Deloitte.

It’s time to be proactive

Tackling fraud and economic crime

August 2023

MAKING AN IMPACT THAT MATTERS since 1845

Contents

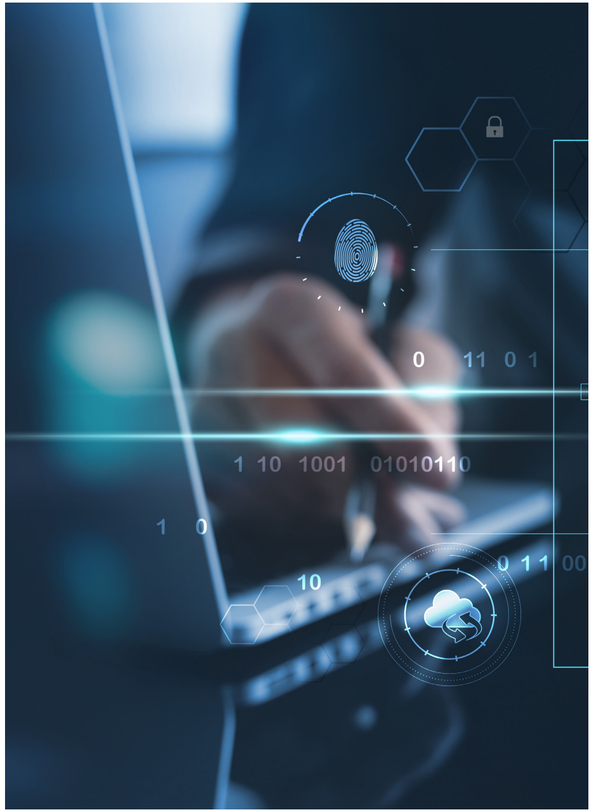
Introduction

Fraud and economic crime follows opportunity and attacks weakness.

The advancement in technology is one of several trends contributing to an uptick in fraud and economic crime. The pandemic and its aftereffects are also playing their part.

Coupled with regulatory developments, including greater focus on an organisation's anti-fraud measures, it has become increasingly important for organisations to be agile and prepared to mitigate fraud and economic crime risks.

By leveraging technology, organisations can mitigate emerging fraud and economic crime trends and significantly enhance their proactive anti-fraud measures, as detailed in this publication.



Emerging trends and heightened risks

The post-pandemic landscape, magnified by the rapid advancement of technology, has brought about a multitude of emerging fraud and economic crime trends and heightened risks. Fraudsters are continually finding new ways to exploit vulnerabilities and perpetrate fraudulent activities. Organisations need to be vigilant. We explore five emerging fraud and economic crime trends and heightened risks.

1. Headwinds in the global economy

The state of the global economy is uncertain, and the past has taught us that there is a correlation between economic downswings and fraudulent activities. Individuals and organisations may resort to dishonest practices to mitigate financial challenges or gain an unfair advantage by exploiting vulnerabilities during difficult times.

Financial statement fraud
In an economy of declining revenues, lower profitability and increased competition, organisations may be pressured to report positive financials at all costs.

Premature recognition of revenue, understating of expenses and asset misrepresentation are some common forms of financial statement fraud schemes. In mergers and acquisitions or initial public offerings, there may also be an incentive for organisations to intentionally manipulate financial statements to present a more favourable picture of their financial health.

Bribery and corruption
In an economic downturn, increased pressure may exist to secure contracts and generate revenue. Consequently, individuals within organisations may be inclined to resort to bribery and corruption to gain an unlawful advantage with respect to securing these opportunities.

Employee fraud
Recessions have historically led to cuts in employee remuneration and benefits, and a fear of job loss. Employees in financial distress may resort to fraudulent activities and rationalise their actions as a necessity to make ends meet. The opportunity to commit fraud can also be increased by the impact of layoffs that weaken an organisation's internal control environment due to redistribution of duties and diversion of focus away from internal controls to business continuity. Improper authorisation and lack of segregation of duties, resulting from a weaker internal control environment, may create opportunities for fraud.

Economic downturns can create an environment conducive to fraudulent activities and other misconduct. Organisations must remain vigilant by implementing preventive measures and promoting a strong culture of integrity.

It's time to be proactive: Tackling fraud and economic crime.

