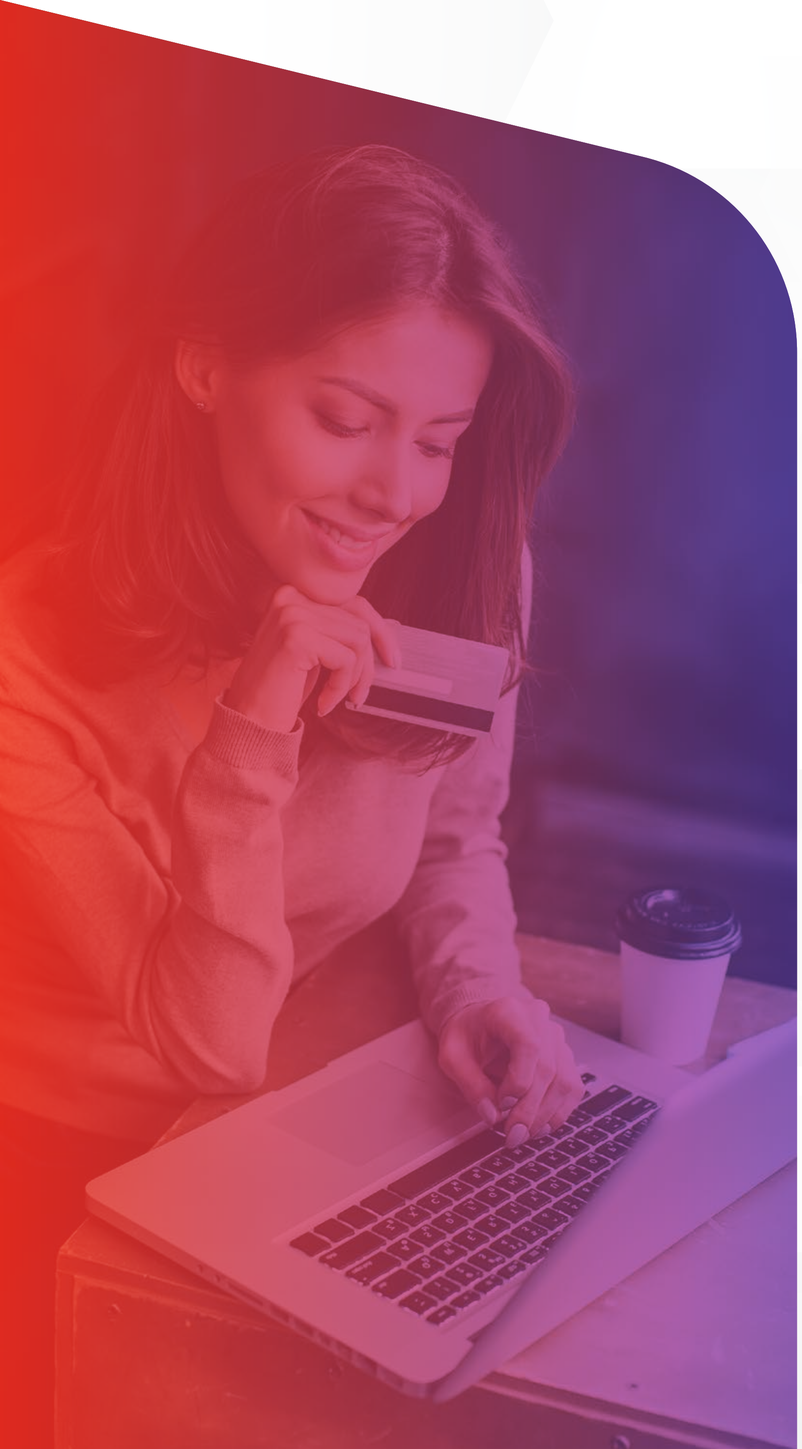
Adverse media screening

The COVID-19 situation has taught us that criminals are capable of finding several new ways of committing financial crimes and launder money during a crisis. Malpractices like hoarding, black marketing, and racketeering of essential goods in limited stock, price fixing, dishonest billing and so on thrive during emergencies. Banks must expand adverse media screening for negative news to cover these areas as well during disasters.

