Emerging stronger from disruptive events

Rethinking fraud and economic crime

pwc

This report looks at the top 10 aspects organisations need to pay attention to from a forensic perspective, in order to ensure better governance in the wake of disruptive events and crises:

01	**Build trust in financial information**	02	**Refresh fraud and misconduct risk and controls**
03	**Safeguard business interests**	04	**Protect against accentuated insider threats**
05	**Safeguard against amplified fund diversion**	06	**Adapt to the paradigm of 'new whistles'**
07	**Manage significantly increased counterparty risk**	08	**Prepare for deeper and intense regulatory probes**
09	**Accelerate digital transformation of forensics**	10	**Renew commitment to crisis management**

As countries, organisations and businesses gradually reopen and restart, it is clear that many fundamental aspects of business have changed drastically in a very short period of time. Unplanned events of the nature that we are currently witnessing across the globe are accompanied by significant disruption and unique challenges. Such an environment often leads to the rise of fraud, misconduct and economic crimes. If organisations fail to address these threats in time, they could have a far-reaching impact on business. In a disruptive environment, traditional deterrents or pre-existing mitigation measures often prove to be ineffective against prevention of frauds. Therefore, the situation becomes more complex. Some of the major challenges organisations face are discussed below:

- Economic uncertainty provides an impetus to financial fraud perpetration. Stemming from the need to show stable business results or recovery or simply to hide 'ghosts of the past', economic crime rears its head whenever unplanned events strike.
- Controls may not have kept pace with the disruptive changes in business in a short span of time. An inflected control environment, in effect, weakens critical lines of defence against economic crime and aids perpetration of fraudulent activity.
- The 'human factor' needs constant attention in rough waters. A 'distanced' workforce, rapid social changes, possibly low morale, uncertain economic conditions, etc., are all factors that exacerbate fraudulent behaviour in troubled times.

Over the last few years, economic crime in India has undergone a significant metamorphosis, with larger and more prominent frauds being perpetrated in changing economic conditions. It is therefore not unreasonable to expect that as companies look to recover from a dampened global economy, altered business scenarios and additional regulatory pressures, the types of economic crime and the measures for containing and combating them will change. Given this context, this report discusses the **top 10 areas** that require immediate consideration and attention from companies from a forensic perspective.

01 Build trust in financial information

Outlook

Degraded or significantly impacted operations create scepticism in the minds of users about financial information. In this scenario, we expect users of financial information to inquire into the following aspects:

- Is the full impact of the disruption captured completely and disclosed or reflected accurately and transparently?
- Is there any intent to misapply accounting principles to soften the blow or show a different financial picture, or otherwise manage earnings in the short or medium term?
- Are any ghosts of the past surfacing? Is there any attempt to disguise the impact of past frauds and club these with the disrupted business scenario?
- Is there rigour around reporting – both with internal and management reports? Are internal decisions backed by accurate and verified internal information?
- Is the current situation being used to build 'cookie jar' reserves for the future?
- Do any transactions lack substance over form?
- Does the financial information present the true financial position of the underlying businesses or is there any element of disguise for stakeholder management?

What's next

We can expect to see an increase in focused forensic reviews and investigations, particularly as various stakeholders would want to follow a 'trust but verify' approach. We expect these activities to cover special transactions – for example, movement and end use of funds, arm's-length transactions, changes in accounting policies or practices, substance over form of significant transactions, write off or write on of significant amounts, impact of significant or material financial transactions, material transactions for significant acquisitions or divestments, undisclosed related-party transactions and general health of customer or vendor portfolios. These reviews are likely to be commissioned by:

- boards, audit committees, independent directors and investors (including private equity) on presented financial information and operational results
- potential investors during mergers and acquisitions, particularly in the case of distress sales or strategic acquisitions
- lenders in cases of extension or acquisition of facilities to assist in recovery plans or for monitoring end use of funds by borrowers
- regulators (stock market and otherwise) since the disrupted business environment could result in additional whistle-blowing complaints to regulators
- parties/counterparties in significant, high-value and complex business contracts.

02 Refresh fraud and misconduct risk and controls

Outlook

Rapid changes in business and working in 'survival mode' require reassessment of risks and adjustment of controls that may not have kept pace with disruptions. Companies therefore need to ascertain that their fraud and misconduct risks are updated to reflect the realities of changed business scenarios, particularly remote working or changed modes of interactions with vendors, customers and other third parties.

