

 eBook

fiserv.

Financial Crime Survey 2020

January 2021


THEMIS

Introduction

Every year, it is estimated that between two and five percent of global GDP is laundered through our global financial networks.¹ However, only one percent of illicit financial flows are intercepted globally. Criminals clearly remain several steps ahead and COVID-19 has only given them an extra edge.

In the first half of 2020, Fiserv conducted a four-part survey to understand industry views on the current state of financial crime and financial crime prevention, especially in light of COVID-19. All those surveyed were anti-money laundering (AML), fraud, financial crime or general compliance professionals from across the Europe, Middle East and Africa (EMEA) region. The four survey parts received differing numbers of responses, ranging from 126 in Part I to 55 in Part IV. The survey was carried out using SurveyMonkey.

An analysis of responses revealed four prominent interweaving themes across the different survey parts. The following report is structured according to these four themes, which are illustrated in Figure A. Together, they explain current financial crime risks and effective prevention techniques, as seen by compliance practitioners.

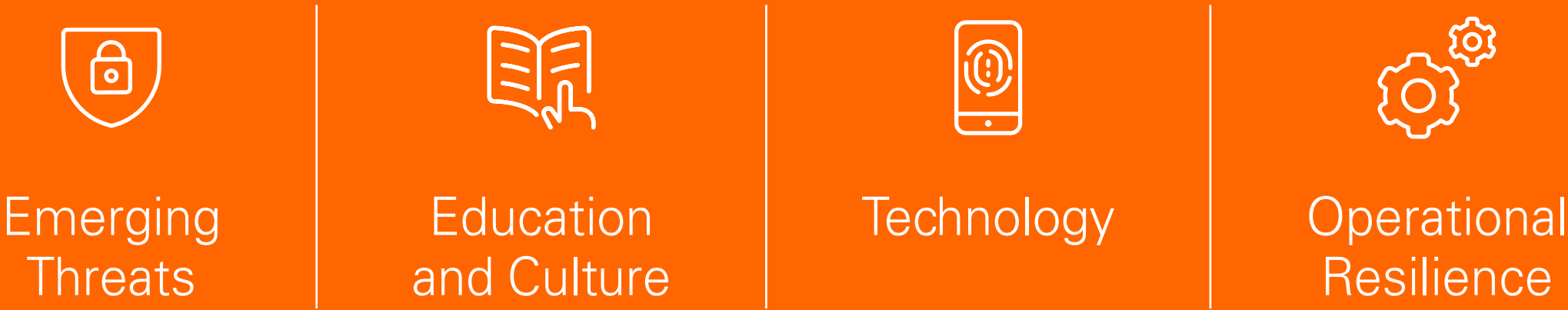


Figure A. Core financial crime survey themes

¹[unodc.org/unodc/en/money-laundering/globalization.html](https://www.unodc.org/unodc/en/money-laundering/globalization.html)



