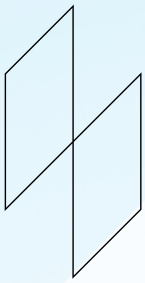


FINTECH
FINCRIME
EXCHANGE

# Keep calm & keep planning

## Pandemic Planning for FinCrime

FINTRAIL

rdc
Smarter Screening

ffe_admin@fintrail.co.uk
www.fintrail.co.uk/ffe

# What's the plan?

No business sector has been left unaffected by the outbreak of the coronavirus. The financial sector, including FinTechs, is no exception. In times like this, working together as a community is more important than ever.

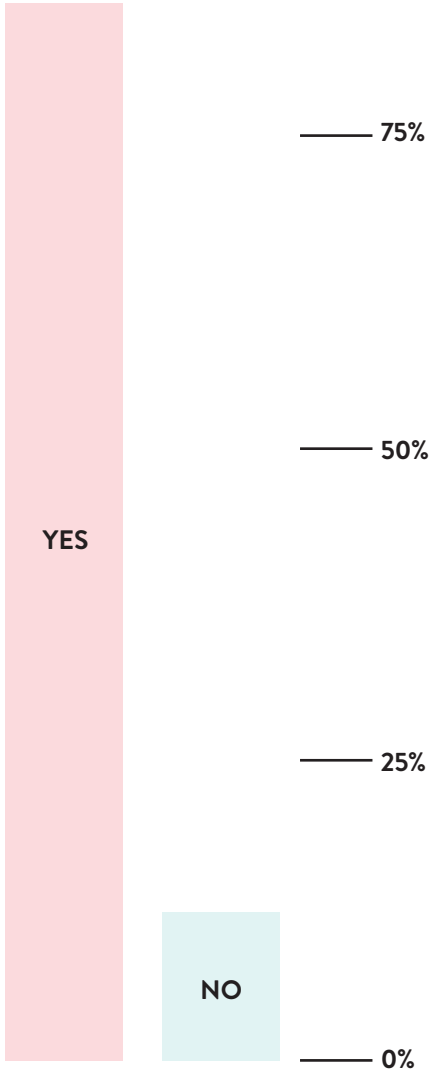
The FinTech FinCrime Exchange (FFE) is founded on the principles of sharing information and best practice, and during times of such uncertainty, we feel it is vital for us to continue to provide a platform for the community to share and collaborate. In this document we have collated examples of how COVID-19 has impacted the FinCrime operations of our members and how the teams have responded as they pivot to almost exclusively remote operations, as well as presenting some best practice guidance for a business continuity plan (BCP) and remote anti-financial crime (AFC) compliance.

This guidance is based on research conducted by FINTRAIL across the FFE community. This includes a survey sent to all global members, review of 31 responses, 15 follow-up interviews, and additional research and analysis conducted by FINTRAIL. The survey and interviews were conducted during the week commencing 16 March 2020.

As highlighted in the opening statement, a large majority of respondents reported that their firms have been affected by the outbreak of the coronavirus. Individual impacts vary from firm to firm based on their size, complexity and type of products offered.

Overall, FinTechs who contributed to our research did not find switching to remote working too difficult. Most of them had been offering flexible working arrangements to their staff already. However, we have all realised by now that the changes currently required go beyond working from home, and the traditional approach to business continuity planning may no longer be sufficient. Therefore in this document we will be discussing pandemic business continuity planning. But before that, we will look at...

**Has COVID-19 affected your business**








EMEA | APAC | USA
ffe_admin@fintrail.co.uk
www.fintrail.co.uk/ffe

# What are the regulators saying and doing?

International bodies, financial regulators and law enforcement agencies across the globe are closely monitoring the coronavirus situation. It is more crucial than ever that FinTechs pay close attention to statements and guidelines issued by their respective regulators. These may be updated very frequently in order to address rapidly changing situations.

After reviewing the most recent communications from a variety of organisations globally (see details below), FINTRAIL would like to highlight some of the areas of regulatory focus related to financial crime and customer due diligence, which we will look at in more detail throughout this document:

- Financial crime remains unacceptable and reporting suspicious activity is still a priority;
- Criminals are already profiteering from COVID-19 related scams, therefore FinTechs must be able to adopt their controls to quickly evolving fraud typologies;
- Regulators are warming up to responsible digital customer onboarding and encourage wider adoption of technology, so FinTechs should take a full advantage of this;
- A risk based approach, including (where appropriate) simplified due diligence, should be applied to ensure customers' easy access to financial services.

In its most recent statement, the **Financial Action Task Force (FATF)** encouraged governments to work with financial institutions (FIs) to use the flexibility built into the FATF's risk-based approach to address the challenges posed by COVID-19 whilst remaining alert to new and emerging illicit finance risks. The FATF encourages the fullest use of responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures. This is especially good news for FinTechs, who fully embrace technology in their KYC processes.

When FIs identify lower money laundering/terrorist financing (ML/TF) risks, the FATF encourages exploring the appropriate use of simplified measures to facilitate the delivery of government benefits in response to the pandemic. This call was followed by the **German Federal Financial Supervisory Authority (BaFin)** announcing that it will not object if the identification processes for granting state promotional loans are carried out in accordance with Section 14 of the Money Laundering Act, for example by sending a copy of ID, and countering the ML/TF risks through appropriate customer and transaction monitoring as part of the ongoing business relationship.