Further, there are a few special areas where reassessments will be crucial:

- **Bribery and corruption:** Due to the changed contours of business interactions, the modus operandi for bribery and corruption would change, mandating an update to policies and procedures. For example, entertainment, cash payments or similar methods (which may not be physically possible because of social distancing or work from home) could morph into additional payments through third parties.

  Further, the risks associated with obtaining additional licences, approvals or consent (to operate facilities, movement of people, inspections for containment, etc.) also need to be considered, along with reassessment of associated third-party risks.
- **Anti-trust or anti-competition:** Given the challenging business environment, businesses could enter into informal agreements to control prices (rent, supply chain, logistics, etc.) or grant relief (quantum of rent waivers, discounts, etc.). At this time, it is important for companies to recognise these additional risks, particularly in the recovery period, and take proactive steps to demonstrate that their behaviours emulate good practices and compliance with laws.

What's next

We expect to see companies update their fraud risk assessments, and re-evaluate and prioritise fraud risks in all major business processes to reflect the following:

- additional fraud risk scenarios or modus operandi arising from changes in the way of doing business or changes in their key business processes
- adjusting for changes in existing fraud risks for likelihood of occurrence and potential impact based on changed operations
- adjusting controls to reflect work from home and changed modes of interaction between employees and the external ecosystem
- determining the responsiveness of existing controls to reassessed risks and additional interventions required to enhance effectiveness of the controls.

Companies may also seek to evaluate fraud risk assessments – specifically those related to financial reporting – and review fraud controls over internal management information systems.

03 Safeguard business interests

Outlook

Economic adversity creates circumstances where companies can fall prey to external threats and bad actors that compromise their business. Companies will need to be agile in identifying these threats and addressing them effectively before they cause irreparable damage. Under the current scenario, we expect business threats that emanate from the following:

Fake news

Misuse of social media could cause reputation issues besides financial damage. Rogue agencies could spread fake news to gain competitive advantages in the short term. Thus, it is important to check and address such incidents on time. In a situation where information is exchanged on a large scale digitally, without adequate opportunities for fact checking, fake news can indeed pose significant threats.

Claims, litigation and disputes

Disruptions arising from unplanned events can pose significant challenges to specific performance of contracts. From repudiation of contracts to increased time and cost overruns, an organisation can be significantly tied down to interventions – mediations, arbitration or litigation. Companies will need to assess legal remedies and quantification of claims/losses/damages in preparing strategies both for making or defending claims. Further, companies should also evaluate more innovative and efficient approaches for redressals, such as renegotiation of contracts and pre-dispute amicable settlements.

Privacy and confidentiality

As work moves out of workplaces into homes and off-site operations, security of data and information will become paramount. Companies will have to take proactive steps to build trust with stakeholders (internal and external) on the security and safety of data and information in the remote working scenario.

Productivity lapses

Out of site cannot be out of mind. Internal work allocation, external work contracts and every other activity will require extension of governance and control outside of physical offices.

What's next

In times of stress, protecting assets and interests is vital and companies will certainly seek measures to limit intentional wastage and abuse, internal or external. Containment measures will likely involve interventions such as the following:

Focused investments in enhanced early warning systems (EWS)

Aspects such as sentiment analysis, social media monitoring and behavioural surveillance will become an integral part of EWS to identify fraud and misconduct.

Periodic threat assessments

Companies would conduct more frequent and detailed threat assessments. There has always been a debate on balancing legitimate electronic surveillance (often deemed intrusive) with threats, and the current scenario will once again bring this to the fore. Companies will need to introspect long and hard to balance the need for individual privacy with confidentiality and protection of business interests.

Proactive claims evaluation

While there will likely be a surge in informal mediations in the short term, economics and commerciality of disagreements, disputes, litigation and arbitration will drive legal strategies in the medium and long term. Companies will probably take a long and practical look at the costs/benefits of both making and disputing claims before making financial commitments to their resolution process.

Productivity forensics

Companies will invest in fraud control measures related to the productivity of the remote workforce or off-site service providers who in turn have a remote workforce. This will have a significant bearing on the examination of elements of costs that can be contained, protection against wastage and abuse internally as well as renegotiation of commercial terms with third-party service providers or vendors. We expect companies to seek out new ways of assessing relevant efforts for tasks/projects and thereby optimise their operations and payouts (both internally and externally). To this end, productivity forensics is the need of the hour.