Digital identity and on-boarding

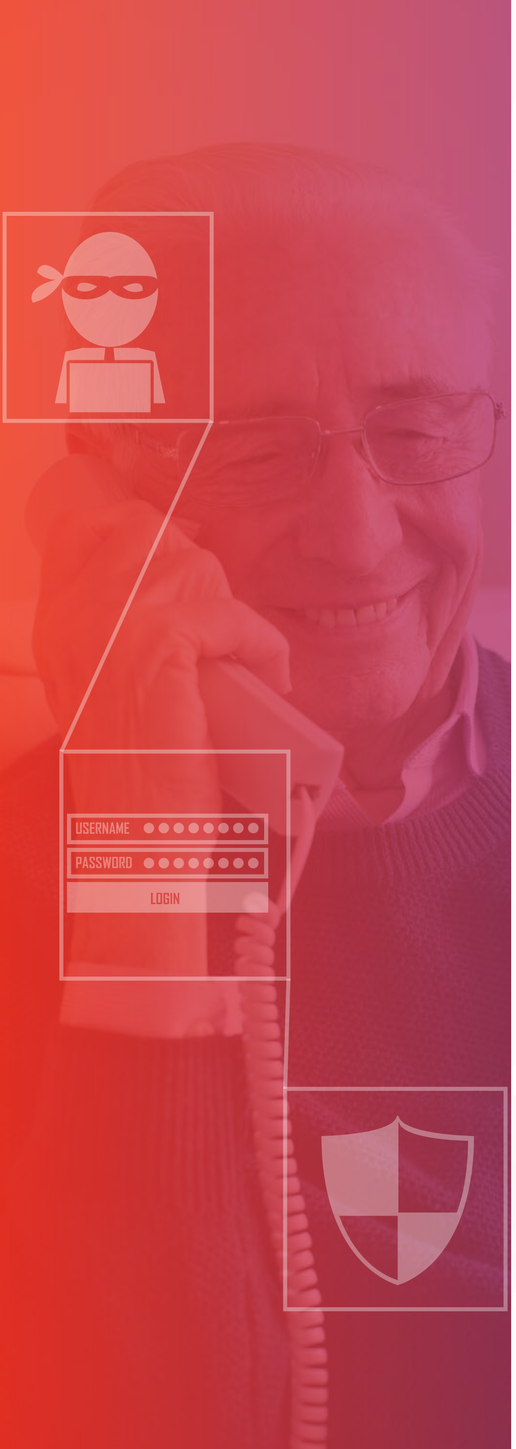
The Financial Actions Task Force (FATF) has recently released guidelines directing banks to explore the use of digital identities for fraud prevention and digital onboarding for reduced customer contact with bank branches in keeping with social distancing norms.[2] As digital channels are widely used during such disasters, banks must strengthen their screening and monitoring platforms to enable seamless performance even when volumes surge on a single channel. Regulatory technology (RegTech) solutions offer several options for enhanced compliance around customer onboarding as well as transaction monitoring for digital channels. Banks can consider investing in these technologies to avoid compromising on compliance even when FCC has to be manually handled. From mobile app based know your customer compliance, biometrics for fraud prevention, and customer self-service for auto-resolution of alerts to compliance data remediation, digital innovations can go a long way in ensuring compliance even in a crisis.

2 Finextra, FATF promotes digital ID during Covid-19, Apr 2020, Retrieved Apr 2020, https://www.finextra.com/newsarticle/35570/fatf-promotes-digital-id-during-covid-19



The Way Forward

Financial crimes have proliferated during the COVID-19 disaster, and banks must take measures to stop this from continuing or repeating. Strengthening FCC platforms, reviewing the performance to regularly fine-tune FCC detection models and, collaborating and sharing information on financial crime and criminals with peers and global regulatory agencies will help strengthen global compliance. Given the scale of the crisis and the scope for financial crime proliferation, banks must consider partnering with a trusted service provider to prevent fraud and remain compliant.



About the **Authors**

Sujata Dasgupta,
Head, Financial Crimes Compliance Advisory,
Banking, Financial Services and Insurance, TCS

Sujata Dasgupta heads the Financial Crimes Compliance Advisory, within the Banking, Financial Services and Insurance unit at TCS. With over two decades of experience across banking and IT services and consulting, Sujata also specializes in financial crime and regulatory compliance. She is a qualified Cost and Management Accountant (CMA) from The Institute of Cost Accountants of India (ICMAI) and a Certified Associate of the Indian Institute of Bankers.

Zeeshan Rashid (Zee),
Global Head, Risk and Compliance Advisory, Financial Services and Insurance, TCS

Zeeshan Rashid (Zee) is Global Head, Risk and Compliance Advisory and the LIBOR Transition initiative within the Banking, Financial Services and Insurance unit at TCS. He brings to the table over 19 years of industry experience in banking and consulting. His responsibilities include strategy, sales and pre-sales, advisory, mentoring, thought leadership, and consulting. He has authored a number of white papers in the area of risk and compliance and spoken at various seminars and business schools. Zee is a GARP-certified Financial Risk Manager (FRM) and holds a master's degree in business administration from the Institute for Technology and Management, Mumbai, India.

Contact

For more information on TCS' Healthcare solutions and services, please visit https://www.tcs.com/life-sciences-healthcare

Email: healthcare.solutions@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match.

TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at **www.tcs.com**

Corporate Marketing | Design Services | M | 06 | 20

PURPOSE-DRIVEN

RESILIENT

ADAPTABLE