Similarly, the **European Banking Authority (EBA)** called on competent authorities to support FIs' ongoing efforts by sharing information on emerging ML/TF risks, setting clear regulatory expectations and using supervisory tools flexibly.

The **UK's Financial Conduct Authority (FCA)** updates its website regularly. Early on in the crisis, it announced that it stood ready to take any steps necessary to ensure customers are protected and markets continue to function well. The FCA recognises that a growing number of people may use online or phone banking services, in some cases for the first time. Firms should remind consumers to be aware of fraud and protect their personal data. Scammers are sophisticated, opportunistic and will try many things. Therefore it expects firms to help vulnerable consumers access their banking services – online or over the phone.

In a more recent Dear CEO letter, the FCA provided examples of remote client verification and additional checks which firms can use to assist with verification including requesting 'selfies', gathering and analysing additional data to triangulate evidence provided by the client (such as geolocation, IP addresses, etc.) or verifying phone numbers, e-mails and/or physical addresses by sending codes to the client's address to validate access to accounts. Most FinTechs have already deployed these techniques successfully.

The **Monetary Authority of Singapore (MAS)** has been issuing advisory notices since January, as this country experienced the outbreak of the coronavirus much earlier than Europe, calling on FIs to continue maintaining effective internal controls across their operations and anticipate and be prepared to manage any increase in demand for certain financial services. MAS was perhaps also one of the first regulators warning FIs about COVID-19 related fraud typologies (which we will explore further in the Appendix).

After the US president declared a national emergency in response to COVID-19, the **Financial Crimes Enforcement Network (FinCEN)** requested FIs affected by the pandemic to contact FinCEN and their functional regulator as soon as practicable if a COVID-19-affected FI has concern about any potential delays in its ability to file required Bank Secrecy Act (BSA) reports.

In a similar way, the **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** reminded its reporting entities about an expectation to meet all of their obligations, including in relation to reporting. It highlighted that a priority should be given to submitting suspicious transaction reports (STRs). In exceptional circumstances where a reporting entity may be in possession of critical information related to terrorist activity financing but, for some reason, cannot submit the STR in the usual manner, FINTRAC temporarily offers an alternative reporting route.

Suspicious activity reporting is definitely one of the priorities highlighted by many other regulators including the **Danish Financial Supervisory Authority** which also called for FIs to be aware of the importance of monitoring their clients' transactions and their duty to report any suspicious transactions.

On the other side of the globe, the **Australian Transaction Reports and Analysis Centre (AUSTRAC)** stated that it would consider firms' circumstances when applying the Anti-Money Laundering and Counter-Terrorism Financing laws. AUSTRAC also shared examples of identified areas of criminal exploitation where the financial system may be more vulnerable during the COVID-19 pandemic which may include: movement of large amounts of cash following the purchase or sale of illegal or stockpiled goods, or exploitation of workers or trafficking of vulnerable persons in the community. Finally, AUSTRAC invited FIs to report any significant shifts observed in relation to financial crime and fraud monitoring, which it can then share more widely to inform the industry.

Similarly to AUSTRAC's decision to extend a reporting period for the Compliance Report, without risk of compliance action, **Luxembourg's Commission de Surveillance du Secteur Financier (CSSF)** announced that it will not apply a strict enforcement policy with regards to reporting if delays are duly justified, during the COVID-19 crisis. Due to the current situation with the ongoing spread of the coronavirus, the Swedish Financial Supervisory Authority (Finansinspektionen) has also postponed the deadline for the annual reporting on money laundering and financing of terrorism.

Despite these provisions, whilst financial firms, including FinTechs, are reviewing their current arrangements to address the evolving situation managing the risks to their employees and customers, the EBA's message is clear – financial crime remains unacceptable, even in times of crisis such as the COVID-19 outbreak.

# What are the best practices and principles for business continuity according to FinCrime regulators?

In general, most regulators expect all financial firms to have contingency plans to deal with major events and for plans to have been tested.

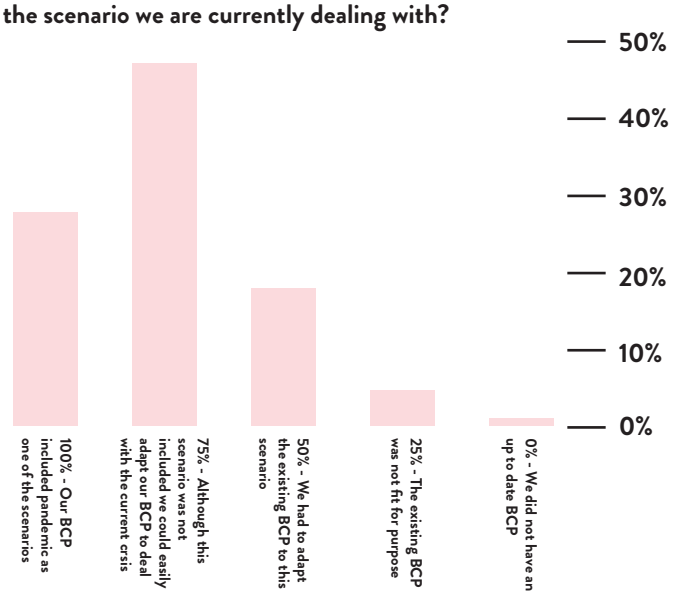
When developing BCPs, FI management typically considers the effect of various natural or man-made disasters that may differ in their severity. These disasters may or may not be predictable, but they are usually short in duration or limited in scope. In most cases, malicious activity, technical disruptions, and natural/man-made disasters typically will only affect a specific geographic area, facility, or system. These threats can usually be mitigated by focusing on resiliency and recovery considerations.

