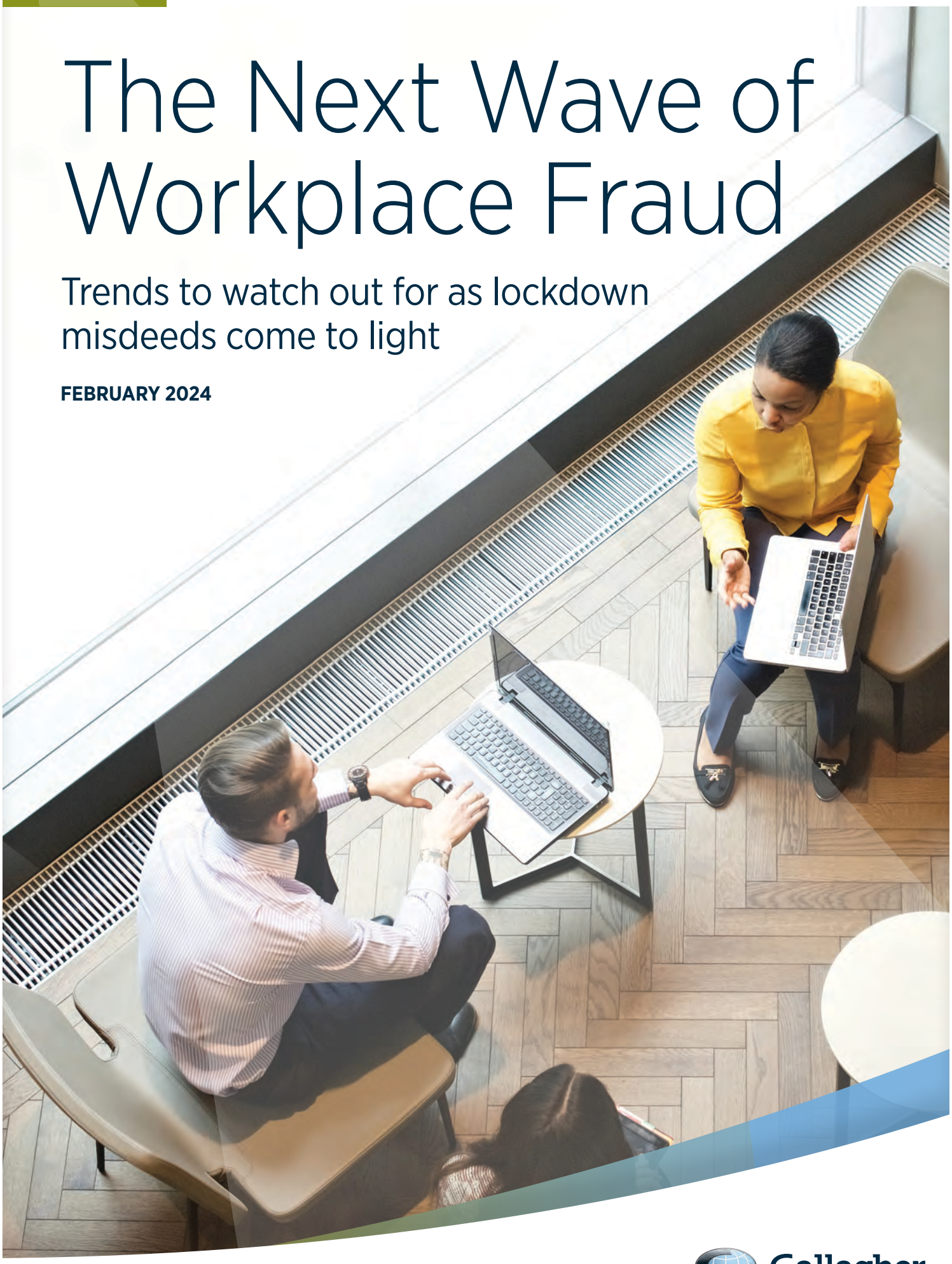
The Next Wave of Workplace Fraud

Trends to watch out for as lockdown misdeeds come to light

FEBRUARY 2024



Gallagher

Key findings

1. Corporate fraud is thought to erode 1.6% of equity value annually.[1]
2. There is typically a time lag between a fraudulent act being perpetrated and the crime being discovered, with the true impact of crimes committed in lockdown only now coming to light.
3. The onus is on companies to maintain strict anti-fraud controls. Supervisors are introducing new rules, requiring companies to do more to tackle crime in their midst.
4. Trends to watch out for include more sophisticated, AI-driven social engineering, ESG, and supply chain fraud.

