COVID-19:

# Q2 summary of analysis highlighting the impact on financial services firms

Thomson Reuters Regulatory Intelligence

THOMSON REUTERS®

# Contents





With thanks to the whole Thomson Reuters Regulatory Intelligence team

# INTRODUCTION

This is the second report in Thomson Reuters Regulatory Intelligence's (TRRI) series of quarterly reports following developments in the financial services industry as a result of the COVID-19 pandemic; it covers Q2 2020. Like the Q1 report, this report is a collection of extracts from articles that have appeared on the TRRI site during Q2 2020. It focuses on the regulatory impacts of the crisis and is not intended to be a detailed chronology of its development.

At the end of Q1 the financial services industry was coming to terms with the implications of the pandemic. Business continuity plans were being implemented and regulators were beginning to make changes to allow the industry to adapt to the restrictions being imposed. The TRRI Q1 report[1] explored the good and bad practices emerging from firms' business continuity plans, explored the risks firms were having to manage and documented the changes regulators were making.

Q2 has seen the world shift again while trying to cope with this fast-paced and unpredictable virus. Whereas in Q1 firms were preparing for lockdown and economic hibernation, some countries are now preparing to reopen their doors and return to business as usual. Financial services firms are making cautious preparations to resume operating from offices and branches, albeit with health and safety restrictions in place and the knowledge that there will be a return to lockdown if there is a second wave.

This has posed new problems and enhanced existing ones. Q2 brought the financial impact on firms into sharper focus as annual accounts season was delayed and extended. Firms turned their attentions away from the black and white of the business continuity plan and focused more on what was needed to get up and running again.

The world is only a little clearer about when the pandemic will be fully over, which means continuing uncertainty for firms. At best Q2 was a transitional quarter that perhaps moved the industry from the beginning to the middle of the pandemic.

1 https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/reports/covid-19-q1-summary-of-analysis-and-insight.pdf

# PROGRESSING THROUGH THE CRISIS

## Effects on firms

In Q1, TRRI reported on regulators' early response to the crisis and their praise for the swift measures introduced in the early stages. As the pandemic has proceeded the effects on financial services firms have become clearer. In Q2, mainly through their annual accounts, many firms have begun to outline the impact the pandemic might have.

> "What about the banking sector? This sector is likely to be hit the hardest. Even the billion-euro rescue packages for the real economy will not be able to completely prevent some borrowers from defaulting in the coming weeks, months or years, perhaps."
>
> **Felix Hufeld,** president of the Federal Financial Supervisory Authority (BaFin). May 2020

In Europe, Deutsche Bank explained that travel restrictions and the decision to maximize the number of staff working from home during the COVID-19 pandemic might adversely affect business activities and their operations. The group has established extra controls and processes, such as additional reporting, to ensure relevant senior stakeholders including the management board are up to date. All this could affect the bank's Common Equity Tier (CET) 1 ratio, and Deutsche could fall modestly below its CET 1 target of at least 12.5% in upcoming periods, it said.

Credit Suisse has taken thorough measures on COVID-19 business continuity and had no major operating incident as 70% of its staff work at home. Redundancies are on hold during the pandemic, and the bank is in no hurry to get staff back into the office, although some are thinking of returning, said Thomas Gottstein, chief executive. Tier 1 leverage ratio was 5.8% at the end of the first quarter, up from 5.5% at the end of the previous quarter, benefiting from the decision by FINMA, the Swiss regulator, to temporarily allow local banks to calculate the leverage ratio without central bank reserves.

Standard Chartered Group's operational resilience has "never been more thoroughly tested" than during the pandemic. The bank is supporting staff to "work flexibly and adapt roles", with no coronavirus-related redundancies or furloughing, but levels of working remotely vary greatly. Operating income rose 13% from Q1 2019, but credit impairment increased by $878 million to $956 million. Underling profit before tax fell 12% to $1.2 billion.

The pandemic has tested HSBC and its staff, but the bank's operations have been highly resilient, said Noel Quinn, chief executive. A short-term hold on 35,000 redundancies to benefit business continuity has cost the group $380 million in foregone savings for 2020, recoverable elsewhere. "The COVID-19 pandemic is testing us all in ways we could not imagine," Quinn said. "It is causing huge disruption and stress." The group's reported profit before tax fell to $3.2 billion, down 48% from Q1 2019, due to the pandemic and the drop in oil prices.

In the United States, Capital One was one of the large banks most exposed in the early stages of the shutdowns. The bank reported a $1.3 billion first quarter loss, after loss reserves of $5 billion for anticipated credit payment problems. The reserves were in line with banks nearly 10 times its size. Capital One doubled the loss provisions for most of its consumer-based credit portfolio, with the largest area of concern centered on auto loans that require relatively larger monthly payments than credit cards or low-dollar consumer loans.

Insurer Travelers Cos Inc reported a 25% drop in quarterly profit and warned that potential claims tied to compensation coverage for furloughed and laid-off employees would hit results for the year. The company also booked catastrophe losses of $333 million in the first quarter, compared with $193 million a year earlier. The rise in catastrophe losses was mainly due to a string of tornadoes that tore through Nashville, Tennessee and surrounding counties early in March, with several U.S. regions also seeing wind storms and winter storms.

Travelers, often seen as a bellwether for the insurance sector because it typically reports before its industry peers, reported pre-tax net charges of $86 million related to the pandemic and related economic turmoil. Net income fell to $600 million in the latest quarter ended March 31, from $796 million a year earlier. Core income was $2.62 per share, lagging estimates of $2.85 per share, according to Institutional Brokers' Estimate System (IBES) data from Refinitiv.

National Australia Bank (NAB) made provision for a long-drawn-out economic downturn and looking to reduce costs as it focuses on capital-raising to cover rising bad debts, following the pandemic. NAB announced that it had

reduced the interim dividend by 64% to 30 cents per share, to help improve its balance sheet position and shore up the greater number of credit impairments. At the same time, it is dealing with thousands of distressed customers who are applying to defer mortgage payments and business loans. The bank is also fending off a series of regulatory actions in the Federal Court of Australia in relation to "fees for no service", as well as numerous class actions by law firms. By all accounts the bank is getting ready for one of the most turbulent times in its 38-year history.

DBS, Singapore's largest bank, has strengthened its operational resilience by expanding its digital capability and enhancing its cyber-security framework as the pandemic has played out, the bank said in the latest observations report issued by its chief executive. DBS said more than 90% of its relationship managers, 70% of its traders, 99% of its developers and 50% of its operational staff have been working from home since the onset of the circuit breaker in the city-state on April 7.

Canada's Office of the Superintendent of Financial Institutions (OSFI) has taken several measures to offset the effects of the market instability caused by the COVID-19 pandemic. Many of these measures address the operational challenges affecting the regulator and the deposit-taking institutions it oversees, including regulatory filing extensions and the delay of previously planned regulatory changes, while others build upon years of regulatory preparations for the kinds of scenario now unfolding.

adapting to the pandemic. The regulator has started to focus on the longer-term impact, said Megan Butler, executive director of supervision- investment, wholesale and specialists.

"We have already taken rapid action to respond to the immediate shocks of coronavirus," Butler said.

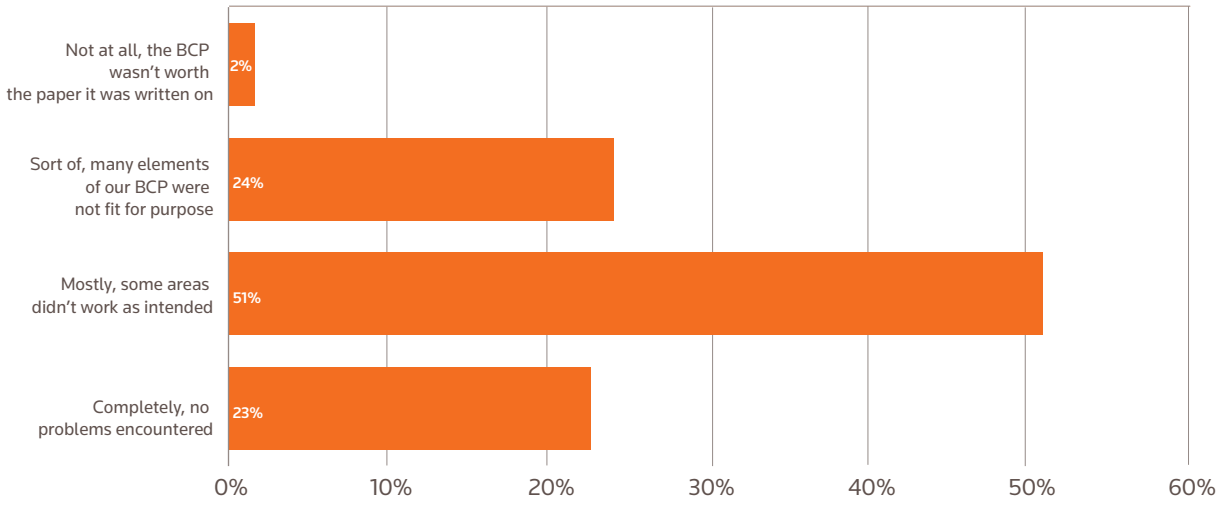
"Acting with speed has been the absolute priority, but as we adapt to the long-term impact of coronavirus, we have already begun to transition from the immediate incident response toward focusing on longer-term impacts and our strategy for tackling these," she said in a keynote speech.