As such, a traditional approach to FinCrime function continuity planning would usually include:

- Identifying important FinCrime services that if disrupted could expose the business to a greater risk of financial crime, harm the consumer or stall/halt business services;
- Setting impact tolerances for each important FinCrime service (i.e. thresholds for maximum tolerable disruption to help achieve consumer and firm protection);
- Mapping (identifying and documenting) of the people, processes, technology, facilities and information that support important FinCrime services;
- Testing the firm's ability to remain within its impact tolerances through a range of severe but plausible disruption scenarios;
- Conducting lessons learnt exercises to identify, prioritise, and invest in the firm's ability to respond and recover from disruptions as effectively as possible;
- Developing internal and external communications plans for when important FinCrime services are disrupted.

According to survey results, only 29% of respondents' BCPs included pandemic as one of the scenarios, with a further 48% stating that their current BCPs, although not entirely sufficient, were easily adapted. On the other side of the spectrum, 3% of respondents confirmed that their existing BCPs were not fit for purpose.
Although on the back of these results, we may be tempted to conclude that in general FinTechs seamlessly switched into the BCP mode, it is important to note that we are only in week 3 of a much longer period of remote working. Additionally, most FinTechs have so far not experienced staff shortages due to illness which might happen should authorities fail to control the epidemic.

**To what extent does your Business Continuity Plan (BCP) cover the scenario we are currently dealing with?**



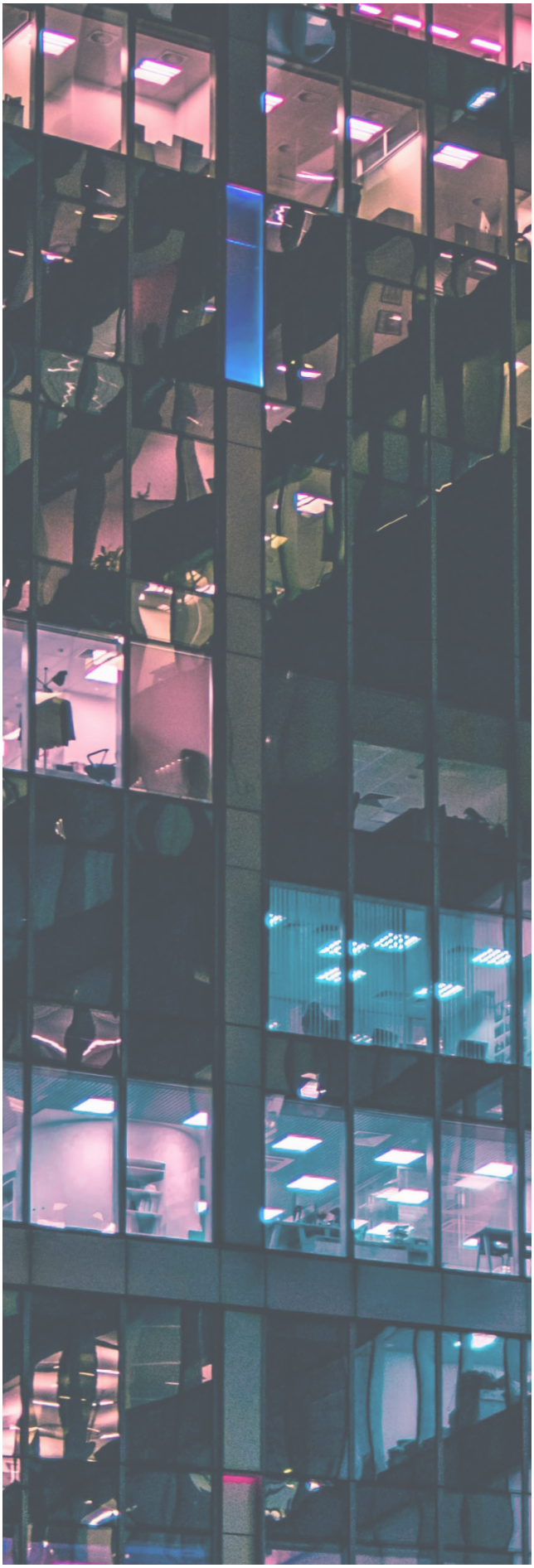

As such, the traditional approach to BCP may not be sufficient and FinTechs should start planning, if have not done it already, and implement pandemic conditions (i.e. staff shortages) within their BCP.

As highlighted by the US Federal Financial Institutions Examination Council (FFIEC), there are distinct differences between pandemic planning and traditional business continuity planning. Pandemic planning presents unique challenges to financial institution management. Unlike natural or technical disasters, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. Therefore, pandemic plans should be sufficiently flexible to effectively address a wide range of possible effects that could result from a pandemic and consider the systemic nature of the crisis when designing response strategies.

As an example, a traditional BCP may address a scenario where a particular vendor's platform became temporarily unavailable. However a pandemic BCP should consider degradation or limited availability of core infrastructure such as mass transit, telecommunications and internet connectivity. Considering the extended duration of the current situation, the BCP should also facilitate FinTechs' ability to fasttrack the exception approval process when it has to deviate from standard policies and procedures.