Data privacy and security evaluation

Owing to the shift to remote working, organisations would have to re-evaluate their policies, protocols and controls around data privacy and security. This especially applies to new technologies or techniques adopted to address the remote working scenario.

04 Protect against accentuated insider threats

Outlook

History has proven time and again that 'the enemy within' can be extremely damaging at crucial times and when the battle lines are drawn outside. Fraud that is aided, abetted or perpetrated by employees, at a time when business is recovering from a significant unplanned event, can cause irreparable financial and reputational damage, besides contributing to a greater crisis in already troubled times. These risks may manifest in the following forms:

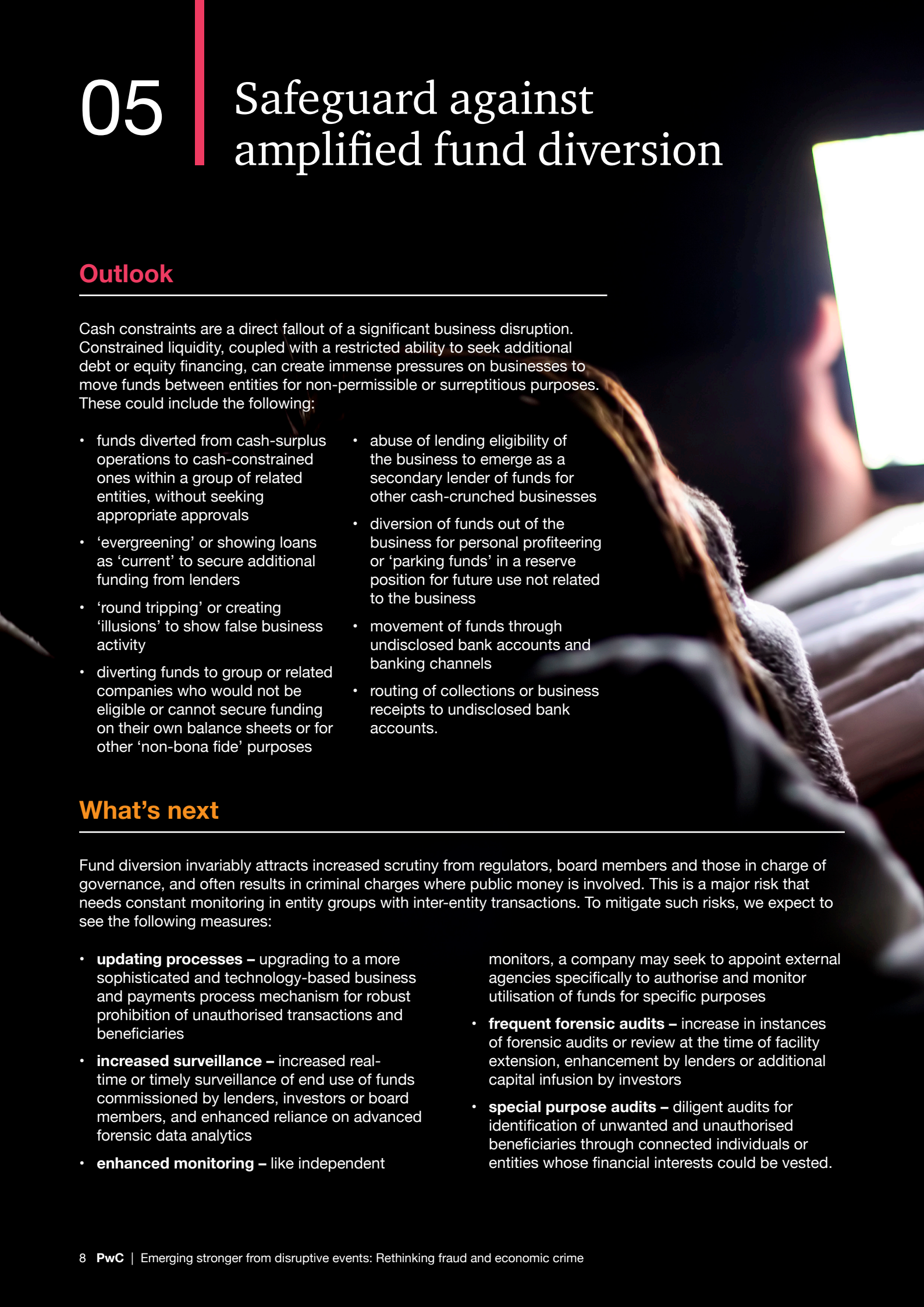
- Insiders are the first to notice vulnerabilities in systems or chinks in the armour. Extraneous circumstances (such as an uncertain future, dissatisfaction) can drive them to take advantage of these vulnerabilities.
- Misadventures are harder to detect if organisations are not specifically looking for them. Focused efforts of business leaders at times of crisis are often directed towards resurrection or damage containment, while fraud detection may not be a top priority.
- A dispersed remote workforce can pose unique challenges through 'virtual' interactions. There is a need to document decisions even more and create audit trails of how these are arrived at.
- Policy, privacy and confidentiality violations become harder to detect as the definition of a workplace greatly expands and blends into the personal physical space of employees.
- Code of conduct issues such as harassment, bullying and verbal abuse would require constant attention. Diminished physical workplace boundaries and human interaction in an unsupervised digital space require a thorough policy refresh and education of employees around adverse behaviour.