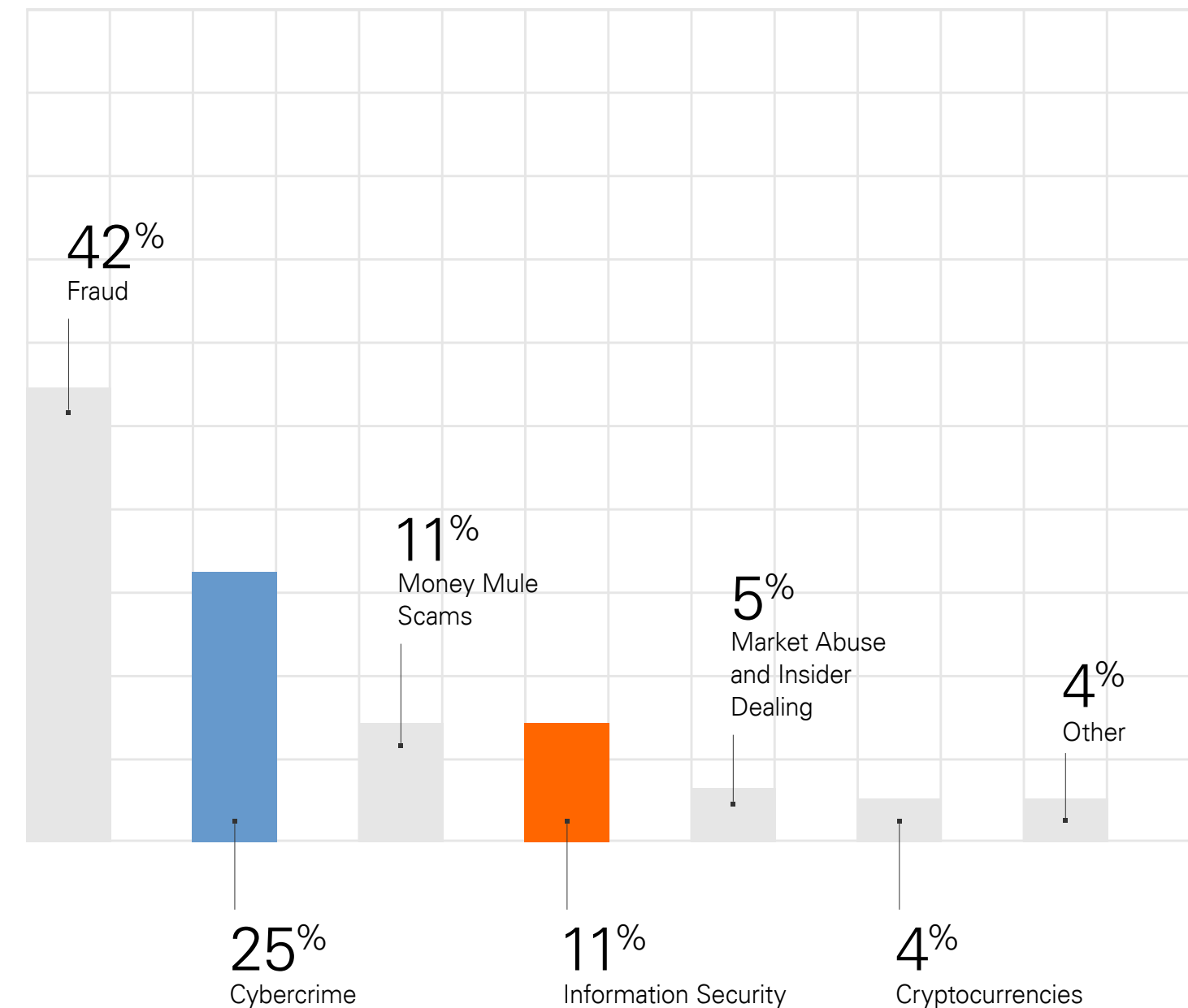
Emerging Threats

Trying to pin down emerging financial crime threats is as challenging as trying to estimate the cost of financial crime. External risks are not static and continue to shift in accordance with the weakest links in firms' anti-financial crime measures. The ability of financial criminals to stay ahead of the game by adjusting their methods to changing circumstances stood out as a key survey theme. Just over half of respondents believed that regulators should focus their lockdown work on educating financial institutions and the public about criminals' changing approach.

COVID-19 was cited as being partly responsible for this increased criminal adaptability and 61.4 percent of respondents indicated that COVID-19 has created new financial crime threats. Although the vast majority of that group said its impact has been relatively "minor," it is likely that the true extent of financial crime arising during the pandemic will not be realised for a considerable period. Other emerging risks pre-date and have simply been accelerated by COVID-19.

Survey respondents were particularly concerned about two latent financial crime threats. When asked about criminals' main area of focus during the global lockdown, 42.1 percent said fraud and 24.6 percent said cybercrime, as shown in Figure B. An analysis of qualitative responses enabled a further breakdown of these two main threats into sub-categories, illustrated in Figures C and D.

Figure B. What areas do you think criminals will focus on in order to take advantage of the global lockdown?



According to recent estimates, fraud is costing the global economy approximately £3.89 trillion per annum, which equates to 6.05 percent of the world's GDP.²

The two types of fraud most frequently cited as a worry for Fiserv survey respondents in 2020 were personal protective equipment (PPE) procurement fraud and COVID-19 bailout fraud, both of which have emerged as a direct result of the pandemic. The urgent need for medical supplies saw many governments relax procurement checks and balances, with the desire for speed frequently coming at the expense of scrutiny. The flipside of less scrutiny is more opportunity for cronyism and corruption, and therefore a greater probability of procurement-related misspending. Concurrently, governments have mobilised unprecedented support programmes and stimulus packages in response to the pandemic. Given the speed and scale at which these schemes have been expedited, some mispayment has been inevitable. Indeed, in early September, HM Revenue and Customs estimated that 5–10 percent of furlough payments in the United Kingdom (UK) may have been claimed fraudulently or paid out in error. Survey respondents were acutely aware of both of these trends.

²[crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf](https://www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf)