**From now on, your BCP should be a live document, regularly updated, allowing you to re-prioritise FinCrime services that are absolutely critical to protect the firm and its customer.**

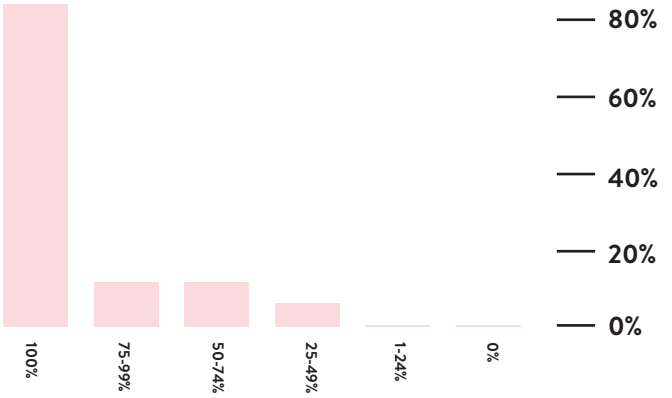
If we were to draw some lessons from disaster management, communities' and individuals' reactions to the disaster usually follow predictable 'heroic', 'honeymoon', 'disillusionment' and 'restoration' phases. After the initial heroic phase, in our case involving launching the BCP and switching to remote working, comes the honeymoon phase. We settle into a new way of operating and are quite optimistic about how well we are dealing with the crisis. However, after 2-4 weeks the optimism starts to wane, especially after our resources are stretched to their limits. In the next section, we will look at how to ride out the disillusionment phase to successfully reach the restoration phase, by looking at the current situation and how you monitor effectively against it.



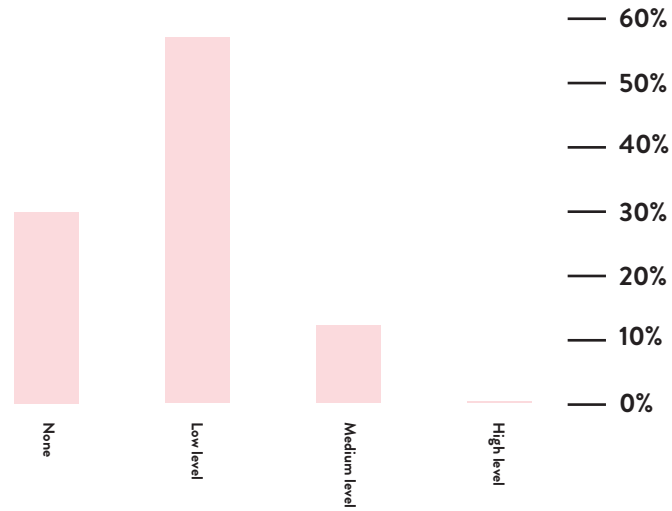
# Current state of play

When completing the survey, 87.5% of FFE members said they were already working remotely. This shows that the FinCrime community in the FinTech space was perfectly placed to respond quickly to the COVID-19 crisis. Equally 91.6% said they had low level or no impact on their day-to-day duties and were confident they could manage their responsibilities remotely. FFE members not only demonstrated that they were able to respond quickly but were also able to adapt well to the new working environment. Flexible, often remote, working practices have always been associated with FinTechs, therefore there is no surprise at the speed with which FinTechs have adapted to a new reality. Only 8% of respondents reported a medium level impact on their day-to-day duties, with no FinTechs reporting a high level impact. Having a robust BCP, deployed quickly and communicated well, has certainly been a contributor to this successful transition. However, that is not where the process ends as we move out of the honeymoon period.

**What percentage of your FinCrime team is currently working remotely?**

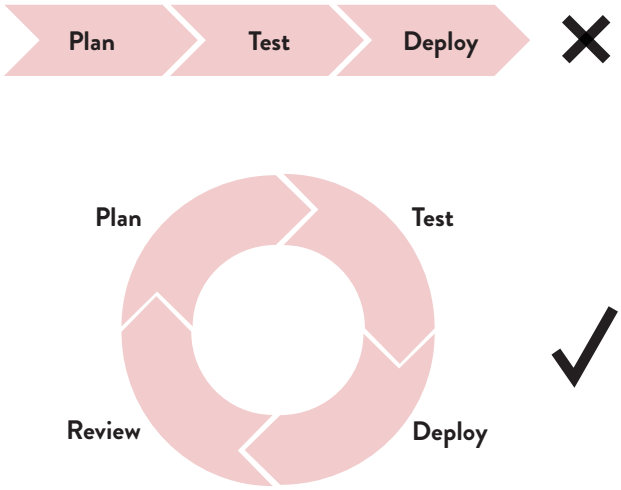



**If working remotely, to what extent has working remotely impacted your day to day duties?**




## How to monitor your FinCrime Business Continuity Plan

A common misconception is that a BCP adopts a linear approach of planning, testing and then deploying, with the majority of Fintechs now at the deployment stage. Monitoring your BCP will ensure your AFC programme remains effective during this period of disruption. This means that approaching the process as a recurring cycle, once deployed, will leave you in a more agile position should you need to adjust or reprioritise. Looking at the principles mentioned earlier relating to a traditional approach to a FinCrime continuity plan, we can explore some best practices to keep your plan on track now you are deployed and in the review phase.