What's next

To counter evolving insider threats, companies will need to rapidly accelerate their preparedness and response. This will require companies to invest time and effort in the following aspects:

- Using advanced forensic analytics effectively to predict adverse employee behaviour and conduct in the digital space. Companies will have to complement existing measures on surveillance to identify rogue employees proactively (e.g. automated expense reviews, proactive forensic payment reviews, new vendor onboarding controls).
- Companies will have to adapt their code of conduct and policy guidance to specifically address issues emerging from the changed environment of employee interactions. For example, issues around cyber harassment, sexual harassment, bullying and inappropriate conduct will need to be identified and reaffirmed to employees as well as business partners, as applicable.
- There will also be a need to reassess domains where information related to potential adverse conduct is likely to reside. For example, companies may have to rethink policies regarding archival of chats, meeting recordings and logs to support investigative efforts that may be needed in the future.
- Similarly, companies may need to constitute, build and keep ready on-call rapid investigation teams as well as redefine investigation protocols to deal with evidence collection or preservation in case of actual perpetration.
- Deployment or upgrade to real-time monitoring mechanisms for timely detection of diversion and misuse of company funds will also be important.
- Organisations would also need to change their training material around data privacy, security, harassment and bullying to suit remote working scenarios. Employees need to be reminded of the consequences of misdeeds, whether in the physical or cyber world.

05 Safeguard against amplified fund diversion



Outlook

Cash constraints are a direct fallout of a significant business disruption. Constrained liquidity, coupled with a restricted ability to seek additional debt or equity financing, can create immense pressures on businesses to move funds between entities for non-permissible or surreptitious purposes. These could include the following:

- funds diverted from cash-surplus operations to cash-constrained ones within a group of related entities, without seeking appropriate approvals
- 'evergreening' or showing loans as 'current' to secure additional funding from lenders
- 'round tripping' or creating 'illusions' to show false business activity
- diverting funds to group or related companies who would not be eligible or cannot secure funding on their own balance sheets or for other 'non-bona fide' purposes
- abuse of lending eligibility of the business to emerge as a secondary lender of funds for other cash-crunched businesses
- diversion of funds out of the business for personal profiteering or 'parking funds' in a reserve position for future use not related to the business
- movement of funds through undisclosed bank accounts and banking channels
- routing of collections or business receipts to undisclosed bank accounts.

What's next

Fund diversion invariably attracts increased scrutiny from regulators, board members and those in charge of governance, and often results in criminal charges where public money is involved. This is a major risk that needs constant monitoring in entity groups with inter-entity transactions. To mitigate such risks, we expect to see the following measures:

- **updating processes –** upgrading to a more sophisticated and technology-based business and payments process mechanism for robust prohibition of unauthorised transactions and beneficiaries
- **increased surveillance –** increased real-time or timely surveillance of end use of funds commissioned by lenders, investors or board members, and enhanced reliance on advanced forensic data analytics
- **enhanced monitoring –** like independent monitors, a company may seek to appoint external agencies specifically to authorise and monitor utilisation of funds for specific purposes
- **frequent forensic audits –** increase in instances of forensic audits or review at the time of facility extension, enhancement by lenders or additional capital infusion by investors
- **special purpose audits –** diligent audits for identification of unwanted and unauthorised beneficiaries through connected individuals or entities whose financial interests could be vested.