The FCA expects all firms to have contingency plans to deal with major events, and that these plans have been tested properly, Butler said. The regulator is reviewing the contingency plans of a wide range of firms. This has included assessments of operational risks, firms' ability to continue to operate effectively and the steps they are taking to serve and support their customers, she said.

During Q1 TRRI also hosted a couple of webinars to gauge whether firms felt they had managed the impact of the pandemic adequately. The first was aimed at a European and Middle East audience and the following poll was carried out.

The poll showed that, by and large, financial services firms' business continuity plans had worked satisfactorily. Nearly 51% of respondents said the invocation of their plan had mostly worked, although there were problems in some areas. A very encouraging 23% of firms had had no problems as all.

**Did your Business Continuity Planning (BCP) work in practice?**




Source: Thomson Reuters Regulatory Intelligence, Experts Talk webinar series. Episode 1: COVID-19 and Business Continuity Planning. April 2020

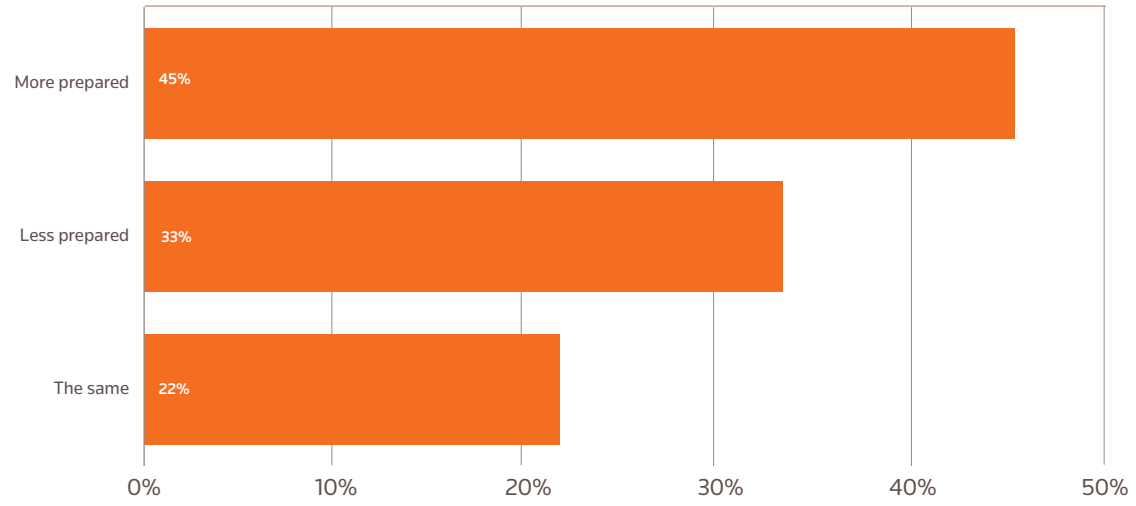
### But no major crises, yet

The UK Financial Conduct Authority reported that business continuity appeared to be working in operational terms, glitches have been worked through and firms seemed to be coping and

Another Q2 webinar on financial crime during the pandemic included a poll to assess preparedness in the industry after COVID-19.

This poll showed that most respondents felt more prepared, but a worrying third of respondents felt less prepared.

**In your current role, do you feel more or less prepared for the future in your industry after COVID-19?**




Source: Thomson Reuters Regulatory Intelligence, Financial Crime during COVID-19: Tackling fraud, scams and misinformation – June 2020

As the financial services industry moves through this pandemic and firms begin to return to business as usual, firms will begin to progress lessons learnt exercises.

This has already started in the regulatory community. The Financial Stability Board (FSB) is asking financial institutions whether they have learnt any lessons from the pandemic and related cyber activity which have contributed to their cyber incident response and recovery practices. The incidents include theft and fraud, but could also be political or espionage, involving threat actors ranging from criminal syndicates to nation states, and the roles of the board and senior management are specified.

The impact of the pandemic is at the heart of the FSB's first question in its consultation, which sets out the roles and responsibilities of the board. This includes empowering senior management to take decisions to deploy cyber incident response and recovery activities.

Efficient and effective response to, and recovery from, a cyber incident are essential to limiting any financial stability risks, the FSB said in the consultation document, "Effective Practices for Cyber Incident Response and Recovery", which includes a toolkit of effective practices to assist financial institutions.

# GOVERNANCE

"Good governance, proper conduct and continuous compliance to capital market regulations are imperative to the functioning of capital market intermediaries."

**Syed Zaid Albar,** chairman, Securities Commission Malaysia. April 2020

With the effects of the pandemic becoming clearer, the focus of the industry has turned toward how firms will control risks in future. A large part of this is governance and how firms are set up to manage the incident at hand. During Q2 TRRI published a number of articles on firms' governance during the pandemic.

BP&E Global suggested that:

- Boards which were kept informed of, and involved in, scenario planning fared better and helped support and guide executives, as appropriate.
- Firms which communicated promptly with customers and staff to provide reassurance were less inundated with queries from worried people and gained a public relations advantage.
- Boards which were distant or regularly given the "rose-tinted" view from the executive received a nasty shock and were less able to respond quickly.

BP&E Global reported that one firm carried out a pandemic-focused scenario test more than a year ago. The surprise for that firm back then was that it had a back-up server in a remote building, together with access to that building. It realized, however, that if none of the staff could be together during a pandemic, such a facility was of no use. This particular firm returned from the away-day, at which the implications had been thoroughly tested and reviewed, and immediately arranged to change over to a cloud-based system.

When the pandemic hit, therefore, IT was not a problem and remote working was a smooth transition to make. The only aspect that had not been fully tested across the whole business was communication en masse by video conference. Some systems work well for up to four people (if it is necessary to see all those people in a meeting at once on the screen) but beyond that some packages did not enable all attendees to be seen.

For the next board meeting the firm changed to another video conference provider, which enabled the whole board and attendees all to be seen at once on screen (in their various locations). It was easy to see who was speaking, and when, and therefore for people to avoid speaking over one other.

Overall, BP&E Global found:

- Those firms where operational resilience had been thoroughly tested fared better, especially where the board had been involved to some degree.
- Firms with older and more unwieldy IT systems suffered more and were much slower to respond.
- Those firms which had previously scenario-tested a pandemic fared better.
- Firms where agile working was already in place fared better and found it easier to adjust.

Operational resilience used to be the poor relation or boring part of risk management in most people's minds, with the more exciting risk management ascribed to fraud and more tangible risks. Regulators have long been asking firms to pay more attention to operational resilience, which the FCA's Butler, has defined as: "... the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions ...".

TRRI reported that the aftermath of the COVID-19 crisis will test firms' Senior Managers and Certification Regime (SMCR) compliance programmes, when regulators examine how firms and their senior managers, responded to everything from business continuity planning to treating customers fairly. The FCA said as much in its recent business plan. "We will remain vigilant to potential misconduct. There may be some who see these times as an opportunity for poor behavior – including market abuse, capitalising on investors' concerns or reneging on commitments to consumers. Where we find poor practice, we will clamp down with all relevant force," the FCA said.

This crisis is the first where the FCA and the UK Prudential Regulation Authority (PRA) will have access to firms' responsibility maps and individual responsibility statements. It will therefore be clear which firms have implemented SMCR properly and where responsibility lies

for failures. A rise in enforcement action and customer litigation is anticipated once a kind of normality resumes and the regulator is in a position to assess any damage.