**Conduct lessons learnt exercises to reprioritise your BCP and assess your AFC programme.**

If you haven't already, consider conducting retrospectives as part of your feedback loop for your BCP and current performance of your AFC programme. This process shouldn't be limited to the end of the COVID-19 crisis and will be a key measurement of success should we see ourselves in the same position in 3-6 months' time.

Here are some steps for consideration that your retrospective should include:

- Review and assess tolerance thresholds;
- Assess existing risks and identify emerging risks;
- Review effectiveness of your BCP and AFC programme;
- Re-prioritise and re-communicate.





EMEA | APAC | USA
ffe_admin@fintrail.co.uk
www.fintrail.co.uk/ffe

In line with your tolerance thresholds, you should ensure you identify vulnerabilities within your FinCrime BCP once it has been deployed, with a view to ensuring you invest in the areas that need configuring according to the circumstances you are facing. Your plan should be a living document, so don't be afraid to change your priorities.

**Review and assess tolerance thresholds**

In line with regulatory expectations you are likely to have set tolerances or risk appetite statements for your FinCrime services. Setting these against each service, process or technology is a robust way of monitoring against your framework, and is generally encouraged regardless of whether you have deployed your BCP. This will enable you not only to assess the level of risk that may entail from backlogs or systems failures, but also enable you to make a judgement call on when to escalate should your tolerance be exceeded. The FINTRAIL blog on risk appetite entitled *How Hungry Are You* is a good reference for this.

Now is the time to review these tolerances to determine which ones have been exceeded. This will be the best indication of what is working effectively on your AFC programme and what isn't. It will also be one of the two key drivers of how you reprioritise in the current landscape. If your tolerance thresholds were previously signed off by the board you should also consider whether they should be reassessed, modified and reapproved.

**Assess existing risks and establish new ones**

- **Review your tolerance thresholds / risk appetite statements**
- **Use exceeded tolerance thresholds as a driver for reprioritisation**
- **Reassess these thresholds and modify with board approval**

It is likely that as a FinCrime function you began January having completed your latest risk assessment with a full understanding of your inherent financial crime risks and plans to mitigate any outstanding risks which remain residually high. Whilst these risks may still exist, you should consider a reassessment of them and also the identification of any new risks that may have materialised in the current conditions. Scenarios such as COVID-19 are one of the main reasons why businesses are encouraged to view their risk assessments as a dynamic living document which should be updated when required.

Criminals will look to abuse these uncertain times with scams being well documented within the FFE as well as external headlines. Annex 1 outlines common scams which have been identified. Some FFE members, such as Monzo, have taken a proactive approach to ensuring their customers are aware of new scams to which they could be susceptible.

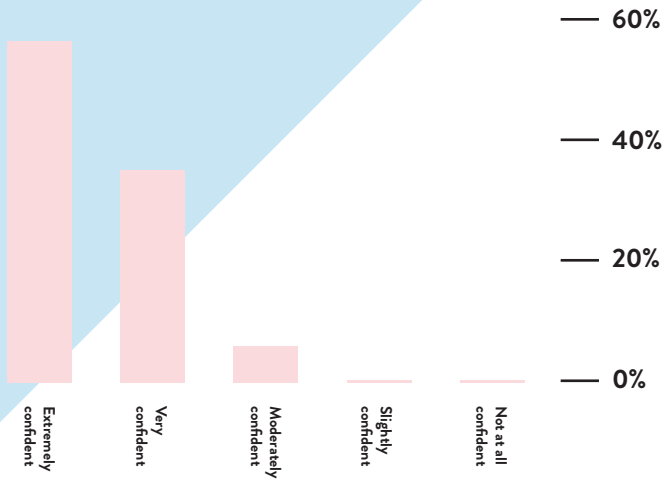
It is not just scams connected to fraud you should be looking out for though, so ensuring you pay attention to any other behavioural changes within your customer base will help you identify other forms of activity that may be suspicious and linked to financial crime. We also asked FFE members whether they had noticed any change in financial crime activity since the outbreak. Although respondents of the survey were aware and monitoring for new COVID-19 related fraud typologies, very few had actually identified new trends so far outside of the fraud scams already identified. In order to identify new trends, consider applying a model like Benford's Law which looks for outliers in your customer activity. Additionally are there operational risks to consider or should internal fraud now be reassessed within your risk assessment now that the business is working entirely remotely? If your entire workforce becomes sick, what does that mean for the tasks they conduct? Once you have completed your reassessment you can use any changes identified as a way of reprioritising alongside the tolerance thresholds that may have exceeded.

- **Consider updating your risk assessment**
- **Reassess your existing risks, taking into consideration the current landscape**
- **Identify new inherent risks that may have materialised such as internal fraud and operational risks**
- **Use the outcome of your reassessment to drive your priorities within your BCP and AFC programme**

**Review effectiveness of your AFC programme and reprioritise your BCP accordingly**

In general, respondents were overwhelmingly confident in their ability to manage their daily duties remotely. Of the 31 people that were asked whether they felt they could do this, 35% said they were very confident and 58% said that they were extremely confident. This suggests that going into this pandemic FinCrime professionals in the FinTech community were comfortable that their AFC frameworks were well positioned to adjust.