06 Adapt to the paradigm of 'new whistles'

Outlook

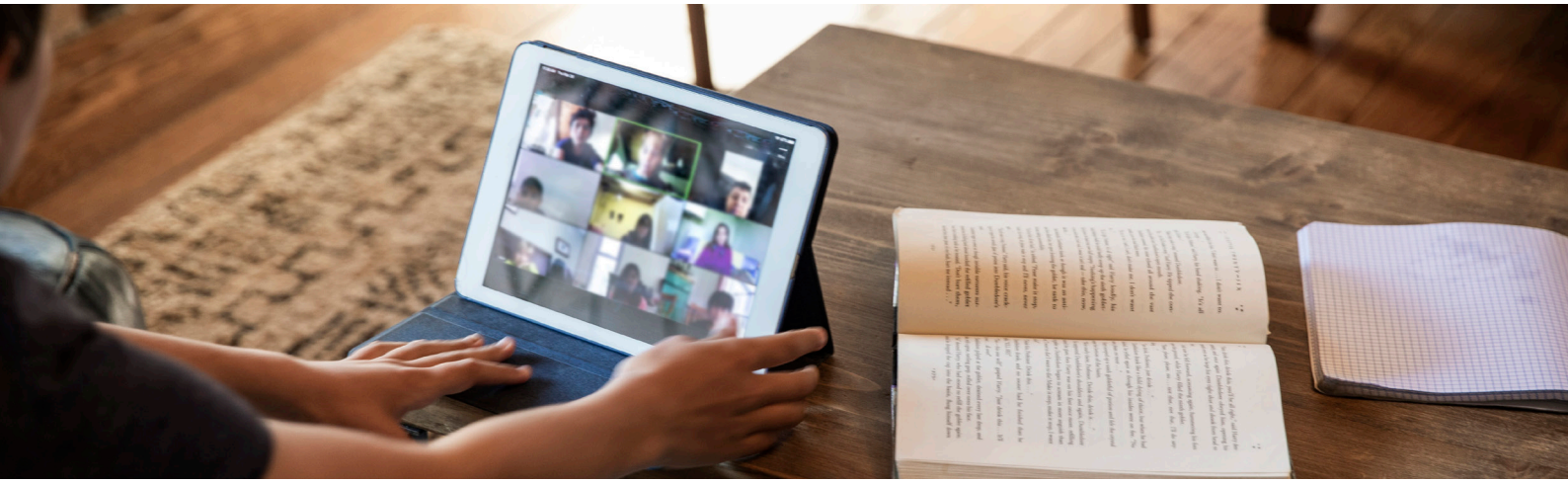
Hear no evil, see no evil, speak no evil. Traditional whistle-blowing has always worked contrary to this popular Japanese maxim of the three wise monkeys, and whistle-blowers are constantly encouraged to speak out when they see or hear something. Fast forward to today's business environment, where at least for the foreseeable future, human interactions would be limited, and discussions/meetings would be conducted in the relative privacy of people's homes or with limited participants. Whistle-blowing is set to change in this scenario, and it can be expected that:

- The number of 'generic' complaints could reduce as there are fewer opportunities for whistle-blowers to claim first-hand knowledge of incidents with little direct access to situations or data.
- The overall investigative quality of complaints in cases where a whistle is blown would be superior. Whistle-blowers would make extra efforts to collate information or background in order to make the complaint credible, or otherwise run the risk of the complaint not being admissible or investigated for want of background or context.
- In the short term, more code of conduct related whistles can be expected, specially from closer personal and 'unsupervised' interactions in a digitally connected work environment.
- Whistle-blowers may need more assurance on protection of their identity if they choose to remain anonymous.

What's next

Changes would be required to make whistle-blowing more effective and to add quality to the triage process of handling complaints when they come in. These would include measures such as:

- providing additional guidance on making complaints, including what constitutes reportable conduct in a changed working environment
- at the board level, having deeper discussions on matters reported and inquiring into complaints that do not get investigated further because of information insufficiency
- opening additional electronic channels for whistle-blowers to provide data without compromising their identity and providing them requisite assurance on this aspect.