Also in the UK, HM Treasury wants more ambitious diversity targets at financial firms as the pace of hiring women to top jobs is too slow. HM Treasury launched a Women in Finance charter in 2016 in a bid to improve diversity in the financial sector: in 2015, just 14% of executive committee members were women. More than 370 firms with more than 900,000 employees in total have signed up to the charter and committed themselves to voluntary diversity targets. A review by New Financial, a think tank, of 187 of those firms found that only a third have met or exceeded their own targets.

Women make up 32% of senior management on average, still short of the 33% minimum target HM Treasury would like to see for all signatories, the review said. The review found only 26 signatories have set themselves the goal of parity between men and women in senior roles, and that nearly 60% of firms have set a target of 33% or above for female representation.

"The COVID crisis has shown just how quickly companies can adapt," New Financial said. "There is an opportunity now to challenge legacy thinking in all areas (not just flexible working), cement diversity as a strategic business priority and accelerate the pace of change."

# RISK

"...given the exceptional uncertainty generated by the current crisis, we expect insurers to increase their monitoring of the additional risks presented by COVID-19, and where necessary to update their risk and capital assessments accordingly".

**Charlotte Gerken,** executive director of insurance supervision, Bank of England. May 2020

## General

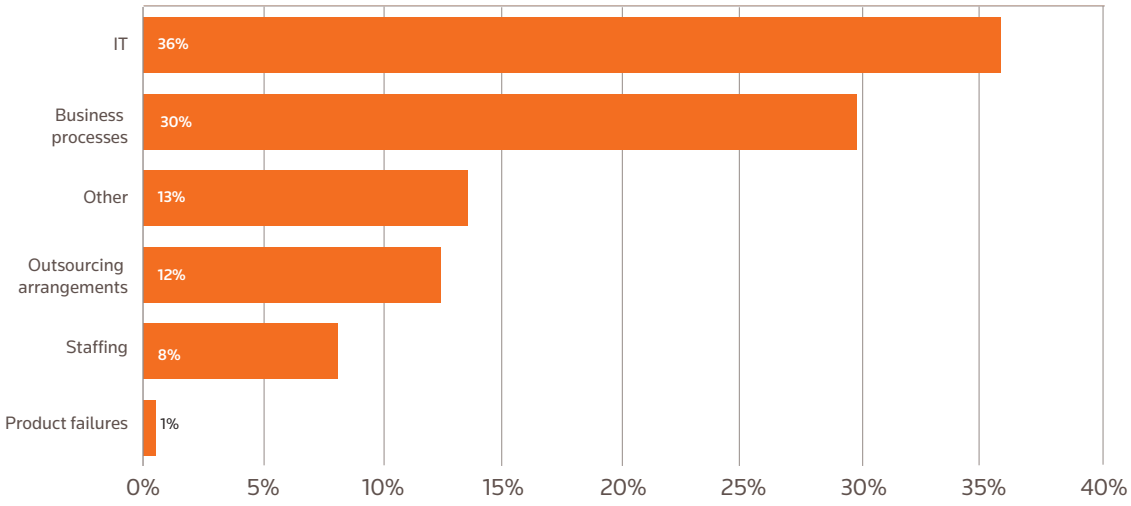
During the TRRI webinars on the Q1 report, participants were asked about the risks they encountered when implementing business continuity plans.

People risk and operational resilience came out as the top operational risks to which firms have been exposed. In many firms' risk taxonomies, people risk will include health and safety. Some firms will have health and safety as a separate risk category, but for this exercise health and safety was included under people. Firms will be highly sensitive to following social distancing and hygiene measures and will be putting controls in place to ensure the continued wellbeing of their employees. Operating these measures alongside their operational resilience plans, which are intended to keep the firm running, poses additional risk.

From a conduct risk perspective, the risk of regulatory non-compliance probably relates to a number of things. First, adapting to changes in regulations that are being made during the pandemic; secondly, the volume of regulations to be complied with; and, finally, the clarity and understanding of some of those regulations when applying them to a firm's particular situation.

TRRI's Cost of Compliance Report 2020[2] found compliance officers identified greater regulatory change as the number one challenge for 2020, and it was seen as the second biggest challenge at board level.

**What were the key issues or challenges encountered in using your BCP?**




Source: Thomson Reuters Regulatory Intelligence, Experts Talk webinar series. Episode 1: COVID-19 and Business Continuity Planning. April 2020

2 http://financial-risk-solutions.thomsonreuters.info/Cost-of-Compliance-2020

The heightened risk that customers may be treated unfairly, including the potential effect on vulnerable customers, is another reason for the emphasis regulators have placed on this area. Regulators have reminded financial institutions to continue to treat customers fairly during the crisis; particularly the insurance and banking sectors. The UK FCA has moved to ensure firms make provisions for vulnerable customers with facilities to strengthen the continued access to cash, and payment holidays for those with loans and mortgages.

Fund managers will also need to navigate some unprecedented systemic risks, according to the latest World Economic Forum (WEF) Global Risks Report. Banks and asset managers will need to pay close attention to a broader array of operational and non-financial risks for an extended period, the report said.

Some of the main systemic risks include technological disruption, geopolitical stability, climate change, demographic shifts, water security and low and negative real long-term interest rates. These are challenges which financial services firms may not have considered as deeply in the past. On the other hand, organizations that pay attention to these risks may be able to thrive in a more complex operating environment.

As part of WEF's plan to help financial services firms translate these risks into opportunities, the report introduced a six-step governance framework to foster a better investment environment. These six steps are: understanding, collaboration, design, investing, transforming and monitoring.

## Prudential and credit risk

Australian banks doubled their lending to the most leveraged homeowners just as the country shut its economy due to the pandemic, putting them at risk of acute mortgage stress if prices fall as predicted.

The UK PRA issued a "Dear CEO" letter to banks providing guidance on the regulatory and accounting treatment of mortgage borrowers who take or extend a mortgage holiday due to experiencing temporary payment difficulties caused by the pandemic. This is the second such letter and followed an update from the FCA on its mortgage holiday guidance in relation to how lenders should treat borrowers at the end of the initial deferral period.

With banks assessing the capital and accounting treatment of the various ways in which the initial mortgage holidays might end, the PRA said it was sending the letter to update its earlier guidance issued to help firms implement the requirements in a consistent way.

The U.S. Securities and Exchange Commission (SEC) has opened a wide-ranging, cross-agency inquiry into what it called the "mechanistic" impact of debt ratings, benchmarks, index rebalancing and other investment strategies that could lead to "forced divestment" of assets at a time of market volatility and economic uncertainty. The SEC said the inquiry was aimed at understanding the potential for further market disruption fuelled by downgrades or index changes, and whether it should act to reduce the impact. It offered no specific ways it might intervene.

The U.S. Federal Reserve said it will continue to rely on a stress test built before the onset of the coronavirus pandemic to set big-bank capital requirements but will make use of pandemic-specific analysis to inform whether banks can pay out funds to investors.

## Cyber security

Firms' risk of cyber attack will remain high despite some shifting operations back to the office or moving to hybrid working models. Cyber criminals may launch back-to-the-office spoofing campaigns and seek to exploit desktop systems which have not had security patches installed for months. Firms should remain vigilant to insider threats, cyber security officials told TRRI.

Once lockdowns were announced, firms rushed out infrastructure — virtual private networks, servers, laptops — to enable working from home, which introduced new security challenges. Overnight, firewalls used to secure the corporate perimeter were expanded to protect a distributed network of home workers. That shift brought a wave of cyber crime, particularly phishing attacks, and the return to more normal working conditions will provide criminals with similar opportunities.

The financial services sector in Singapore has become one of the country's most vulnerable sectors to digital and cyber-crime risk, despite having relatively mature cyber-security infrastructure. Lee Shih Yen, senior vice president of Ensign Labs at Ensign InfoSecurity, told TRRI the rapid growth of e-commerce had made the financial sector a lucrative target.

"As the popularity of e-commerce continues to grow, so does the interest of threat actors in attacking and breaching it," Lee said. Digital or cyber attackers often attempt to compromise the financial service provider's online payment applications to steal customers' credit card information, Lee said.

The firm's latest report unveiled Singapore's top cyber threats in 2019. Malware-related activities had increased by more than 300% in the city-state in the first six months of last year, it said.

"This was evident from prevalent detections of malware with credentials theft attributions, including Trojan viruses, to steal financial data for illicit monetary gain."