2. Fraud and misconduct being uncovered post-pandemic

The COVID-19 pandemic was a catalyst for reinventing work practices with new technologies and work arrangements. However, it also created an environment of heightened fraud risk, primarily resulting from distracted management, the shift to remote work and economic uncertainty. The result of this may have seen existing fraud controls and procedures compromised, or even entirely disregarded. Coupled with delays or cancellations of internal audits, fraudsters may have exploited these weaknesses and carried out fraudulent activities which are yet to be detected.

With the world reopen, management returning onsite and and internal audits and the like resuming, we are likely to see the fraudulent activities and misconduct that occurred during the pandemic bubble to the surface, which will need an appropriate investigation response. Management should also proactively consider what fraud and misconduct may have occurred when borders were closed, when they were offsite, or when their attention was diverted.

3. Advancement of technology and cybercrime

The advancement of technology is a double-edged sword. Whilst it has accelerated the digitisation of finance and the economy, it has also increased the methods available to fraudsters in perpetrating their crimes. Forbes projected in their 2023 Technology Council post that by 2025 the cost of global cybercrime will rise to an annual value of US$10.5 trillion.[1]

Phishing, Business Email Compromise (BEC), cyber extortion and deepfake are just some of the sophisticated methods used by fraudsters against victims. Here are some interesting, published facts:

In Southeast Asia, the number of phishing attacks in the first half of 2022 exceeded the total number of attacks in 2021 according to The Nation Thailand.[2] Phishing is a form of cybercrime that involves the use of deceptive emails or websites to trick individuals into providing sensitive and confidential information, such as passwords or financial details.

It is estimated that the global BEC market size will rise to US$3.3 billion by 2028 based on Business Wire.[3] This figure only continues to grow globally. In a BEC attack, the fraudster impersonates or hacks the email account of an entity or individual to request a wire transfer payment, often appearing to be for a legitimate invoice.

Ransomware is a significant threat in the ASEAN region. In the first three quarters of 2020, there were 2.7 billion ransomware attacks detected in ASEAN according to Interpol.[4] Cyber extortion attacks involve the threat to disable or compromise business operations unless a ransom is paid to the attackers.

Deepfake videos are growing rapidly, with an estimated compound annual growth rate of 42% through 2026, according to Bloomberg.[5] Deepfake attackers, using Artificial Intelligence, create realistic and accurate videos replicating the face, voice, and movement of people. Attackers can replicate trusted individuals such as employees and vendors. By doing so, it enables them to obtain confidential information.

The cost of cybercrime continues to grow globally, and methods are ever evolving. It is important for businesses to ensure that robust systems and procedures are in place to prevent and mitigate cybercrime – this includes conducting regular training to ensure all employees are aware of the threats.

1 https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=348e0153b0c4
2 https://www.nationthailand.com/business/tech/40020976
3 https://www.businesswire.com/news/home/20230110005759/en/Global-Business-Email-Compromise-BEC-Market-Report-2022-to-2028---Featuring-Broadcom-Fortinet-Cisco-Systems-and-Trend-Micro-Among-Others---ResearchAndMarkets.com
4 https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf
5 https://www.bloomberg.com/news/articles/2023-04-20/deepfake-detection-is-one-corner-of-ai-tech-that-isn-t-booming#xj4y7vzkg

4. ESG and greenwashing

Globally, corporate sustainability has become an essential aspect of operations, with internal and external stakeholders putting pressure on companies to adopt an Environmental, Social, and Governance (ESG) framework and report on the same. This in turn has given rise to the risk of greenwashing where organisations provide falsified information when making these ESG disclosures.

ESG policies, goals, and metrics are being demanded by investors and public entities for their review. Regulatory bodies around the world are establishing comprehensive ESG related disclosure requirements. The progressing regulatory requirements and increasing expectations from stakeholders on ESG matters may create pressure for organisations to appear well positioned to meet regulatory requirements and gain greater access to capital. As a result, organisations may be quick to set sustainability projects or key performance indicators (KPIs) that drive ESG-related initiatives without the necessary due diligence, supporting data and processes.

Carbon offsetting is one of the many ESG-related initiatives implemented by major organisations. It is a process through which organisations compensate for their greenhouse gas emissions by investing in projects that would counterbalance the emissions produced. However, it can be vulnerable to corruption when there is a lack of transparency.[6]

A recent investigation found that more than 90% of carbon offsetting projects by a leading carbon standard and certifier are mostly futile and could worsen global warming.[7]

The lack of uniform ESG reporting standards and metrics[8] makes it easier for organisations to be less transparent and misrepresent their ESG framework. Moreover, information and data on ESG matters may involve estimates, judgments, or forecasts which are subjective and can be manipulated or influenced by bias. The ambiguity of ESG reporting practices allows for subjective interpretation and selective disclosure, potentially enabling greenwashing practices to go unnoticed or unchallenged.