07 Manage significantly increased counterparty risk

Outlook

In the face of disruptions at the global level, organisations need to reassess their supply chains and realign business relationships with dependencies on counterparties (such as suppliers, logistics and warehouse operators, distributors and resellers). Such business changes in counterparty engagement (existing or new changes brought on board in an expeditious manner) increase the exposure to a spectrum of risks, ranging from financial to legal, regulatory, compliance, reputational, and health and safety.

Counterparty risk management will thus assume additional importance and will require assessment of risks for informed business decisions, so organisations would do well to ask the following questions:

- Are counterparties expected to continue to be operational? What kind of challenges are they facing that can impede business continuity on a prolonged basis?
- What are the dependencies that counterparties have in resuming business as usual?
  - Will they be able to manage financial liquidity during low/no-demand situations?
  - Are they located in containment zones?
  - How much do they depend on their vendors to fulfil contractual commitments?
  - What is their level of access to workers to continue operations or scale up in the immediate future?
- What is the estimated time required for them to return to business as usual?
  - Is there any change in the risk categorisation?
  - Considering the nature of business, does the counterparty expose the organisation to a higher health and safety risk?

What's next

Businesses will need to rely more on counterparties to stabilise operations, and their scale of dependence could grow in the short and medium term. A comprehensive and almost real-time assessment of counterparty risk will thus be a key part of assessing exposures and decision making on creation and implementation of future business continuity plans.

01	As a direct outcome of such assessments, organisations may need to identify alternatives and on-board additional counterparties to address contingencies in their supply chain. Such on-boarding may need to be done in truncated timelines and hence, diligence procedures may need to be customised in such situations.
02	When faced with financial or time constraints, the risk of choosing an inappropriate counterparty will be high and fallouts could be severe from a business or reputation perspective.
03	Companies will therefore invest more efforts in choosing the right partner and will likely adopt additional risk-based due diligence procedures for making informed decisions. This will include assessments around reputation, solvency and ability to deliver, besides newer aspects such as implementation of containment measures and compliance with intermediate or final guidelines on operating under pandemic regulations.