The report said 70% of organizations in Singapore's financial sector were affected by malware-related threats in 2019. These attacks can be almost invisible to conventional signature-based cyber-security solutions, Lee said.

## Financial crime

Now more than ever, banks need to raise the bar and start to invest in and implement technology-enabled solutions to improve how they monitor and combat financial crime.

**Rani Kamaruddin,** partner, head of AML and sanctions at KPMG China in Hong Kong, in KPMG's Hong Kong Banking Report 2020, "Adapting to a New Reality".

This TRRI Q2 report purposefully devotes more space to financial crime risk. It is an area that has received a lot of attention from regulators, and about which TRRI subscribers have requested more information. A schematic at appendix 1 provides more detail on financial crime risks and controls.

Perpetrators of serious crime make 110 billion euros' profit annually across the European Union, with only 1.1 billion euros of assets retrieved, and some are now adapting their money laundering skills to COVID-19, Europol said. It launched its new European financial and economic crime centre to "follow the money".

More than half of public and private sector anti-financial crime professionals surveyed reported an increase in risk resulting from the pandemic, in part due to the IT challenges associated with remote working and delayed reviews of monitoring system alerts, according to a report by FinScan, an anti-money laundering solutions firm. FinScan conducted a survey of anti-financial crime compliance professionals to establish how they are dealing with the pandemic and areas where additional risk has emerged.

The survey included financial institution compliance professionals, auditors and consultants, regulators and law enforcement authorities, and vendors. Overall, 53% of respondents reported a perceived increase in risk exposure. The regulator and law enforcement authorities group had the most "pessimistic" view, with 43% — the highest among all groups — stating that risk exposure increased "significantly". Only 13% of compliance professionals saw a significant increase.

The Financial Action Task Force (FATF) has warned of unintended new threats from COVID-19-related crime and the impact on money laundering and terrorist financing risk. These include the risk that some financial institutions are unable to verify customers' identity remotely. Certain population segments may be less familiar with using online banking platforms, and therefore more susceptible to fraud, the standard setter said. "Reports indicate that online bank fraud targeting financial or account information is on the rise."

BaFin, the German regulator, has said it will tolerate simplified customer due diligence for the identification process, as set out in s 14 of the Money Laundering Act (Geldwäschegesetz (GwG)), during the COVID-19 pandemic. Should more serious money laundering risks come to light, however, appropriate additional measures must be taken at a suitable time.

The pandemic could prove to be a "tipping point" for the development of an effective digital identity framework for the financial sector, senior AML, legal and banking figures have predicted. The rapid pivot toward non-face-to-face and digital financial services in recent months has triggered a new wave of interest in digital ID solutions, they said. Regulators are also focusing on this, following of FATF's guidance on COVID-19, money laundering and terrorism financing risks.

A new era of post-pandemic money laundering is beginning to open up, as cash payments diminish. HSBC has drawn attention to a shift from cash payments, which enables illicit activities in "these trying times". Money launderers have not been defeated, however, and Europol has said that, post COVID-19, new strategies might include laundering into art and property, and that criminals will continue to abuse capital markets to layer and integrate criminal proceeds.

UK Finance said the pandemic had accelerated already detailed discussions about maintaining the role of cash for those that need it. "But it's too early to understand what the full impact of COVID-19 and lockdown will be on the use of cash," a spokeswoman said.

Even so, Europol has predicted the importance of cash as a payment medium and the availability of cash-intensive businesses will diminish. Money launderers may therefore look to other options to launder money in the longer term, it said in a recent report, "Beyond the Pandemic: How COVID-19 will Shape the Serious and Organized Crime Landscape in the EU".

Other areas highlighted by TRRI during Q2 included:

- Phoenixing — The UK FCA is attempting to limit "phoenixing", a practice whereby firms or individuals deliberately seek to avoid their liabilities to consumers or a poor conduct history by closing down, only to re-emerge in a different legal entity. Phoenixing has been a long-time problem which the regulator has been largely powerless to stop, and which it now fears will get worse as a result of COVID-19.

- Speed of SARs —The speedy processing of suspicious activity reports (SARs) related to COVID-19 is the main priority of the UK Financial intelligence Unit (UK FIU), said Ian Mynot, who heads the unit. The UK FIU, part of the National Crime Agency (NCA), has received SARs "in the low hundreds" connecting money laundering and fraud with the pandemic. Concern about fraudulent sales of personal protective equipment (PPE) and other COVID-19-related items has led the unit to treat coronavirus-related SARs with high priority.
- Mule activity — The National Crime Agency (NCA) has found possible mule activity in a recent increase of suspected fraudulent claims for COVID-19 government priority schemes, it said. Europol has separately identified that mules are linked with organized crime groups, including "middle management" money laundering experts in Europe. There is an enhanced risk of mule activity at a time of non-face-to-face know-your-customer checks, including from government loans issued in a hurry to existing and new clients, said Michael Knight-Robson, senior manager, BDO. Banks can be flexible in their KYC checks related to government lending, as they would be with other customers, he said.

Authorities in Denmark have pledged closer cooperation following concerns that criminals may be using the pandemic to facilitate fraud and find new ways of laundering money. The country's financial intelligence unit has teamed up with the tax authority and the companies register to monitor financial flows more closely, to look out for unusual or suspicious activity. The authorities said the lockdown and financial aid packages doled out by the government to aid businesses amid the pandemic had caused a rise in technology-related financial crime and had given rise to other opportunities for financial crime.

In the United States, banks have fallen under greater scrutiny from a wave of fraud cases already emerging from the $500 billion U.S. economic relief program, through which banks lend to distressed borrowers under government-backed terms to revive the economy. Banks have already been thrust into the middle of the string of cases aimed at borrowers' fraudulent applications in what promises to be a prolonged period of legal proceedings for firms that could rival the clean-up following the 2008 financial crisis. These include:

- Numerous instances of borrowers securing PPP funds and depositing them in bank accounts which then are put to banned uses such as lavish personal expenses.
- A $1.7 million loan approved for an individual in the film industry already widely known to have been the target of a major fraud case.
- Money movement in a number of the fraud cases that could point to suspicious activity that would have to have been reported under AML law.
- Loans to stressed clients to help them repay troubled debts, a potential violation of PPP terms and banking rules on conflicts of interest.

The Singaporean authorities have warned investors to be alert to the financial fraud risk posed by unregulated online trading platforms. The Monetary Authority of Singapore (MAS) and others have stepped up their investigations of malicious conduct in these markets. "Most unregulated online trading platforms are located outside Singapore and pose a greater risk of fraud [to our investors] since the credibility of their operations cannot be easily verified," the regulator said.

MAS teamed up with the Singapore Police Force (SPF) and Infocomm Media Development Authority (IMDA) to take action against unauthorized trading service websites such as Arotrade. The SPF investigation revealed that Arotrade had been linked to fraudulent marketing tactics, including the use of fake news articles falsely claiming that prominent individuals, such as holders of political office in Singapore, had endorsed investments in cryptocurrency. This misled investors and channelled them to Arotrade's website, the regulator said. Investors who used the site had subsequently discovered unauthorized trades in their accounts or encountered difficulties when they withdrew their money, it said.

The U.S. SEC has urged investment advisers to address the heightened risk of insider trading amid the pandemic. Making sure the firm's code of ethics is sufficiently strong, that personal-trading policies are appropriate and that training programs are updated to reflect the pandemic are all good places to start.

In another example, U.S. authorities have charged a 36-year-old Chinese national in Manhattan with scheming to win $20 million in funds for fictitious companies involved in COVID-19 products and services. Four out of five banks turned down him down for loans on suspicions of fraud, but one application was funded by the Small Business Administration. The U.S. Attorney in the Southern District of New York charged Muge Ma, who took the name Hummer Mars when he became a permanent U.S. resident, with multiple counts of bank fraud and making false statements to the banks and the Small Business Administration.

The U.S. Treasury Department's anti-money laundering unit issued an advisory warning financial institutions about medical scams related to the COVID-19 pandemic, including red flags compliance officers should be aware of, and clarifying suspicious activity reporting expectations. FinCEN's medical scam advisory was based on data gathered from Bank Secrecy Act filings, such as SARs filed by financial institutions, as well as information provided by law enforcement partners, FinCEN said

## Conduct risk

Insurers have come under the spotlight for their approach to claims. Many policies will not have had pandemics of the nature of COVID-19 built into insurers' risk assessments and term and conditions, and so many claims made, across all types of policies, are being rejected.