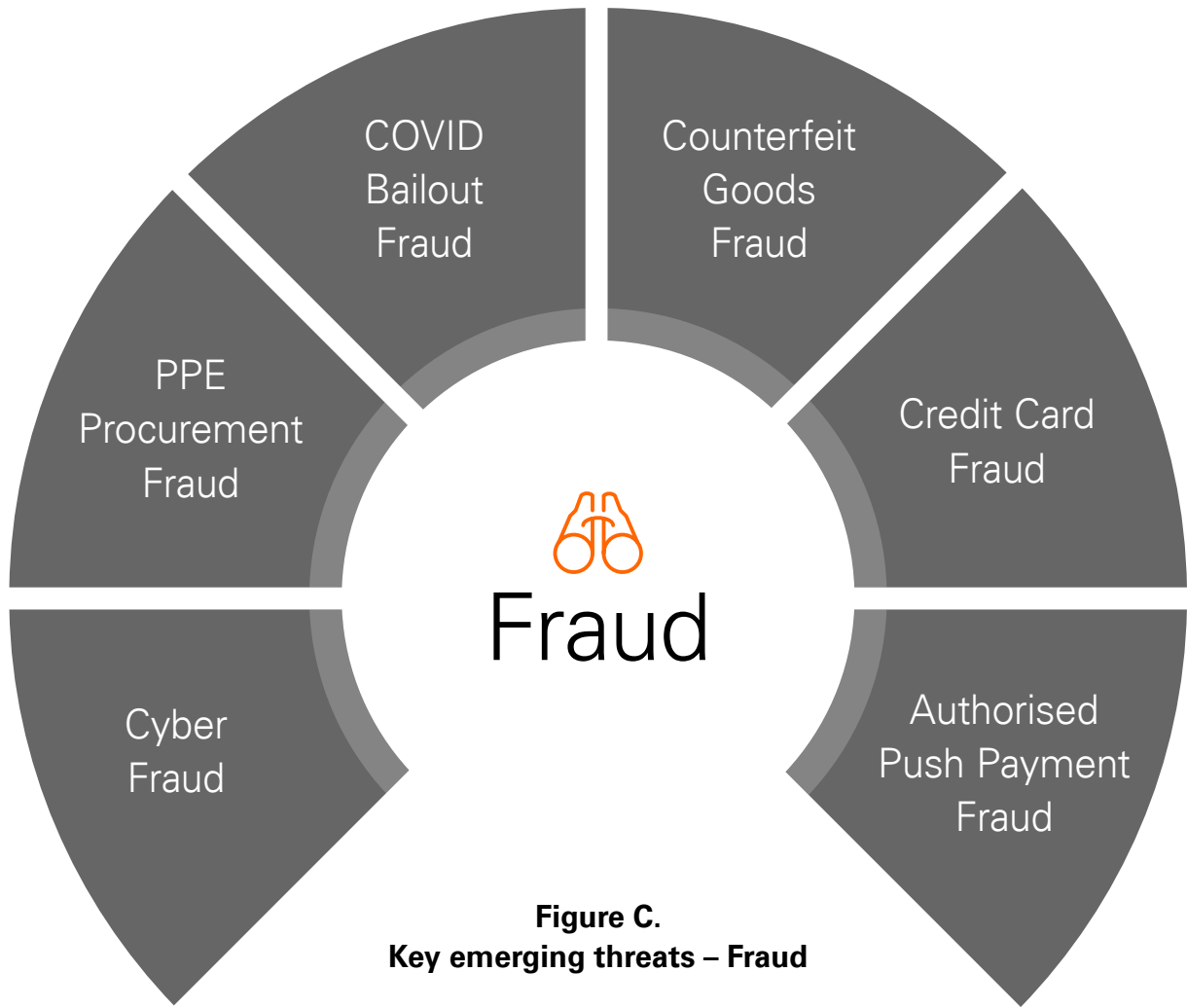


Figure C.
Key emerging threats – Fraud



The other forms of fraud highlighted by respondents reflect broader current patterns of criminal activity that are not directly related to COVID-19. Two of them – authorised push payment (APP) fraud and credit card fraud – echo the recent focus placed on payment fraud by regulators and international authorities. For example, the Financial Conduct Authority (FCA)’s Annual Report 2019/2020 notes that reported APP fraud in the UK increased from £354.3M (84,624 cases) in 2018 to £455.8M (122,437 cases) in 2019. At the European level, the European Payments Council has expressed particular concern about a rise in technologically sophisticated payment fraud, such as Advanced Persistent Threats (APTs). APTs involve malicious software which targets specific databases containing valuable card or customer information, with the aim of compromising the system to gain payment card data.

After fraud, cybercrime was the second most frequently cited emerging threat in the survey. Respondents were worried about several particular types of cybercrime, namely phishing, cyber fraud, digital ID theft and cryptocurrency abuse, as shown in Figure D. This is again largely in keeping

with both the immediate and longer-term concerns of regulators and international organisations. Interpol, for example, analyses cybercrime developments on a continuous basis. In August 2020, it produced a detailed assessment of the impact of COVID-19 on cybercrime which highlighted a significant global increase in online scams, phishing, disruptive malware, malicious domains and misinformation as a result of the pandemic.³

According to survey results, the pandemic has not only given rise to certain new financial crime threats, but also increased public pressure on regulators and financial institutions to tackle these threats. A majority (56.1%) of respondents believed the public will “expect more protection” following the COVID-19 crisis. Fortunately, the number of respondents reporting an improvement in their financial crime team’s effectiveness during the pandemic is slightly higher (27.6 percent) than the number reporting a fall in detection effectiveness (22.1 percent). Furthermore, many respondents highlighted the new financial crime typologies being developed by their teams in response to emerging risks.

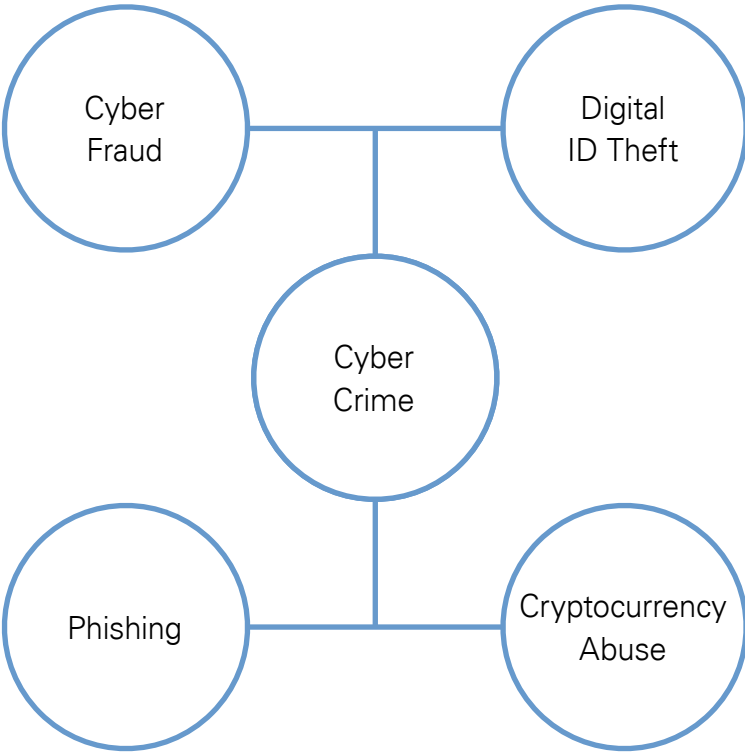







Figure D. Key emerging threats – Cybercrime

³[interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19](https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19)