08 Prepare for deeper and intense regulatory probes

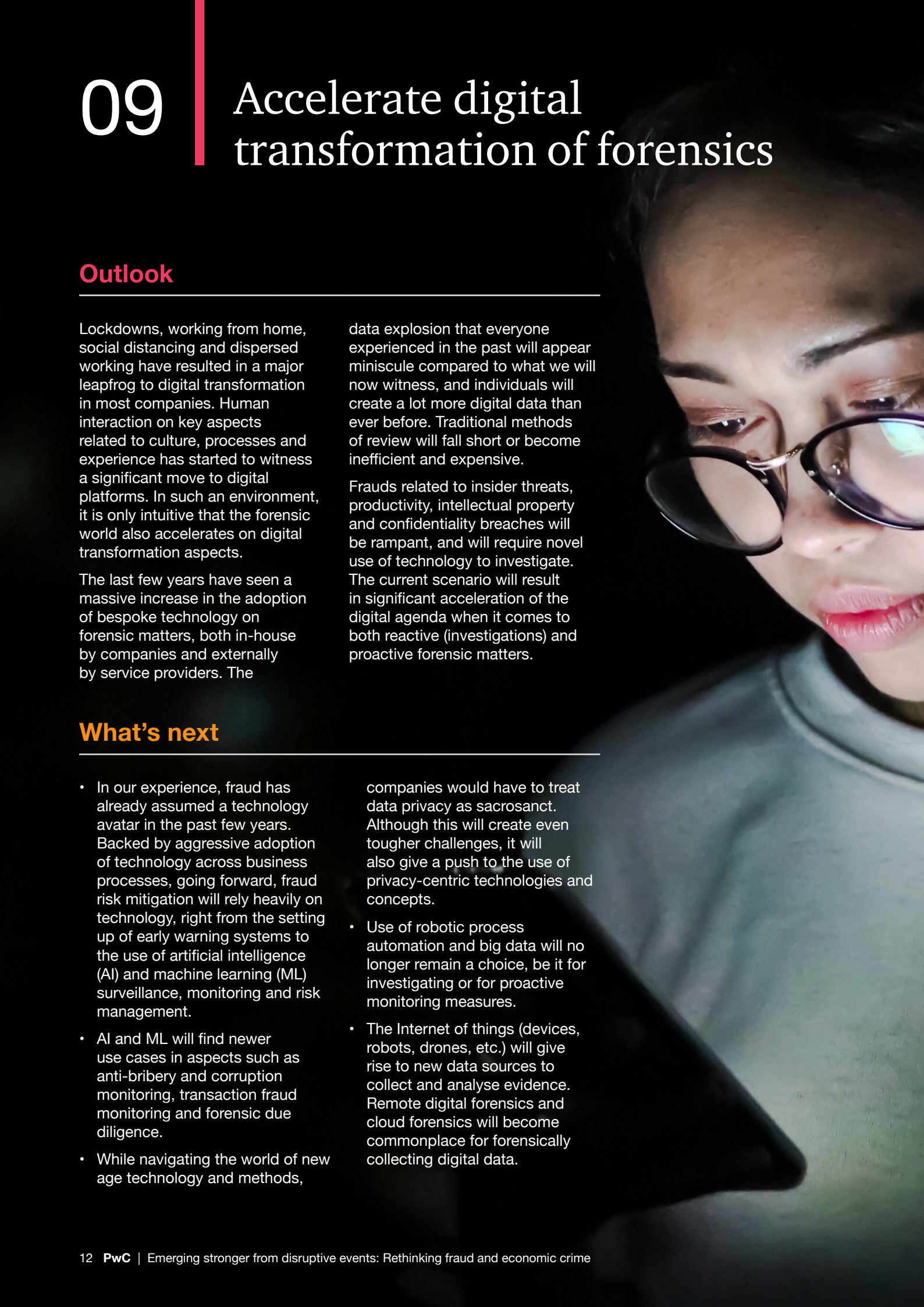
Outlook

In an era of disruption, there is a huge responsibility on governments to provide systemic economic interventions to protect and restart economies. At the same time, regulators also recognise the fact that public interest in companies needs to be protected and significant economic disruption is not used as an excuse to rationalise general or intentional corporate failures. Stress on business and liquidity will likely increase the possibility of companies stopping operations or being unable to continue business and/or reaching potential insolvency. It is highly likely that many of these matters will be subject to close regulatory scrutiny and investigation.

What's next

Regulators may direct companies to provide independent investigation reports or drive their own investigations into corporate failures, alleged misadventures and ethical shortfalls of people in charge of governance. It will also not be unreasonable to expect heightened cooperation between various regulatory agencies, both domestic and international (owing to travel restrictions), on matters related to enforcement or investigation of cases that get picked up for inquiry.

09 Accelerate digital transformation of forensics



Outlook

Lockdowns, working from home, social distancing and dispersed working have resulted in a major leapfrog to digital transformation in most companies. Human interaction on key aspects related to culture, processes and experience has started to witness a significant move to digital platforms. In such an environment, it is only intuitive that the forensic world also accelerates on digital transformation aspects.

The last few years have seen a massive increase in the adoption of bespoke technology on forensic matters, both in-house by companies and externally by service providers. The data explosion that everyone experienced in the past will appear miniscule compared to what we will now witness, and individuals will create a lot more digital data than ever before. Traditional methods of review will fall short or become inefficient and expensive.

Frauds related to insider threats, productivity, intellectual property and confidentiality breaches will be rampant, and will require novel use of technology to investigate. The current scenario will result in significant acceleration of the digital agenda when it comes to both reactive (investigations) and proactive forensic matters.

What's next

- In our experience, fraud has already assumed a technology avatar in the past few years. Backed by aggressive adoption of technology across business processes, going forward, fraud risk mitigation will rely heavily on technology, right from the setting up of early warning systems to the use of artificial intelligence (AI) and machine learning (ML) surveillance, monitoring and risk management.
- AI and ML will find newer use cases in aspects such as anti-bribery and corruption monitoring, transaction fraud monitoring and forensic due diligence.
- While navigating the world of new age technology and methods, companies would have to treat data privacy as sacrosanct. Although this will create even tougher challenges, it will also give a push to the use of privacy-centric technologies and concepts.
- Use of robotic process automation and big data will no longer remain a choice, be it for investigating or for proactive monitoring measures.
- The Internet of things (devices, robots, drones, etc.) will give rise to new data sources to collect and analyse evidence. Remote digital forensics and cloud forensics will become commonplace for forensically collecting digital data.