The UK FCA is challenging this approach and has sought clarity from the courts on whether the wording of some insurance policies should provide cover during the pandemic; the ruling was due to be made at the time of this report going to press. It has selected 17 examples from business interruption (BI) insurance policies used by 16 insurers, eight of which were asked to take part in the court case: Lloyd's of London insurers Hiscox, Arch, Argenta and MS Amlin, as well as RSA, QBE, Zurich and Ecclesiastical. Hiscox, RSA and QBE will take part in a UK test case to decide whether their policies should pay out millions of pounds to companies hit by the pandemic.

The Australian Securities and Investments Commission (ASIC) has written to insurers asking them to handle claims with utmost good faith and to deal with complaints "genuinely, promptly, fairly and consistently" during the

### Top 10 frauds to be aware of during the COVID-19 pandemic

Source: Thomson Reuters Regulatory Intelligence. Top 10 frauds to be aware of during the COVID-19 pandemic, by Patrick Rappo, Katie O'Hara and Calum Ablet, DLA Piper

| | |
|---|---|
| **Increased risk of cyberattacks** | Current events are likely to have a negative impact on companies' cyber security position. The existence of significant financial and operational challenges may lead to the de-prioritisation of cyber security and planned IT security improvement programmes being put on hold. In addition, the increased use of remote access tools by employees while working from home increases the risk of cyberattacks.<br><br>Malicious cyber actors can take advantage of these changes by:<br>• targeting remote access systems with denial of service attacks, seeking to disrupt business operations or to extort money<br>• Increasing phishing attacks<br>• Infiltrating home WiFi networks and accessing IT systems via VPNs |
| **Phishing, whaling and smishing attacks** | "Phishing" is the use of fake emails or web links to obtain sensitive information about victims, such as passwords, usernames or bank account details. Phishing can also be used to deploy malware. "Whaling" is similar to phishing but is highly targeted and aimed at senior executive-level individuals. For example, a senior executive may receive a fraudulent email from what appears to be a trusted supplier, partner or employee within their organisation requesting a transfer of funds. This type of activity has seen huge returns for fraudsters. Finally, "Smishing" is a phishing-style fraud carried out via SMS.<br><br>Regulators have issued warnings about such schemes to individuals, but dangers to businesses and their investors are equally increased. Barracuda reported a recent spike in COVID-19-related phishing attacks since the end of February: 77% were scams, 22% were brand impersonation, 1% business email compromise. |
| **Account takeover fraud** | Account takeover fraud occurs when a fraudster accesses an individual's (e.g. an employee's) account and uses the account to carry out unauthorised transactions or gain access to confidential information. Fraudsters can obtain account details using various techniques, including phishing, smishing, data breaches and the use of malware. |
| **CEO fraud/ impersonation fraud/business email compromise fraud** | CEO fraud and impersonation fraud exist where individuals inside an organization receive emails purporting to be from a senior executive, instructing the transfer of money to a fraudster's account or requesting financial information. This may be carried out in one of two ways:<br>• Name spoofing – uses the name of the CEO but a different email address (which may be similar to the company's email address).<br>• Name and email spoofing – the CEO's email address is compromised and attacker uses the CEO's name and correct email address.<br><br>The pandemic has increased the risk of both CEO and impersonation fraud as employees work remotely and this can be used as justification for unusual and non-routine payment requests. Alternatively, emails or calls may purport to be from the company IT team and are designed to obtain passwords or enable malicious software to be downloaded onto a company's IT systems. |

| | |
|---|---|
| **Invoice fraud** | Invoice fraud occurs when fraudsters send communications purporting to be from company suppliers, asking for the supplier's bank details to be changed to re-route money to fraudster's bank account. Related to this is "invoice hijacking", where a fraudster serves a false invoice on a business after positioning itself in the middle of correspondence between the company and one of its suppliers. This is often achieved through email hacking and observing patterns of behavior and correspondence.<br><br>There is a greater risk of invoice fraud and hijacking during the pandemic due to:<br>• More employees working from home, and the resulting IT security weaknesses.<br>• The pandemic making it easier to justify changes in payment details.<br>• Employees already being distracted as a result of changes to working routines. |
| **Investment fraud** | With interest rates low and volatile stock markets, fraudsters can take advantage of companies seeking higher-return investments or financial safe havens. Fraudsters may attempt to induce businesses to buy or sell investment products on the basis of false information. For example:<br>• "Good cause" investments – fraudsters seek investment for good causes such as the production of sanitiser, manufacture of personal protection equipment or new drugs to treat the virus, with the promise of high returns.<br>• "Pump and dump" schemes - an attempt to boost the price of a stock via false pandemic claims and later selling the stock at the inflated share price.<br>• Fraudulent investments offering hedging against stock market volatility. |
| **Fraud in the supply chain** | The pandemic has put more pressure on many companies' supply chains, for example: closed borders in certain jurisdictions; suppliers invoking force majeure clauses; a shortage of components and raw materials. This can increase the risk of fraud in a variety of ways, including:<br>• Reliance on alternative suppliers.<br>• By-passing of controls and due diligence.<br>• Risk of improper payments to "grease the wheels". |
| **Insider fraud** | Insider fraud occurs when a current or former employee, contractor or any other party who had access to data (often confidential information) commits this fraud by misusing the aforementioned data. The insider may seek to profit from the stolen data, for example, by selling the data or using the information to make investment decisions.<br><br>During the pandemic, financial institutions may be forced to make elements of their workforce redundant, or reduce working hours. Disgruntled employees facing redundancy may look to remove intellectual property, gain financially or otherwise cause reputational or financial damage to their employers. |
| **Advance fee fraud** | When carrying out advance fee fraud, fraudsters usually pose as the government or the employee of a business. The fraudsters require businesses to pay a fee before receiving a product, service and/or money. After paying the fee, the victim does not receive the item for which they thought they were paying for.<br>Examples include:<br>• Fraudsters may exploit short-term financial struggles caused by the current situation and ask for an upfront fee when applying for credit that the company never receives.<br>• Fraudsters may impersonate local authorities or government bodies and seek to take advantage of companies seeking assistance from government support schemes by requesting an advance fee in exchange for assistance. |
| **Associated crimes** | Fraudulent activities such as those previously listed come with a number of associated risks, for example:<br>• Employees seeking to cover up internal fraud may commit offenses such as accounting misstatements or misleading auditors.<br>• Acts committed in the supply chain may expose companies to criminal liability under S7 of the UK Bribery Act 2010 for "failure to prevent bribery" e.g. facilitation payments.<br>• Failure to conduct adequate due diligence on counterparties may create money laundering risks.<br>• The potential for reportable regulatory breaches which may result in increased regulatory supervision of the firm and/or regulatory enforcement action. |

**How to guard against the greatest risk of fraud**

- Ensure that remote access systems are patched and secure for employees working from home.
- Have adequate security controls which are able to withstand distributed denial-of-service attacks.
- Ensure the cyber-security team is able to continue working effectively in the current circumstances.
- Providie employees with guidance and training on the potential fraudulent activity which may affect the business, such as how to avoid cyber-security breaches and how to spot suspicious activity.
- Engage audit committees at an early stage to ensure appropriate financial controls are in place.
- Document how and why financial decisions are made and make it clear what acceptable practice is.
- Ensure employees use the Financial Services Register and Warning List to check who is being dealt with, even when contacted by phone.
- Implementing additional verification procedures before making payments.
  - ensure an electronic invoice is genuine by: contacting multiple contacts to validate invoice;
  - check the email address from which the email from; and
  - send a new email to a known contact rather than replying to the email received.
- Ensure the compliance function is fully operational and visible to employees.
- Ensure compliance and monitoring tools are functional.
- Ensure existing policies and procedures are adequate.
- Provide employee training.
- Focus on due diligence.
- Monitor financial controls and ensure they are effective.
- Increase scrutiny and transparency (internal and external).
- Engage with management.

*Source: Thomson Reuters Regulatory Intelligence. Top 10 frauds to be aware of during the COVID-19 pandemic, by Patrick Rappo, Katie O'Hara and Calum Ablet, DLA Piper*

pandemic. This followed an update from ASIC earlier on its regulatory work, in which it told firms that customers must be treated fairly and urged them to avoid adding to customers' financial burdens.