Figure E. Top 5 areas regulators should focus on when developing new regulatory directives

-  Issuing clearer guidance and updating typologies to reflect new technological developments
-  Increasing collaboration and information-sharing between regulators and financial institutions, including internationally
-  Implementing more effective monitoring systems and tools
-  Increasing focus on training, especially in the field of technology
-  Demonstrating greater flexibility towards firms' different risk profiles

Respondents were also fairly positive about the way in which regulators have approached pandemic-era threats. For example, 71.1 percent indicated that regulators had communicated amendments to mandatory timelines as a result of COVID-19. Similarly, 62.9 percent expected “slight changes” on the part of regulators “to reflect changes in the economy” once the pandemic has subsided. In the longer term, respondents emphasised the need for a more collaborative regulatory approach to financial crime risks, as shown in Figure E. Survey responses repeatedly mentioned the importance of greater collaboration between regulators, between financial institutions, and between regulators and financial institutions. In this vein, the overriding majority (87.5 percent) of respondents said that the European Union’s proposed new European anti-money laundering supervisory body would have a long-term benefit on the international fight against financial crime.

This is, in theory, an admirable desire and there have been some examples of successful collaboration that have had a marked impact on financial crime. Notable amongst these is the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT), a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats. However, many firms see financial crime as a competitive issue and will not share or divulge financial crimes that have occurred within their organisations. It is, therefore, important to take advantage of any joined-up approaches to tackle financial crime, but it is even more important for firms to build up their own defences. Emerging threats tend to strike the weakest link in an organisation first.



Education and Culture

A concerted fight against financial crime hinges on acute awareness, understanding and appreciation of threats by the public, compliance experts and senior management alike. As was indicated throughout the survey, criminals will continue unchecked if their methods are not understood.

When asked how best the general public can support the fight against financial crime, the overriding majority of respondents said by becoming more knowledgeable about risks. Public awareness was seen as important for two reasons. Firstly, an informed public is better placed to spot suspicious activity and report it to authorities. Secondly, aware individuals are less likely to become victims of financial crime themselves.

Respondents cited a range of ways in which public understanding of financial crime can be increased, as illustrated in Figure F. The role of regulators and financial institutions in educating consumers through campaigns, training courses and informational material was particularly underlined. For instance, 87.7 percent of respondents said that banks need to place more focus on helping their customers “spot criminal activity”.

Figure F. Main ways to increase public awareness of financial crime risks



Governments including financial crime in school curricula



Regulators and other relevant authorities providing online courses focused on financial crime awareness



Regulators and other relevant authorities carrying out more anti-financial crime advertising and campaigns



Banks educating customers to spot criminal activity



Raising public awareness to help consumers protect themselves against financial crime threats is a top current priority of many regulators in the EMEA region, as recommended by Europol and other international bodies. In keeping with the view of survey respondents, Europol’s annual “Organised Crime Threat Assessment” reports repeatedly emphasise the need for EU Member States to continue promoting preventive and educational initiatives to increase public understanding of cyber and other types of crime.

Alongside their emphasis on public education, survey respondents highlighted the importance of continued learning on the part of experts within financial crime teams. Ongoing training to help anti-financial crime professionals understand emerging threats and bolster technological skills was seen as particularly key. Accordingly, respondents were positive about the opportunities for upskilling that COVID-19 has provided, notably through webinars and e-learning tools.

To facilitate further education, respondents underlined the need for regulators to provide financial crime teams with more guidance material, especially with regard to new technologies. This is illustrated in Figure E and explored in more detail in the “technology” section.

However, the survey also indicated that knowledge and appreciation of financial crime risks within financial institutions cannot be confined to specialist anti-money laundering and compliance teams. Respondents conveyed a strong message about the importance of organisation-wide anti-financial crime culture, including at senior management levels. This is a theme repeatedly echoed by regulators across the world. For instance, the UK’s FCA set “culture in financial services” as a key priority in its 2020/21 Business Plan, whereas in the United States, FinCEN published a document entitled “Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance”

Figure G. Can regulators enforce an anti-financial crime culture without fining financial institutions excessively?

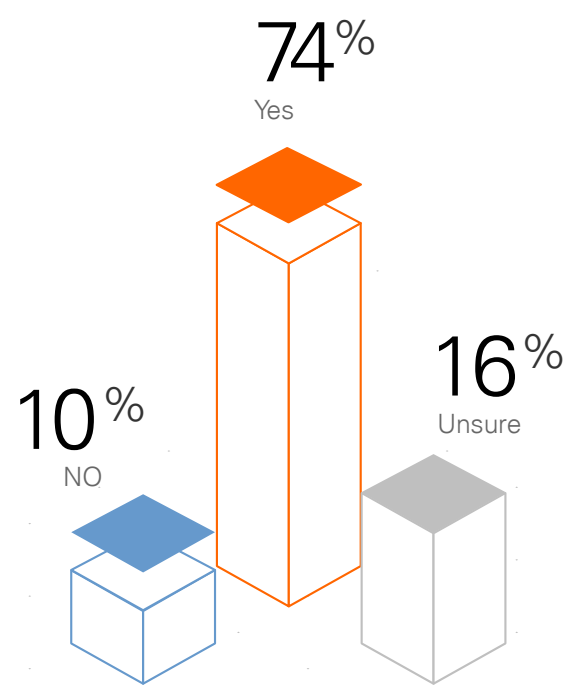


Figure H. Top seven most effective ways to create an anti-financial crime culture in financial institutions



Although creating the right anti-financial crime culture is not always easy, it is the surest and most sustainable way to curtail the success of financial criminals in the long-term.