6 https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/esg-financial-crime-risk-screens/
7 https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe
8 https://blog-idceurope.com/the-need-for-harmonised-esg-reporting-for-financial-entities/

It's time to be proactive: Tackling fraud and economic crime.

5. Geopolitical tensions and sanctions

The speed, scope, and scale of sanctions changes may catch corporations off-guard. With heightened geopolitical tensions, sanctions are rapidly increasing in number and complexity, posing significant economic crime risks.

The complexity of sanctions regulations compounds the risk of non-compliance. Sanctions often involve intricate legal frameworks, with various entities, individuals, and activities subject to different restrictions. Understanding the nuances and intricacies of these regulations becomes even more challenging when changes occur rapidly. Individuals and organisations may inadvertently engage in activities that violate sanctions due to lack of awareness and understanding of the latest restrictions updates. Failure to navigate the complexities accurately can result in inadvertent violations and potential legal consequences.

The pace of change also affects the ability of companies to implement necessary compliance measures. Compliance programs require time to adapt and incorporate new requirements into existing processes and systems. Rapid changes may not allow businesses sufficient time to update their internal procedures, conduct necessary due diligence, or retrain employees, increasing the likelihood of non-compliance.

In the ever-evolving nature of sanctions, organisations should develop a proactive approach to monitor and adapt to developments.

Regulatory expectations

Along with the emerging trends and heightened risks, there is continued focus and increasing expectations by regulators as to the actions organisations should take to mitigate fraud and economic crime from occurring.

1. Anti-bribery and anti-corruption

In recent times, combating corruption and promoting integrity have become a key aim of many governments in Southeast Asia. For instance, the Malaysian Anti-Corruption Commission Act 2009 was amended to introduce a corporate liability provision for bribery and corruption under Section 17A, and Vietnam's ongoing anti-graft campaign has initiated criminal investigations against many individuals.

The United States (US) government continues its fight against bribery and corruption with its enforcement of the US Foreign Corrupt Practices Act of 1977. At the 20th International Anti-Corruption Conference held in December 2022, Assistant Attorney General Kenneth Polite emphasised that the fight against corruption locally and internationally is a top priority for the Biden Administration.[9]

The development and enforcement of anti-bribery and corruption legislation in developing nations reflect local recognition of a lower tolerance for bribery, corruption, and other misconduct.

Organisations need to align their practices and uphold high ethical standards to effectively combat bribery and corruption.

2. Failure to prevent fraud

In efforts to improve fraud prevention systems and protect victims, the United Kingdom (UK) government will introduce an offence that will hold organisations liable for failing to prevent or minimise fraud. This will prompt more companies to establish or enhance prevention procedures, leading to a shift in corporate culture in their fight against fraud.

Introduced as an amendment to the UK's Economic Crime and Corporate Transparency Bill, the "failure to prevent fraud" offence is expected to come into force by the end of 2024. Under the offence, large organisations incorporated in or with nexus to the UK will be liable if a specified fraud offence, intended to benefit the organisation, is committed by an employee or agent, and the organisation did not have in place reasonable procedures to prevent fraud. Similar to the UK Bribery Act 2010, this offence is likely to set a new global benchmark.

In Southeast Asia, Indonesia's New Criminal Code, set to take effect from January 2026, imposes criminal liability on corporations and parties within and/or outside the corporation if it fails to prevent and minimise fraud or crime offence that unlawfully benefits the organisation. This encompasses the failure to have in place necessary measures and comply with legal provisions to prevent fraud or crime offence.

These developments will raise the bar on expectations on an organisation's fraud prevention efforts.

9 https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-closing-remarks-20th-international

It's time to be proactive: Tackling fraud and economic crime.

3. Whistleblowing

Whistleblowing is crucial in the fight against fraud. This is highlighted by the Association of Certified Fraud Examiners (ACFE) in their 2022 Report to the Nations[10] where tips are identified as the number 1 way fraud is detected.