In other conduct-related issues, the European Securities and Markets Authority (ESMA) said national competent authorities have recently noticed a "significant" increase in retail clients' trading activity. In the UK, there was a large increase in investment platform accounts opened in March during the height of COVID-19-related volatility. Platform operators chalked up the new interest to retail investors seeking to bargain hunt and exploit volatility, but some of that activity could be personal account dealing. The FCA has already said it is concerned about market abuse and insider dealing risk during the COVID-19 lockdown.

The FCA has been monitoring personal account dealing (PAD) throughout the lockdown, during which firms have relaxed policies and allowed traders to work from home. A communication from the regulator on PAD policies and compliance is forthcoming, officials said.

The Australian conduct regulator has urged financial services firms to "check in" with their customers to ensure COVID-19 relief measures, including loan repayment delays, are still working as intended. The recommendation comes as ASIC adjusts its supervision and enforcement priorities to respond to the pandemic-induced financial disruption.

The U.S. Consumer Protection Financial Bureau has issued guidance intended to give more flexibility in terms of waiting periods and disclosures in mortgage transactions amid disruptions caused by the pandemic. The actions aim to help consumers receive proceeds of mortgage transactions more quickly if they face a financial emergency due the pandemic.

Banks and other credit providers need to pay special attention their responsible lending obligations as the pandemic plays out, despite some targeted relief from regulators. Lawyers said ASIC was trying to provide as much flexibility as possible to allow lenders to support customers through the extended period of economic disruption.

Banks and other firms are using "workarounds" to secure signatures electronically that fail to meet adequate standards, lawyers said. This comes amid an upsurge in electronic signings even after the UK FCA set out its expectations for firms dealing with the need for wet-ink signatures.

## Data governance

The UK Information Commissioner's Office (ICO) issued guidance setting out how it intends to approach the enforcement of data protection legislation during the pandemic. While it confirms what had been widely

anticipated, it provides useful assurance to organizations seeking to maintain data protection compliance, including the EU General Data Protection Regulation (GDPR), as implemented in UK law. Particular takeaways for financial services organizations are:

- Financial services organizations must ensure that they maintain a high level of compliance with data protection legislation, including the GDPR, even with the allowances made by the ICO.
- Internal policies and protocols should be updated to account for changes to working practices and personnel that might affect the ability of organizations to meet GDPR compliance and reporting requirements.
- Employees should be educated about the enhanced risks, particularly relating to phishing scams requesting personal data and seeking to misdirect payments. With more limited face-to-face interaction, employees working from home in isolation are far more likely to fall victims to such attacks, which are increasing in sophistication and intensity.
- Internal reporting procedures should be reviewed, and appropriate resources should be allocated to data security and IT teams for concerns to be reported and investigated internally.
- Additional risks associated specifically with remote working should be taken into account, including technical risks resulting from VPNs struggling with a spike in remote workers, and human risks from workers not being monitored in a controlled environment as they would be in an office. This may make them more likely to succumb to human nature or to be tempted to take short-cuts relating to security simply to get their job done.
- Organizations should also continue to closely monitor third-party suppliers of any functions that have been outsourced. They should review and enforce audit provisions in data processing agreements, however challenging this may be.

The ICO will continue to approach enforcement in a pragmatic way but has promised to come down hard on any flagrant abuse, which suggests a cautious approach, as ever, is sensible.

## Third party and outsourcing

Amid a tendency for financial services firms to rely on outsourcing providers, the International Organisation of Securities Commissions (IOSCO) is consulting on updated principles to ensure operational resilience for firms that rely on such providers. IOSCO said in the last 10 years, reforms and technology developments had changed the trading landscape for firms. Furthermore, more widespread electronic trading and process automation have heightened the complexity of markets and strengthened the focus on operational efficiency, it said.

"It is increasingly commonplace for firms to use third-party service providers to carry out, or otherwise support, some of their regulated business activities," IOSCO said. "While this approach can deliver economic benefits, it may also raise concerns about risk management and compliance when such tasks are outsourced to entities that are not regulated and/or are based in different jurisdictions. In particular, it can diminish regulators' ability to regulate or supervise certain functions within firms."

"Risk management and audit oversight of bank operations needs to keep pace with the rapid implementation of pandemic-related business continuity plans and transitioning from traditional operations to a heightened operational level. Independent oversight and validation of controls' effectiveness is essential to safeguard operational integrity in the current stressed environment."

**The Office of the Comptroller of the Currency (OCC),** Semiannual Risk Perspective, Spring 2020

# WORKING REMOTELY AND GETTING BACK TO WORK

The lockdown has taken its toll on financial services workers' mental health. Many are working longer hours while struggling with anxiety about returning to work, job security fears and stress, mental health professionals and advocates have said. The UK FCA is increasingly concerned about employees' mental health and wellbeing, its own staff included.

"The FCA has acknowledged this by making clear that it does not expect any one senior manager to be responsible for COVID-19 issues. Instead they expect a joined-up approach. Compliance functions should be working alongside HR teams now to ensure they clearly identify which roles may need to be prioritized for a return to work, and why," said Sophie White, partner, Eversheds Sutherland.

> "For the moment, the corona crisis has taken centre stage. But the old challenges remain, and the pressure on banks to scrutinize their business models is mounting. This means that a successful bank must be able to fight on both fronts: they need to address immediate corona-related issues and the longer-term issues related to the viability of their business model at the same time."
>
> **Prof Joachim Wuermeling,** member of the executive board of the Deutsche Bundesbank. May 2020

The FCA told firms at the outset of the pandemic that they had a responsibility to ensure the health of their staff. The regulator had previously said it would hold senior managers responsible for employees' poor mental wellbeing.

In the United States, TRRI reported that compliance and legal departments must work with senior management to stay abreast of the changes and prepare to make careful decisions about any return to the workplace. By most accounts, firms and their compliance departments have adapted and appear to have met the operational challenges. Financial regulators such as the SEC have been cooperative and willing to offer relief in some areas. Enforcements, exams and rulemaking work have continued.

Compliance departments should now be preparing for whatever reopening steps are in the pipeline, in communication with other relevant decision-makers. Although many of the decisions will be outside the realm of compliance, they are also likely to affect compliance functions and processes. Early input from compliance staff will aid preparations and avoid problems.

In addition, compliance and HR need to be working together as bank employees return to the office during COVID-19, lawyers said. Compliance, risk and operational resilience need to be considered alongside all other effects, they said.

Financial services firms may be in no rush to return to office life but a pecking order for who will return first is emerging, with traders at the front of the queue. Banks are being cautioned to ensure they have risk-assessed, not just health and safety, but also their compliance oversight needs before returning traders to their desks.

Monique Melis, managing director and head of compliance and regulatory consulting at Duff & Phelps, said front-line compliance staff need to return at the same time as traders. "You need at least front-office compliance back," Melis said.

Leaving these compliance staff at home to continue dealing with trader queries by telephone is not conducive to a properly functioning trading floor.

Firms in Europe and the UK planning a return to the office are weighing up whether to ask employees to disclose a positive COVID-19 diagnosis, conduct temperature checks or instigate localized track-and-trace programmes. Any of these plans must be backed up by a GDPR risk assessment to ensure any employee health data collection is legal and compliant.

# A GLIMPSE INTO THE FUTURE

"The pandemic could also have a long-lasting impact on global trade. Companies may rethink the vulnerability of cross-border supply chains. Protectionist policies in some countries may accelerate this reconfiguration."

**Timothy Lane,** deputy governor of the Bank of Canada. April 2020

Sir Howard Davies, chairman of the Royal Bank of Scotland and first head of the Financial Services Authority, said phase one has been marked by generally good collaboration between firms and regulators, after a slow start.

"Phase two, the exit phase, will be much harder. We must hope that [the] spirit of collaboration between regulators and regulated firms continues to hold at that time. Anyone who says they know for sure how this crisis will develop should have their loan application turned down. I have never seen such uncertainty. GDP estimates vary diversely and are probably all wrong. We have never seen anything like this before. There could be big shifts in the profile of both demand and supply. That will affect banks and financial institutions. There could be whole sections of the economy that will no longer be viable in the form they were before the crisis hit," Davies said.

During Q2, risk and compliance leaders from London, New York and Singapore joined a virtual roundtable to discuss the implications for their firms of the continuing pandemic. COVID-19 and its uncertainty is having a profound impact on financial services firms, their employees and customers, and risk and compliance officers need to prepare their firms for all eventualities. The virtual roundtable concluded that there were six potential steps risk and compliance leaders could consider:

**Prepare for an acceleration of digital transformation —** Many financial services firms have accelerated significantly the implementation of online product and service offerings during the pandemic, some by as much as three years. Firms are seeking not only to be able to continue to provide existing services to customers but also to remain competitive, as other financial services firms expedite their digital offerings. Digital transformation is here to stay, with business models changing as firms face growing competition from fintechs and Big Tech. Risk and control infrastructures are adapting equally quickly to support the faster pace of transformation and new business models.