**If working remotely, how confident do you feel managing your responsibilities remotely?**




From an operational perspective, all firms have at their disposal cloud-based technological solutions allowing online collaboration and an ability to access their core systems remotely. These are accessed through a Virtual Private Network (VPN) extending a private network across a public network and enabling users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Depending on the jurisdiction your business is operating in, you will now be between 3 weeks and 3 months into your new working environment and now is the perfect time to review the effectiveness of your framework to determine whether it truly has adjusted.

As suggested in some of the best practices for a FinCrime continuity plan, businesses are likely to have already mapped out the core areas of their AFC framework and the importance of that function/control within their programme, and to have an understanding of its impact on the wider framework should it become unavailable or disrupted. If you are unable to perform customer due diligence or customer screening, does this mean you are unable to onboard customers? Additionally, if your monitoring programme is disrupted, are you able to monitor your customers' behaviours for suspicious activity or in a worst case scenario unable to process transactions because of the lack of oversight?

Having this holistic view of your framework is important, but in order to have that visibility you will need to look at the people, processes and technology that support your framework to truly determine its current effectiveness. Using your tolerance thresholds and also the reassessment of your inherent risks to guide you, conducting an effectiveness exercise is going to be a key process to continue operating within this environment. Knowing what aspects within these areas are a P1, P2 or P3 function for the running of your programme will help establish where you prioritise your resources should circumstances change.

- **Map or remap the technologies, people, and processes that support your framework and assign a priority level to them**
- **Use tolerance thresholds are reassessment of inherent risks to conduct effectiveness exerciseç**
- **Consider taking your assurance team with the effetiveness exercise**

**Effectiveness of processes, people and technology**

Using the questions outlined earlier, what are some of the considerations from your effectiveness exercise to establish lessons learned from the deployment of your FinCrime BCP, and what best practices can the FFE share for pandemic planning?

| Framework | Considerations and best practices |
|---|---|
| **Processes**<br>How have your financial crime policies and procedures adapted? | **Considerations:**<br>• In your mapping exercise did you identify the important processes and how are they operating, and were any missed?<br>• Is your current FinCrime policy and procedural framework fit for purpose in the current landscape?<br>• Are there any new operational or financial crime risks that have developed that the current documentation does not cover?<br>• Are the roles and responsibilities outlined within your FinCrime documentation working effectively and are individuals/teams taking accountability for them?<br><br>**Best Practices:**<br>– FinCrime policies and procedures may need further adjusting if they are not working effectively.<br>– Prioritising your processes by high, medium and low was a common theme identified within the FFE to manage workload and ensure key tasks were completed.<br>– In line with tolerance thresholds, consider reviewing and adjusting your risk appetite statements to meet new risks.<br>– Ensure senior management maintains oversight and approval of any FinCrime documentation. If changes to these documents are made, ensure approval is received.<br>– More broadly, members of the FFE were using this as an opportunity to review and refresh financial crime policies and procedures. |
| **Technology**<br>Have the systems, internal or external, that support the framework been working effectively? | **Considerations:**<br>• Have you identified significant reliance on individual systems for either multiple or core services and have they performed effectively with minimal disruption?<br>• Have your tolerance thresholds been exceeded by any of these systems?<br>• Who are the control owners for individual systems and what are the escalation processes should they become unavailable?<br>• Do you have sufficient IT resources readily available to react to any disruption and to reconfigure new system requirements?<br>• Operationally does everyone still have access to the systems they need?<br><br>**Best Practices:**<br>– Maintaining a list of your systems, alongside whether they are external providers, will ensure effective oversight of what technology you may be reliant upon.<br>– Having a clear escalation process outlined will enable a quick response and recovery time.<br>– Identify who within the FinCrime team is the owner of the system and also who is the owner from a developer perspective. Many FinTechs maintain a developer resource within their FinCrime function, making them perfectly positioned to be responsive.<br>– Have a clear understanding of the service level agreement on any outsourcing arrangements and where appropriate consider requesting the BCP of your vendors. This will give you comfort that they have the ability to recover.<br>– Consider your contingency plan for each system and whether there is a back up plan you could deploy. |

Are there any manual work arounds for the task that the system fulfills, and is this a good opportunity to integrate a secondary external system you can redirect the task to?

- Consider reconfiguring the systems to meet new financial crime risks identified.
- Conducting assurance tests against these systems will enable you to identify new vulnerabilities or offer reassurance they are working as they should be.
- From an operational perspective, FFE members mentioned ensuring the team continues to have access to these systems as an important consideration. This can consist of making VNPs available and ensuring IPs are whitelisted. Equally, consider assessing whether you should revoke access to key systems for some individuals who do not need them.

**People**

How are the FinCrime teams performing and do they have the tools required to fulfill their tasks?

**Considerations:**

- Do you need to continue to identify the key members of staff responsible for the running of the framework and does the FinCrime team still have the tools they need?
- How has the FinCrime team responded to the current working environment and do you need to consider adjusting working styles?
- Are priority tasks being completed, or have staff levels reduced due to current circumstances which are impacting these priority tasks?
- Is the current structure of your financial crime operation working?
- Are changes being communicated internally?
- Are there any outsourcing arrangements to reconsider should team members suddenly become unavailable?