The importance of whistleblowing in identifying fraud and misconduct is also demonstrated by regulators. For example, the Singapore Exchange (SGX) Regulation mandated in 2021 that all SGX issuers should establish and maintain a whistleblowing policy. Malaysia's Whistleblowers Protection Act 2010 is an act to promote disclosure of improper conduct and provides protection to whistleblowers.[11] In the US, the Dodd-Frank Act provides incentives for whistleblowers.[12] The US Securities and Exchange Commission (SEC) awarded whistleblowers over US$1.3 billion in 2022 and 90% of such reports were made internally first.[13]

The increase in regulations, high profile cases, and corporate scandals has contributed to more public and media attention to whistleblowing.

Organisations are expected to foster a 'speak-up' culture through careful implementation of whistleblowing policies and procedures that promote ethical behaviour, protect against retaliation, and ensure comprehensive investigations.

10 https://legacy.acfe.com/report-to-the-nations/2022/
11 https://www.sprm.gov.my/index.php?page_id=75&articleid=464&language=en
12 https://www.sec.gov/spotlight/dodd-frank/whistleblower.shtml
13 https://www.sec.gov/files/2022_ow_ar.pdf

Proactive measures to consider

Fraud and economic crime are pervasive threats that can have devastating consequences for organisations. While an appropriate response is crucial when these threats manifest to mitigate financial and collateral loss, prevention is better than cure. Organisations must adopt a proactive stance and implement measures that go beyond being reactive by taking proactive measures to prevent, predict and detect fraud and economic crime.

1. Prevent

Reactive responses to fraud can be costly, involving investigations, legal proceedings, restitutions, and potential fines or penalties. Prioritising fraud prevention can minimise financial losses and reduce reputational damage due to fraud and misconduct.

Understand risk exposures

Understanding fraud and economic crime trends and risks is key for businesses to effectively manage and prevent the risks. Fraud can vary significantly across different organisations due to various factors, including the nature of business, organisational structure, and internal controls. Organisations can leverage fraud sensing surveys to gain insights into their risk profile and identify areas with vulnerability to fraud risk.

The nature of a business also significantly influences the vulnerability of fraudulent activities. The types of fraud and economic crime a business is susceptible to depends on key factors including its size and complexity, whether it is regulated; whether it is customer-facing or business-to-business; and whether it is listed or privately owned. Understanding the specific fraud risks associated with the nature of a business is essential for implementing targeted preventive measures.

Perform a fraud risk assessment

Conducting a successful and dynamic fraud risk assessment (FRA) is critical for organisations to mitigate the potential threats of fraud. This involves evaluating the vulnerabilities and weaknesses of an organisation's systems, processes, and controls that can be exploited by fraudsters. Thereby, assessing the likelihood and impact of fraud risks. Organisations with weak internal controls may be more susceptible to various forms of fraud.

It is important to establish a comprehensive understanding of the organisation's operations, processes, and systems to identify potential fraud risks. This can be achieved by conducting interviews with key personnel, reviewing relevant documentation, and analysing historical data. By conducting a comprehensive FRA, organisations can determine areas that require immediate attention and implement targeted measures to strengthen their defenses against fraud.

Be equipped and have awareness

By having extensive knowledge of internal controls and awareness of current trends and risks, employees can better identify potential red flags and take proactive measures to prevent fraud and economic crime. Regular and comprehensive training plays a vital role in equipping employees with the necessary knowledge and skills.

Organisations should establish training programs to educate employees at all levels on internal controls, fraud risks, and preventive measures. Regular workshops, or seminars should also be conducted to keep employees well-informed about the latest fraud trends. In addition, practical guidance should be provided to help employees identify warning signs, conduct thorough due diligence, and implement control measures.

2. Predict and detect

Predicting and detecting fraud serves as a line of defense against fraudulent activities. By identifying patterns, anomalies, and suspicious behaviours, organisations can anticipate potential misconduct and thus enabling proactive measures to be taken.

Prediction through data driven insights

Continuous monitoring of fraud and economic crime risks through analytics is one of the measures organisations should take to predict and detect fraud. These help in actively identifying new or evolving risk activities, control weaknesses, red flags, and other concerns for investigation. Organisations can leverage advanced analytics tools to identify potential fraud patterns and anomalies, allowing them to take proactive measures.

Through active assessments and monitoring, which can assist in predicting and detecting fraudulent activities, organisations can significantly reduce the likelihood of fraud and misconduct, financial losses, and reputational damage.

Early detection of suspicious activities

Establishing a culture of speaking up is essential to deterring fraud and misconduct and it requires ongoing effort. When channels for reporting ethical concerns are established and encouraged, employees are more likely to report any suspicions or concerns about potential misconduct.