⁴wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf

Survey responses brought out a range of ways in which an anti-financial crime culture can be fostered, as portrayed in Figure H. Interestingly, 74.4 percent of respondents said that large fines or the threat thereof were not the most effective method, as Figure G illustrates. Instead, training, guidance and advice from regulators were seen as particularly powerful, demonstrating the inextricable link between culture and education. The threat of sanctions for senior management came a close second, highlighting the cardinal importance of setting the right tone at the top, including through a sense of personal accountability for compliance breaches at the highest levels. This is fully in tune with the recommendations of regulators and international standard-setting bodies. For example, the Wolfsberg Group, a non-governmental association of thirteen global banks, emphasises that “in order for a risk assessment to be successful, senior management, along with key stakeholders, should provide appropriate support to the effort in the context of fostering a robust culture of compliance”.⁴



Technology

Disruptive new technology is proving a double-edged sword in the fight against financial crime. As one survey respondent put it, “technology is playing a vital role for all financial institutions and criminals”. Fraudsters and money launderers are making use of cryptocurrencies, artificial intelligence (AI) and other new developments to commit a diverse range of cybercrimes, which this survey cites as key emerging threats.

Fortunately, financial crime teams are also assimilating and benefiting from technological advances themselves. Respondents pointed out the positive effects that digitisation, in particular, has had on their work. Migrating processes online has saved time whilst also improving results. Notably, 42.3 percent of those surveyed reported a “notable increase” in their team’s level of detection effectiveness following the introduction of sophisticated new technology. Indeed, there is a clear desire to move beyond simple digitisation to a more thorough embrace

of cutting-edge methods, with 46.5 percent of respondents declaring AI and robotics to be “central” to their team’s strategy.

Sanctions screening was cited as the area of financial crime prevention best addressed by technology to date, with Know Your Customer (KYC) and onboarding faring worst. This dichotomy is unsurprising given the range of online sanctions databases and traditionally face-to-face nature of certain KYC tasks like identity verification. However, there is a sense that COVID-19 is accelerating the digitisation of KYC and onboarding, with 70.3 percent of respondents reporting either a “slight” or “significant” prioritisation of both processes as a result of the crisis, as shown in Figure I. In addition to acting as a procedural facilitator, technology emerged as a key enabler of education and training for surveyed financial crime teams, specifically through e-learning, online courses and webinars.

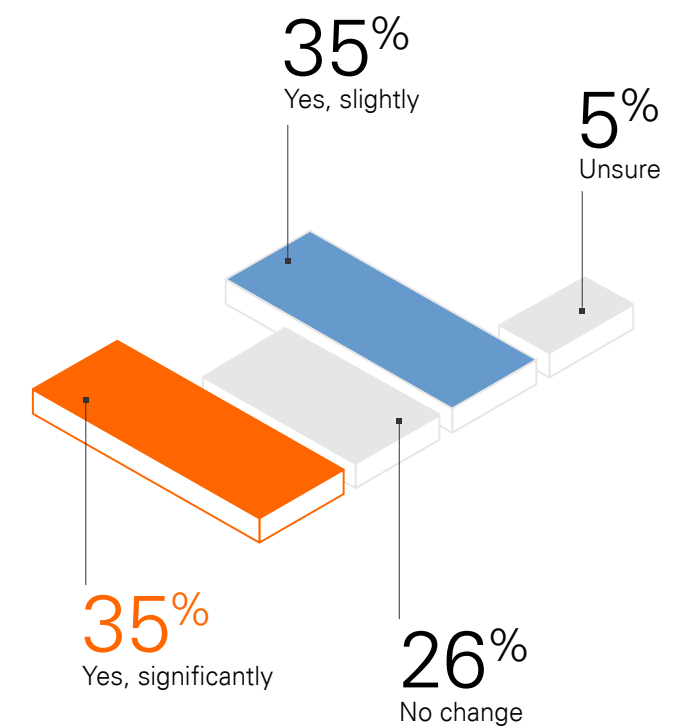
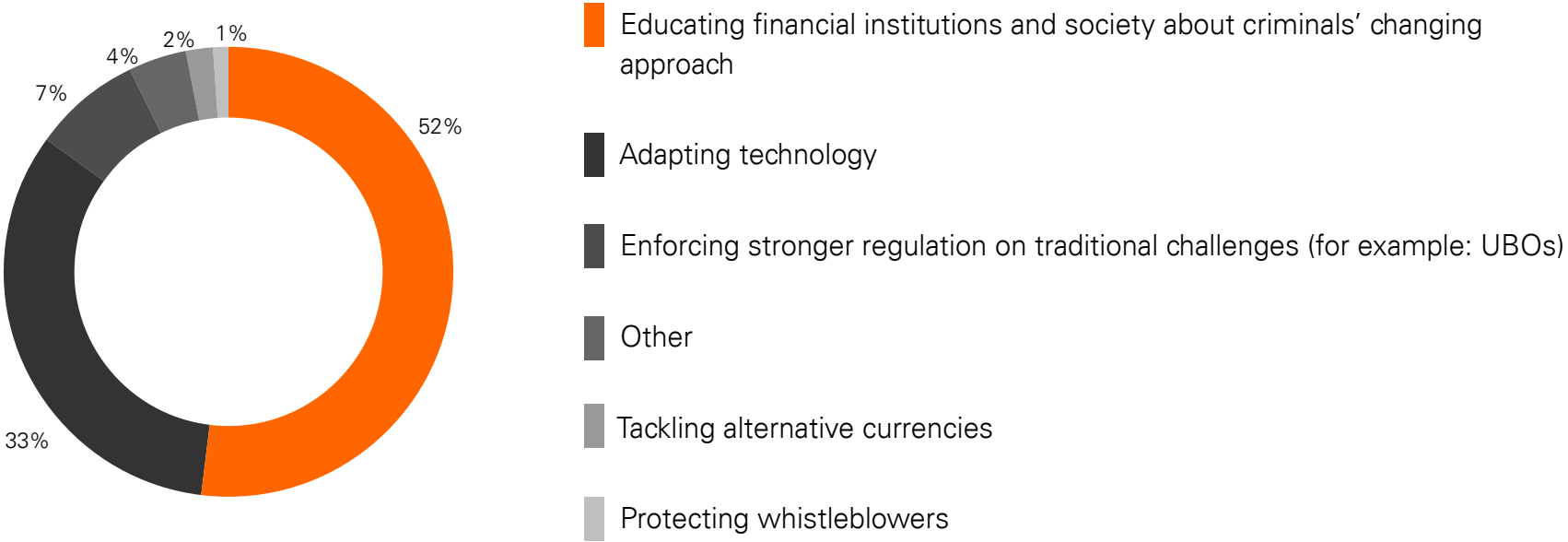