**Best Practices:**

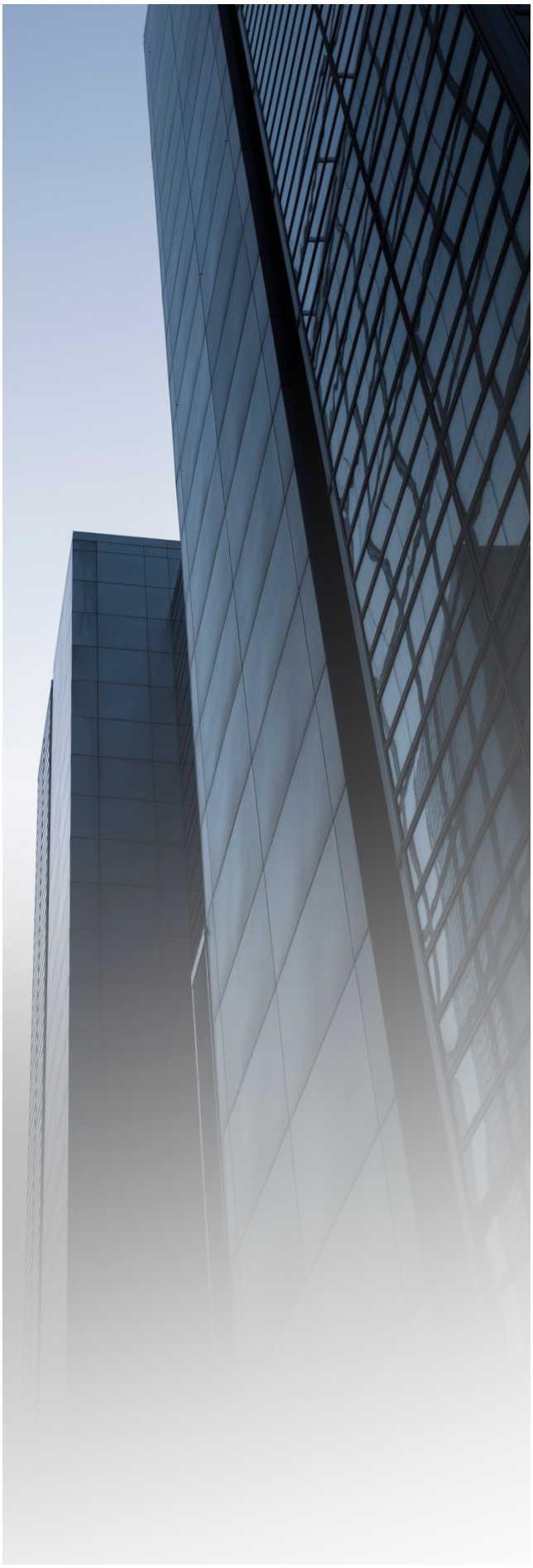
- Now is the perfect opportunity to invest in your FinCrime team to ensure morale and motivation levels are maintained. It would be easy to cancel some of those 'lunch and learns' or training sessions you had planned but don't; keeping your team engaged at this crucial time is as important as maintaining any system.
- With working styles already disrupted, FFE members said this was a perfect opportunity to encourage more flexible working hours. Do your team need to work 9-5, Monday to Friday? Possibly not.
- This could be the right time to reconsider the structure of your FinCrime operation. Depending on the size of your business you may already operate a three lines of defence model, but if you are not, this may be the right time to think about ensuring you have an appropriate and proportionate 1st and 2nd line. Equally if you already have this model implemented, and are happy with the current structure, consider assessing the roles which both lines perform and whether it needs tweaking.
- Whilst resources may be more limited than usual it is still important that enough time is spent on quality assurance and quality control. In these unstable times having the resource to perform assurance on your AFC framework and quality control on the tasks is vital in maintaining effectiveness.
- Similar to the suggestions to have a contingency plan for your systems, you could consider whether there is a plan B for the people that support your framework. Are there opportunities for new ways to automate tasks or should you consider new outsourcing arrangements?
- Consider adopting new tools and relying on existing ones to assist with communicating internally. Members of the FFE continue to communicate with one another via the Slack channel and the first remote monthly meetup was successfully held in March via video conference.
- Updating and distributing management information to senior stakeholders will keep them informed throughout this period where face-to-face relationship management is impossible. Equally, distributing this information to the wider FinCrime team will help to keep them engaged and know what they are contributing towards.
- Don't cancel decision forums within the business such as your Risk Committee. These forums are a vital escalation route.

**Re-prioritise and re-communicate**

Having completed your retrospective by reviewing your tolerance thresholds, reassessing your inherent risks and performing an effectiveness exercise on your AFC framework, it is now the right time to re-prioritise. Never has there been a more appropriate time to rely on your risk-based approach to determine where you need to apply your resources. Once you have determined your priorities, these should be introduced into your FinCrime BCP and recommunicated, and then the cycle should start again as it develops into a pandemic plan.

With thanks to members of the FinTech FinCrime Exchange for sharing best practices.

FINTECH
FINCRIME
EXCHANGE



# Annex 1 - Common scams

According to Action Fraud, the National Fraud Intelligence Bureau (NFIB) has identified 21 reports of fraud where coronavirus was mentioned, with victim losses totaling over £800k since February 2020. It expects reporting numbers to rise as the virus continues to spread across the world. More recently the UK's National Crime Agency published a comprehensive fraud awareness piece on its website.