**Rethink governance structures —** Financial services firms have adapted quickly and sought to cut through bureaucracy to focus on the required agile decision-making. Boards, committees and teams are often meeting more frequently, sometimes in smaller groups made up of key decision makers, and usually online. Risk and compliance teams have also had to adapt to the new governance structures and ensure that the flow of management information has been tailored to the new circumstances to facilitate line of sight to the risks and enable comprehensively documented decision-making.

**Ensure working from home is supported in the longer term —** While some teams may return to office working, a significant proportion of employees will continue to work remotely, either for some time to come or permanently. Risk and control frameworks need to be adapted and refined to continue to support the new multi-site and remote working, together with the compliance challenges involved in ensuring continued compliant activities. Areas of concern are likely to include communications surveillance and, for functions such as credit risk, the issues associated with the efficacy of client relationships given the need for remote meetings and information-gathering.

**Embed connected thinking —** The pandemic has shone a spotlight on how quickly risks can emerge, and how quickly controls can become outdated or fail. Firms need to understand how risks and controls are interrelated in their business. They also need to understand how an emerging risk can coincide with several control failures, or how credit, market, and operational risks may be linked. Wherever feasible, the risk and compliance functions need to work together and with the business to surface all relevant connectivity to ensure emerging risks are captured early and controls remain fit-for-purpose.

**Document, document, document —** As experienced compliance officers know, if it has not been documented then, in regulatory terms, it did not happen. The pandemic notwithstanding, regulators still require evidence of compliant activities and decision-making. Risk and compliance teams must ensure all relevant

documentation is in place to evidence compliant activities, processes and decisions, particularly those that have changed due to COVID-19. Third-party risk, technology risk and new product approval processes are considered areas that may require detailed attention in terms of documentation. The opportunity has been taken to rethink how evidence is captured within a firm and to leverage the potential of technology in record creation, maintenance and retention. Comprehensive recordkeeping can also help offset senior individuals' personal regulatory risk.

**Consider a post-pandemic review —** Some financial services firms have implemented a continuous review process for risk and compliance COVID-19 operations; others are waiting to initiate a wholesale post-lockdown review. A continuous review process could be a more agile approach, ensuring the task list does not build up, but it could also mean that similar issues are reviewed more than once. Whichever methodology firms choose, there does need to be a detailed and well-documented review for risk and compliance to consider how well teams have performed, identify remediation that needs to take place, and consider new ways risk and compliance can support the organization's revised strategic goals. Firms should also be aware that regulators are themselves intending to conduct post-pandemic reviews.

During a TRRI webinar on financial crime, the audience was asked about future actions.

The overwhelming response was to retrain and enhance skillset to adapt to changes that many are predicting.

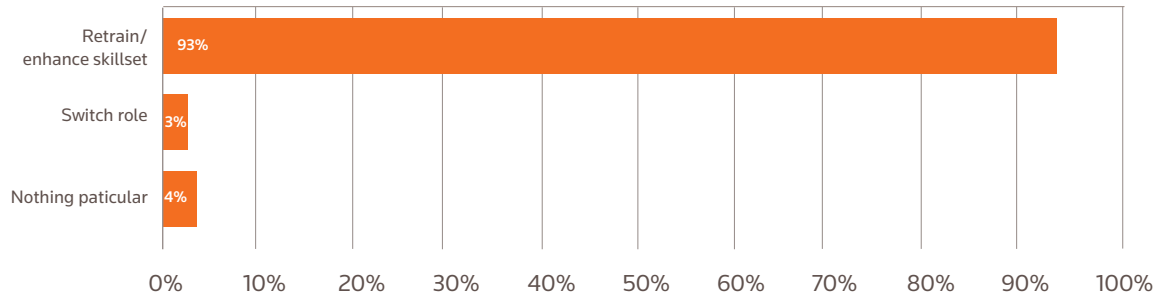
sometimes more demanding expectations in a separate statement for dual-regulated firms.

"Other senior management functions are not 'mandatory', so firms have greater flexibility to furlough the individuals performing them. For instance, if a firm temporarily suspends a business service or function due to the disruption caused by coronavirus it could, in principle, furlough the senior manager responsible for it," the FCA said.

Senior managers will need to move from fire-fighting into a more strategic mode and consider the following probabilities:

- *It will not be the same going back*. Due to space constraints and social distancing, office layouts will look different. Some staff will be fearful about returning to work; some will continue to work from home most of the time. Senior managers will need to be active in terms of rebuilding team spirit, and monitoring mental health, both for those in the office and those still working from home. Some firms will have fewer staff because of the economic situation.
- *Post-COVID-19 review* — firms' systems and controls will inevitably have been stretched during the crisis. Some things may not have gone quite as well as they should have done, albeit unintentionally. Where firms have noted increased risks to their business during the pandemic, there should be a clear audit trail of how they mitigated those risks. The FCA will be reviewing and picking up on any thematic weaknesses which occurred over the period. It will hold senior managers accountable.

**What do you feel you should do after COVID-19 to be prepared for the future?**




Source: Thomson Reuters Regulatory Intelligence, Financial Crime during COVID-19: Tackling fraud, scams and misinformation – June 2020

## Senior management accountability

Senior managers performing required functions such as compliance oversight or acting as a firm's money laundering reporting officer (MLRO) should only be furloughed as a last resort, the UK FCA said. The regulator was setting out its expectations of solo-regulated firms for the SMCR and COVID-19. The regulator also set out its

- *There will be consolidation and mergers* – there will be winners and losers from COVID-19, some firms will have been better placed than others to capitalize on the opportunities, and this may lead to mergers and consolidation. Some fund management and broking firms have been under pressure. Some banks which already had poor loan portfolios and unviable business

models pre COVID-19 will have deteriorated during the crisis.

- *Brexit* — By 2021, the UK-EU regulatory arrangements should be clear, they will be in operation. Firms will have contingency plans in place for a number of scenarios, and so it will be a case of which plan they need to trigger and implement.
- *Climate change* — The financial sector needs to adapt to manage the physical and transition risks that climate change poses. High on the agenda of regulators, it also needs to be high on firms' agendas as well.

In other areas where future developments are perhaps becoming clearer:

- Deutsche Bank will increase its aggregate investments in risk, anti-financial crime and compliance technology in 2020, said Christian Sewing, chief executive. This comes on top of 900 million euros invested across these areas in 2017-2019. In compliance, Deutsche is monitoring more than a million communications daily, he said.
- COVID-19 may have knocked some vital climate initiatives off-schedule but it offers an opportunity to ensure environmental goals are embedded in financial recovery efforts, said Mark Carney, United Nations Special Envoy for Climate Action and Finance. It has also provided a real-life lesson in how to manage systemic risk. "COVID-19 is teaching us how to manage systemic risks, and climate change is the biggest systemic risk," Carney said.
- Bank AML programs are likely due for U.S. regulatory scrutiny once the pandemic ends, AML experts said. Some were wary about potentially being expected to answer for misuse of a major lending program for small businesses and acknowledged they could face questions if bank clients improperly obtain such loans.
- MiFID II transaction reporting teams face a post-crisis clean-up effort as the high trading volumes will likely have a multiplier effect on mistakes, reporting experts said. The 2016 U.S. presidential election, the Brexit vote and the unpegging of the Swiss franc contributed significantly to high volumes, they said.

Finally, the FCA has released a statement setting out its proposal to accelerate the digital sandbox pilot to enhance regulatory support for innovative firms amid the pandemic. The regulator said it is swiftly progressing plans to allow innovative firms to trial services and products in a digital testing environment, especially those that are tackling COVID-19-related challenges.

The digital sandbox will offer enhanced versions of features available through the FCA's Innovation Hub, Regulatory Sandbox and TechSprint programmes. It will allow innovative firms to test and develop proofs of concept in a protected digital environment as well as facilitate collaboration with stakeholders to address industry-wide problems. Though a pre-COVID 19 initiative, the FCA now intends to pilot aspects of the digital sandbox on a modular basis to provide support to innovative firms and their customers during the pandemic.