It is important that whistleblowers have the option to maintain anonymity to reinforce a 'speak-up' culture. This encourages employees to report suspicions or concerns without the fear of retaliation. By cultivating an environment that supports and protects whistleblowers, organisations can receive timely information about potential fraud and misconduct, allowing them to swiftly investigate and address incidents, deter potential wrongdoers, and protect the organisation.

It's time to be proactive: Tackling fraud and economic crime.

Conclusion

The evolving landscape of fraud and economic crime presents significant challenges to organisations. The emergence of new risks and trends highlights the need for organisations to remain vigilant in protecting themselves. Additionally, the impact of regulatory developments emphasises the need for organisations to be proactive in mitigating their fraud and economic crime risks.

Being proactive will allow organisations to safeguard their operations, reputation, and stakeholders' interests. By understanding the risks, implementing appropriate controls, fostering awareness, and nurturing a culture of integrity and accountability, organisations can navigate the evolving landscape of fraud and economic crime with greater resilience and confidence.

How Deloitte can help: Protect, Monitor and Respond

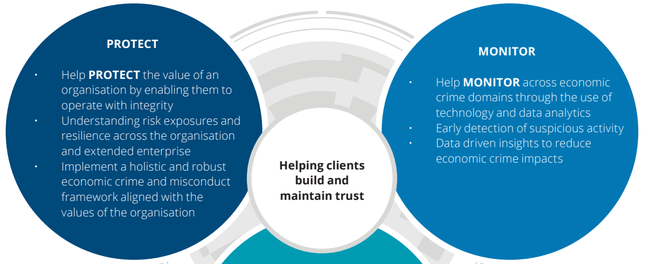
Deloitte Forensic offers advisory solutions that help clients prevent financial losses, reputational damage, and other negative impacts due to fraud and economic crime. We leverage analytics and our highly specialised forensic expertise along with investigative toolsets to transform data into valuable insights that can help clients solve complex issues and also effectively fortify their compliance and anti-fraud programs.

Fraud Sensing

- High level assessment to identify areas with vulnerability to financial fraud risk to give an overview of the risk profile of the Assessed Company
- Tailor made to present the risk, both existing and potential, based on scale of priority
- Industry agnostic

Risk Beacon

- Cloud-based solution that provides a smarter and more agile method of identifying and reporting our clients' compliance gaps and risk profiles
- Allows for the capture and consistent assessment of risks identified by the entity against the entity's own risk rating framework



Through this work, we help our clients...

- Protect wider society against negative impacts
- Prevent loss of value
- Protect reputation
- Avoid fines and penalties

Guard.ai

- A suite of integrated, proactive solutions designed to help mitigate the impact of unfavourable events
- A data driven methodology which utilises a combination of analytical approaches to identify risky compliance situations on an ongoing monitoring basis
- Identify and quantify known and unknown issues such as fraud, waste, corruption and abuse

Conduct Watch

- Digital whistleblowing solution to provide secure and accessible reporting channels for disclosure
- Facilitates case management and provides insight using analytics to enable independent disclosures from remote locations directly to you
- Trained analysts will review incidents, prepare reports and escalate high risk matters for further action

It's time to be proactive: Tackling fraud and economic crime.

Contacts

With an experienced multidisciplinary Forensic team of over 150 professionals located throughout Southeast Asia, we support our clients in solving tough problems and achieving deeper and more comprehensive insights.

Singapore

Jarrod Baker
Partner
jarbaker@deloitte.com

Andre Menezes
Partner
andmenezes@deloitte.com

Indonesia

Widiana Winawati
Partner
wwidiana@deloitte.com

Doddy Ashraf Zulma
Partner
dzulma@deloitte.com

Vietnam

Santosh Balan
Director
sbalan@deloitte.com

Thi Hong Hanh Do
Senior Manager
hanhdo@deloitte.com

Malaysia

Graham Dawes
Partner
gdawes@deloitte.com

Oo Yang Ping
Partner
yoo@deloitte.com

Thailand

Surasak Suthamcharu
Partner
ssuthamcharu@deloitte.com

Panyarat Chutiratmanee
Director
pchutiratmanee@deloitte.com

Philippines

Neal Ysart
Managing Director
nysart@deloitte.com

Deloitte.

About Deloitte Singapore

Designed by CoRe Creative Services. RITM1459104