Figure I. Has COVID-19 accelerated the prioritisation of digital onboarding and simplified due diligence projects?



Survey responses conveyed somewhat more mixed feelings about regulators’ progress in absorbing and promoting new technology. As shown in Figure J, respondents said that “adapting technology” was a key area for regulators to consider during lockdown, second only to educational campaigns about changing criminal approaches. Although qualitative survey answers acknowledged how tricky it is for regulatory directives to keep pace with technological advances, they also underlined the need for greater proactivity in this regard on the part of regulators. Notably, many alluded to a lack of satisfactory regulatory guidance on topics like cryptocurrencies, electronic identity verification and fintech. Existing guidelines were criticised for being too scant, too vague or not tailored enough to different business risk profiles.

Figure J. What areas do you think regulators should be focusing on to combat financial crime during lockdown?



Regulators are acutely aware that they need to keep up with the digital age. The Financial Action Task Force, an inter-governmental body that sets international AML standards, lists “engagement with the FinTech and RegTech” communities as one of its priorities. It has, moreover, published several guidance documents for regulators and financial institutions about the opportunities and risks presented by different technological developments, such as digital identity systems and virtual currencies.



Operational Resilience

The chaos caused by COVID-19 has brought home the importance of operational resilience, which can be defined as the organisational ability to absorb the impact of disruptive events. Survey respondents mentioned a number of adverse ways in which the pandemic has affected their business operations. As illustrated in Figure K, these ranged from reduced business demand and adaptation to new COVID-era financial crime threats to the challenges of adjusting to remote working. Organisations that had thorough business continuity plans and operational resilience frameworks in place have generally weathered the shock of the pandemic better. For instance, some respondents said COVID-19 did not affect their working methods because these were already highly digitised.