The UK is not an exception in this regard - the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) advised FIs this week to remain alert to malicious or fraudulent transactions similar to those that occur in the wake of natural disasters. Similarly, Europol published a report on the latest developments of COVID-19 on the criminal landscape in the EU.

We divided COVID-19 related scams into four categories: imposter, product scams, investment scams, and insider trading. There are other ways criminals may try to exploit the current crisis, including cybercrime, but we have focused on scams which FinTechs may detect through customer or transaction monitoring.

**Imposter Scams**

Bad actors attempt to solicit donations, steal personal information, or distribute malware by impersonating government agencies, international organisations, or health care organisations.

The World Health Organisation (WHO) urges anyone contacted by a person or organisation that appears to be from WHO, to verify their authenticity before responding. It confirms that the only call for donations WHO has issued is the COVID-19 Solidarity Response Fund. Any other appeal for funding or donations that appears to be from WHO is a scam.

Alternatively (as reported by Action Fraud), rather than asking for donations, some fraudsters claim to be able to provide the recipient with a list of coronavirus infected people in their area. In order to access this information, the victim needs to click on a link, which leads to a malicious website, or is asked to make a payment in Bitcoin.

Scammers are also creating and manipulating mobile apps designed to track the spread of Covid-19 to insert malware that will compromise users' devices and personal information.

Another type of a COVID-19 fraud scam, reported by Interpol, involves a telephone fraud – criminals call victims pretending to be clinic or hospital officials, who claim that a relative of the victim has fallen sick with the virus and request payments for medical treatment.

- **Advise your customers to carry out some research before making any donations, especially if prompted to do so by unsolicited emails and texts.**
- **Remind your customers that your firm would never contact them out of the blue to ask for financial details such as their PIN or suggest moving funds to another account.**

**Product Scams**

In a summary of the 21 coronavirus related reports identified by the NFIB, Action Fraud stated that ten were made by victims that attempted to purchase protective face masks from fraudulent sellers. One victim reported losing over £15k when they purchased face masks that were never delivered. FinCEN has also received reports regarding fraudulent marketing of COVID-19 related supplies, such as certain facemasks.

In one of the first cases in the UK, a man has appeared in court charged with making fake kits which claimed to treat COVID-19. He was arrested by the City of London Police's Intellectual Property Crime Unit after it was contacted by US counterparts. The kits allegedly contained harmful chemicals which people were being told to use to rinse their mouths.

Law enforcement agencies taking part in Operation Pangea, coordinated by INTERPOL, found 2,000 online links advertising items related to COVID-19. Of these, counterfeit surgical masks were the medical device most commonly sold online, accounting for around 600 cases during the week of action. The seizure of more than 34,000 counterfeit and substandard masks, "corona spray", "coronavirus packages" or "coronavirus medicine" reveals only the tip of the iceberg regarding this new trend in counterfeiting.

Separately, the US Federal Trade Commission (FTC) and Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19.

Both organisations urge consumers to be on the lookout for scammers taking advantage of fears surrounding coronavirus and report on already identified products including teas, essential oils, and colloidal silver. The FDA says there are no approved vaccines, drugs or investigational products currently available to treat or prevent the virus.

- **Advise your customers to carry out some research before completing a purchase, if they are purchasing goods and services from a company or person they don't know and trust.**
- **Remind your customers to be wary of unsolicited emails and texts offering questionably good deals, and never respond to messages that ask for their personal or financial details.**

**Investment Scams**

Fraudsters often use the latest news developments to lure investors into scams. FinCEN repeated the Securities and Exchange Commission (SEC) warning that urged investors to be wary of COVID-19 related investment scams, such as promotions that falsely claim that the products or services of publicly traded companies can prevent, detect or cure coronavirus.

The SEC has become aware of a number of Internet promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus, and that the stock of these companies will dramatically increase in value as a result. The promotions often take the form of so-called "research reports" and make predictions of a specific "target price".

It specifically identified microcap stocks (low-priced stocks issued by the smallest of companies) as potentially particularly vulnerable to fraudulent investment schemes, including coronavirus-related scams.

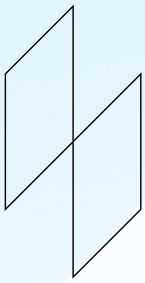
Fraudsters may try to use "pump-and-dump" schemes to increase the stock price of a company by spreading positive, but often false, rumours before quickly "dumping" their own shares before the hype ends.

- **Advise your customers to use the FCA's register and warning list to check if a company is regulated by the FCA.**
- **Remind your customers to not be rushed into making an investment. Legitimate firms will never pressure customers into making a transaction on the spot.**

**Insider Trading**

France's Autorité des Marchés Financiers (AMF) recently highlighted that in addition to human considerations, the current coronavirus epidemic has led to the shutdown of certain fields of business. As such AMF, and more recently SEC, warned about an increased risk of insider trading, as those privy to material non-public information about the negative impacts of COVID-19 on financial performance may be motivated to sell shares before that information is publicly disclosed or tip others with that information. FinCEN has also received reports regarding suspected COVID-19-related insider trading.

In the most recent developments, four US senators are under scrutiny over claims they used insider knowledge about the impending coronavirus crisis to sell shares before prices plummeted.



# FINTECH FINCRIME EXCHANGE

FINTRAIL

rdc
Smarter Screening

ffe_admin@fintrail.co.uk
www.fintrail.co.uk/ffe