**The FCA highlights the following features as foundations of the digital sandbox:**

- *Access to high-quality data assets* – accessing synthetic or anonymized data sets to enable testing and validation of technology solutions.
- *Regulatory call-to-action* – enabling identification of areas of regulatory interest which can increase innovation or issue specific challenges.
- *A collaboration platform* – facilitating diversity of thinking, sharing learnings and fostering an ecosystem to help solve complex industry wide challenges.
- *An observation deck* – observation of in-flight testing to inform policy thinking in a safeguarded environment.
- *Application programming interface (API) or vendor marketplace* – an environment for fintech, regtech and other vendors to list their solutions and APIs to encourage greater interoperability and foster a thriving ecosystem.
- *Access to regulatory support* – development of testing plans, signposting to relevant regulations, informal steers or support to understand the wider regulatory environment or the authorization process.

# CLOSING THOUGHTS

Fairy tales can be an interesting metaphor for real life. On one level the stories and imagery are loved by children for their colourful characterization of simple, easy-to-understand tales. On another level there is often a hidden meaning that points the reader to the difference between right and wrong, good and evil.

Life during the pandemic is not dissimilar. Living through Q1 and Q2 has been rather like inhabiting a fairy tale world. In all good fairy tales there is a point in the story where the worst has happened and good begins to win through. Are we yet at that moment for COVID-19?

The financial services sector is awakening to a different world, which will mean weakened economies, job losses, greater pressure on capital, changing customer habits and opportunities in areas where regulators would rather there were none, such as financial crime and cyber attacks.

There are few good options for dealing with this pandemic and, as is being shown in society as a whole, it is far easier to close things down than re-open them in a controlled way. Regulators and firms alike face such dilemmas.

Q3 will undoubtedly see firms being creative in terms of the solutions they seek to overcome the pandemic. The challenge for regulators is to try to maintain their sympathetic approach to the industry without letting bad practice embed itself.

Governance and culture are essential elements in the make-up of a firm. Success in these areas, with strong governance and a customer-focused culture, will enable firms to manage the risks appropriately and find the right strategy to steer them through the difficult times to come. Firms which underestimate these areas will find the future precarious.

The pandemic will change aspects of life in financial services forever. There is already a more permanent move to home working, for example. Q3 2020 will see the further shaping of that future. It is to be hoped any changes made will see all stakeholders in the sector "live happily ever after".

## Appendix 1

Top five anti-bribery and corruption risks and how to address them (From TRRI article entitled "Top five anti-bribery and corruption risks to be aware of during the COVID-19 pandemic" by Patrick Rappo and Calum Ablet, DLA Piper)

| Risk | Controls |
|---|---|
| ***1. Supply chain risks***<br>COVID-19 has placed significant stress on supply chains. This has created a number of bribery and corruption risks: | ***A Communication and training:***<br>The company's zero-tolerance approach to bribery and corruption should be re-communicated to employees and, where appropriate, third parties. Targeted communication can be particularly effective, for example, directed toward gatekeepers such as finance and internal audit teams, and salespeople. Individuals within the organization who could be considered at higher risk of receiving offers of bribes should be reminded of the company's policy on bribery and accepting gifts and hospitality. Training, either from internal or external sources, is an effective means of reinforcing such messages. |
| • *Alternative third parties:* Companies may need to engage with alternative suppliers and other third parties in new, higher-risk (from a bribery and corruption perspective) jurisdictions. This increases the risk that third parties from those jurisdictions taint supply chains with bribery or corruption. | ***B Existing parties in the chain:*** If one of the parties in the contractual/supply chain is rendered unable to perform its role, the company should consider whether other, existing parties in the chain are able to step in to perform those functions, even if only on a temporary basis. Such parties should have already been subjected to the company's due diligence process and therefore should not increase chain risk from an anti-bribery and corruption perspective. |
| • *Governmental actors:* Government actors may now feature more prominently in the supply chain, either because that is a feature of the industry in the country in which a new supplier is located, or because governments have generally become more active in supply chains or financial services arrangements as part of their responses to COVID-19. Heightened government presence increases the risk of bribery and corruption as a consequence of governmental actors' decision-making functions. | ***C Due diligence:*** Where it is necessary to engage new third parties, companies should ensure that they continue to conduct proportionate due diligence and screening, adopting a risk-based approach. Third parties in higher-risk jurisdictions may merit more intensive due diligence. Companies may wish to extend the list of countries considered "high-risk" to include those badly affected by COVID-19, as there may be higher occurrences of bribery in those jurisdictions. |
| • *Bypassing traditional controls:* Economic pressures may lead companies to bypass or reduce due diligence conducted on new third parties. | ***D Monitoring:*** Companies should consider increasing their monitoring of transactions. For example, if transactions are only reviewed once they exceed a monetary threshold, that threshold could be lowered so that more transactions are scrutinized. This may increase chances of detecting suspicious activity as well as disincentivize such behavior from employees in the first place. |
| 2. ***Pressure on the bottom line***<br>The government response has had a significant impact on the financial standing of many firms, significantly increasing the risk of bribery. Risk areas include: | ***E Whistle-blowing:*** Companies should review their whistle-blowing process to ensure that it continues to function effectively in the light of new working arrangements. Employees should be encouraged to report concerns given the greater risk of bribery and corruption. |
| • *Bribes:* Individuals who are under pressure to meet targets, such as salespeople, may resort to paying bribes to secure opportunities in the private sector. In addition, as governments look to re-open economies, companies should remind employees not to attempt to influence government officials to re-open their business by offering bribes, gifts or hospitality. | ***F Conduct early and effective internal investigations:***<br>Issues that come to light should not be swept under the carpet or "put off" until business returns to normal. Not only is there uncertainty about how long the current situation will continue, but issues may also constitute immediate and significant legal, financial, regulatory or reputational risk to the organization. Regulators will not allow firms to use the current circumstances as an excuse. All such issues should be investigated immediately, using internal compliance and legal teams or external counsel where necessary. |

| | |
|---|---|
| • *Corruption:* In response to economic pressures, companies involved in public sector procurement may attempt to influence decision makers improperly to secure valuable contracts. | ***G Controls on charitable donations:*** Companies may want to consider prohibiting charitable donations altogether. If this is already the case, employees should be reminded of this fact. Alternatively, donations may be permissible provided they are subject to a process of internal authorization (which itself involves an element of due diligence). Any donations made in this way must be accurately recorded for full transparency. |
| • *Facilitation payments:* There may be more incentives to make payments to facilitate the international movement of goods to ease economic pressures. | |
| ***3. Demand-driven risks***<br>While many companies will suffer financially, some may experience significant surges in demand for their products or services, perhaps due to the nature of the sector in which they operate or because they have an important role in the government's virus response (such as financial services companies participating in Coronavirus Business Interruption Loan Scheme). It is important that such companies do not become complacent about the anti-bribery and corruption risks they face: | |
| • *Reduced oversight:* Pressure to meet high demand may lead to reduced oversight within the organization, as managers prioritize meeting demand over compliance considerations. There may simply be insufficient time or resources to ensure normal controls are applied consistently. | |
| • *Heightened bribery risk:* A company's employees may be more likely to receive offers of bribes by customers seeking favourable treatment or priority. | |
| ***4. New working arrangements***<br>One of the most striking aspects of the pandemic has been the requirement in many countries for employees to work from home — even those for whom home working was traditionally considered unsuitable, such as those working on sales and trading desks. This carries with it its own anti-bribery and corruption risks: | |
| • *Due diligence:* Due diligence may become more difficult when carried out remotely, particularly when new, unknown third parties are involved or certain hard copy documents are unavailable. For example, the Financial Action Task Force (FATF) and the FATF-style regional bodies (FSRBs) have noted that remote verification of customer identities may not be possible for some financial institutions. | |
| • *Pressure on employees:* The ability of employees, such as sales teams, to travel is significantly curtailed, making it much harder for them to promote new products and network with potential and existing customers. This can increase pressure to meet sales targets and create incentives to engage in bribery or corruption. | |
| • *Reduced oversight of staff:* Employees may feel that there is less oversight of their activities while they work from home, which may make them feel it is less likely they will get caught engaging in unlawful activity (thereby increasing their propensity to do so). | |
| ***5. Charitable donations***<br>Companies may be looking to make charitable donations in the current circumstances. Such donations carry their own anti-bribery and corruption risks. They can be a conduit for corrupt payments, in that they could be made with the intention of influencing someone to act improperly or as a reward for having acted improperly. For example, a charity could be connected to a political party or a person with a decision-making function. | |