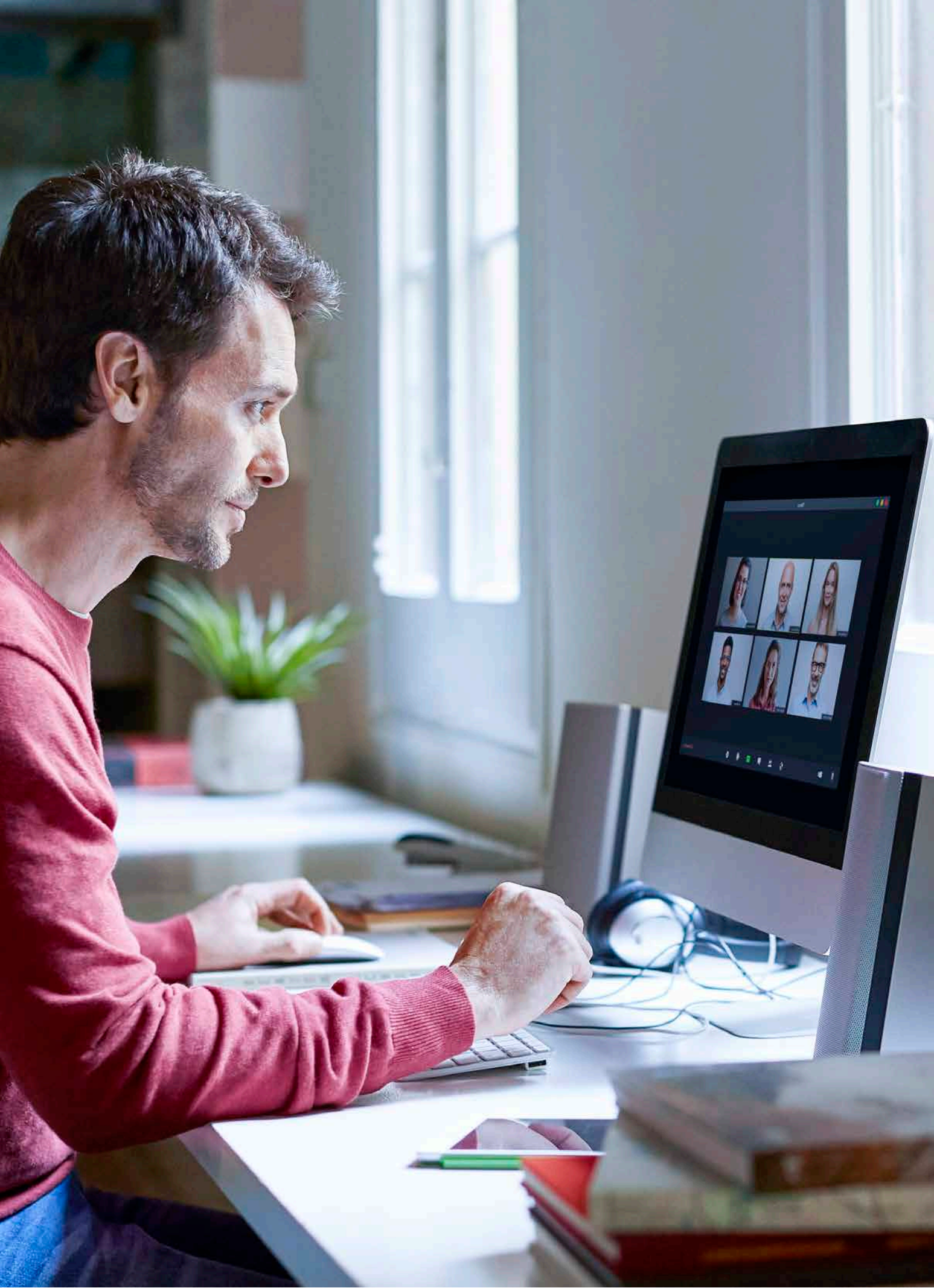
Positive Impacts

- More time to review and enhance systems, policies and procedures
- More opportunities to upskill team members, especially through e-learning and webinars
- More incentive to improve team members' cyber capabilities specifically
- Accelerated digitisation of tasks like onboarding and simplified due diligence
- Updates to operational processes to enable effective remote working

Adverse Impacts

- Reduction in business demand and associated detrimental financial consequences
- Adaptation to new COVID-related financial crime threats
- Operational challenges associated with remote working
- De-prioritisation of some experimental solutions like AI and robotics in favour of more immediately effective methods
- Increased pressure on financial institutions to protect society from financial crime

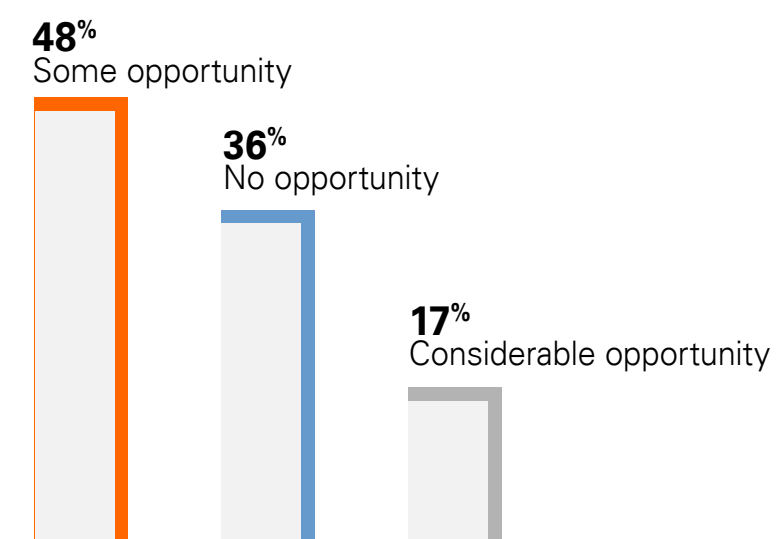
Figure K. Effects of COVID-19 on the work of financial crime teams