10 Renew commitment to crisis management

Outlook

PwC India's Crisis Survey report[1] revealed that crises do not discriminate – they affect organisations of all sizes and across all industries, and no organisation is immune to them. Moreover, the diversity of crises can keep companies guessing. The key differentiators, though, are the size, nature, spread and level of disruption caused by a crisis. Business leaders appreciate this new reality, as 97% of them expected to be hit by a crisis in the near future. Respondents were concerned that the number of crises due to fraud/ethical issues/corruption would be three times higher in the future. One-third of the respondents felt that cybercrime or operational disruptions or both could bring about the next major crisis.

By reverse engineering what was common among companies who emerged stronger from a crisis, we uncovered the secret sauce to turning a crisis into an opportunity – these companies did not leave crisis management to chance; rather, they had detailed crisis management frameworks that were tested and updated regularly.

1 | https://www.pwc.in/assets/pdfs/services/crisis-management/crisis-preparedness.pdf

What's next

Reflecting on learnings from a crisis, companies are likely to invest more time and effort in crisis planning and management frameworks and, in particular, consider the following steps:

- Formally identify and appoint a crisis leader and a dedicated crisis management team consisting of cross-functional heads.
- Create a documented crisis management plan that is easily accessible and available when needed in the future.
- Thoroughly test the plan through simulation and scenario building and update it regularly.

As crisis specialists, we know that the potential damage of a crisis, and whether or not you emerge stronger from it, is governed not so much by the nature of the crisis as by how well you handle it once it arrives. Consequently, the bedrock elements to successful crisis management will comprise the following:

- allocating a budget to crisis management before it hits
- having a plan and testing it
- adopting a fact-based approach and not neglecting key stakeholders
- performing a root-cause analysis and following up
- acting as a team and holding on to your values.

Conclusion

Emerging stronger from a crisis is imperative, and fraud and misconduct are not just passing issues. If not addressed, these threats can increase in uncertain times and cause additional damage to organisations whose attention is already divided among multiple and complex issues. On the other hand, organisations that make use of the opportunity to reinvent and rethink their fraud risks and containment measures by being nimble, adaptive and conscious of the changed environment can absorb the unknown better. This is a unique opportunity for them to add immediate practical experience of dealing with uncertainty, albeit in a forced manner, and realign their business to their changed or altered fraud risk profile.

A 'virus' has indeed crashed systems, and a reboot or reinstall may not work, especially with fraud, misconduct and economic crime! Emerging stronger from disruptive events thus requires an upgrade that not only protects the business of today but also helps build trust and confidence, thereby making organisations more resilient in the future.

Our team

Gaganpreet Singh Puri

Partner and Leader,
Forensic Services
PwC India
E: gagan.puri@pwc.com
M: +91 9818756955

Dhruv Chawla

Partner, Forensic Services
PwC India
E: dhruv.chawla@pwc.com
M: +91 8130166550

Rahul Lalit

Partner, Forensic Services
PwC India
E: rahul.lalit@pwc.com
M: +91 9811806905

Geetu Singh

Partner, Forensic Services
PwC India
E: geetu.singh@pwc.com
M: +91 9619390060

Gautam Dharamshi

Partner, Forensic Services
PwC India
E: gautam.dharamshi@pwc.com
M: +91 9845605434

Ruchi Sharma

Executive Director, Forensic Services
PwC India
E: ruchi.sharma@pwc.com
M: +91 9811604094

Puneet Garkhel

Partner, Forensic Services
PwC India
E: puneet.garkhel@pwc.com
M: +91 9820320181

Dhritimaan Shukla

Partner, Forensic Services
PwC India
E: dhritimaan.shukla@pwc.com
M: +91 9899038326

Darshan Patel

Partner, Forensic Services
PwC India
E: darshan.patel@pwc.com
M: +91 9920202999

Rahul Sogani

Partner, Forensic Services
PwC India
E: rahul.sogani@pwc.com
M: +91 9860091111

Vishal Narula

Executive Director, Forensic Services
PwC India
E: vishal.narula@pwc.com
M: +91 9769876426

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

pwc.in

AW/May 2020 - 6081