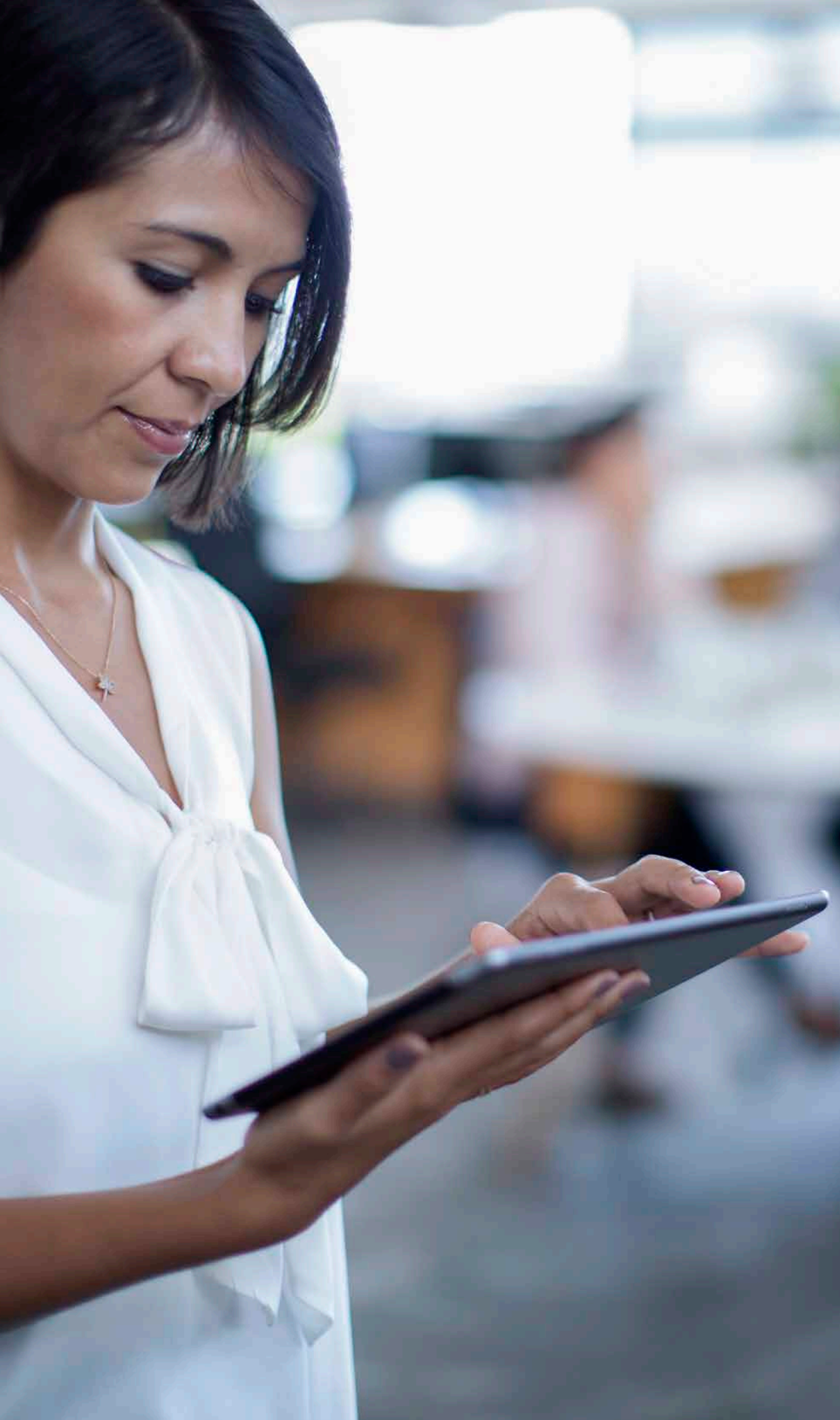


However, most respondents (70.1 percent) said that slight changes to their team’s operational processes did need to be implemented to reflect the impact of remote working. In this sense, the pandemic has represented a disruptive event that tested but ultimately often strengthened operational resilience. Indeed, the survey brought to light a range of positive effects that COVID-19 has had on the work of financial crime teams, as summarised in Figure K. Some respondents have had more time to review procedures or clear backlogs, others have seen their teams accelerate the digitisation of certain compliance tasks. As demonstrated by Figure L, 65 percent saw at least some opportunity to upskill team members during the crisis.

When viewed through the lens of operational resilience, the pandemic-related aspects of this survey gain vital long-term applicability. Lessons learned as a result of COVID-19 will help organisations grapple with the next crisis from a position of strength. The merits of focusing on operational resilience have also been highlighted by regulators and international bodies in recent years. For instance, the Basel Committee on Banking Supervision, which is the primary global standard-setter for the prudential regulation of banks, published a consultative document entitled “Principles for Operational Resilience” in August 2020. This document emphasises the importance of “a bank’s forward-looking operational resilience regime in line with its operational risk appetite, risk capacity and risk profile”.

Figure L: Have you seen any opportunity to upskill team members during the COVID-19 crisis?





Conclusions

This survey provides valuable insight into the views of AML, fraud and general compliance experts on the state of financial crime in 2020. It highlights the crucial role that technology, education and anti-financial crime culture play in building the operational resilience needed to counter emerging threats like fraud and cybercrime. Many of the survey’s findings are in line with the current priorities of regulators from across the EMEA region, although respondents call for an even more concerted and innovative regulatory push to tackle illicit financial flows. As organisations continue to grapple with the protracted impact of COVID-19, financial crime should be at the top of public and private sector agendas alike.



Nadia O'Shaughnessy
Manager, Themis Think Tank
nadia.oshaughnessy@themisservices.co.uk
+44-(0)-7860-702-744



Viri Chauhan
MD, Themis Community
viri.chauhan@themisservices.co.uk
+44-(0)-7967-451-523



Dickon Johnstone
CEO, Themis
dickon.johnstone@themisservices.co.uk
+44-(0)-7968-537-954

Connect With Us

For more information
about financial crime surveys:

 alan.jarvie@fiserv.com

 [fiserv.com](https://www.fiserv.com)

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today.

Visit [fiserv.com](https://www.fiserv.com) to learn more.