The next wave of workplace fraud: Trends to watch out for

In HBO's award-winning series "Succession," Kendall Roy, the son of media tycoon Logan Roy, falsifies the company's financial records to hide his involvement in a car accident. The Department of Justice discovers the fraud and investigates Waystar Royco's misconduct. The fallout ultimately damages the company's reputation and exposes it to criminal charges.

The fictional storyline undoubtedly draws upon real-life scandals. Recent history offers up many examples of companies that have seen their reputation and stock value in tatters as a result of cover-ups and criminal wrongdoing. From rogue traders to high-profile reporting and accounting scandals in the early 2000s, and more recently, the alleged doctoring of Letters of Credit (LOC) by an insurtech firm.

When corporate fraud comes to light it is often surprising how long the misdeeds have gone unnoticed and unchallenged, particularly those perpetrated by more senior staff members. In 2020, a financial services company reached a $3 billion settlement with the US government over a fraud that had been taking place for a period of 14 years. During that time, insiders had been able to open millions of fake accounts in a bid to meet unrealistic sales targets.[2]

"The issue with crime is that there's often a lag of two to three years between someone perpetrating a scheme, and that loss being discovered," says Miranda DesPain, Senior Vice President at Gallagher. "Say someone creates a fictitious vendor in their system and they're funneling money out to their own bank account, it's often not uncovered until they get egregious with it."

"It might start small and then it gets bigger and bigger, and they get greedier and greedier. And then it's finally detected after 24 to 36 months because the sums start to become more noticeable. I've seen so many claims where it started off with a few thousand dollars here and there, and by the end we're talking hundreds of thousands or even millions of dollars a year that the fraudsters were taking from their companies each year."

"During the pandemic we saw a shift to remote working and now, on the back of a difficult economic environment, there may be fewer checks and balances in place. Some accounting and finance teams have been trimmed down. The insurers are certainly saying that they are starting to see the impact of the pandemic on crime claims trends now."[3]

According to one study published, corporate fraud erodes 1.6% of equity value annually,[4] and this is likely just the tip of the iceberg. The economic damage of insider fraud can be substantial and lasting, taking down global brands and destroying reputations and livelihoods.

Inside the mind of a fraudster

The nature of corporate fraud is complex, and perpetrators are good at covering their tracks. While the threat landscape is forever shifting, there are age-old reasons why disgruntled employees or greedy executives commit wrongdoing, sabotaging their organizations in the process.

Who commits a fraudulent act in an organization[7]

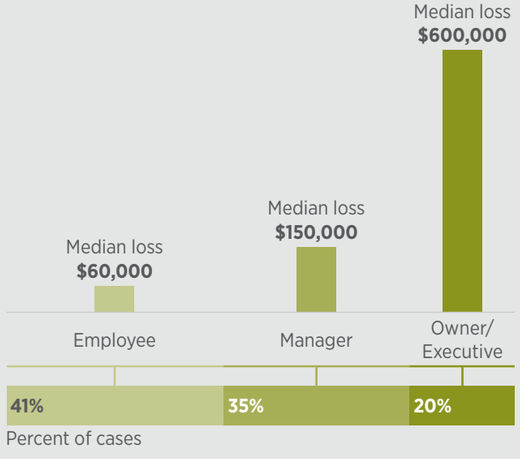
There can be a perception that white collar crime is a 'victimless crime'. Psychologically, this makes it easier for wrongdoers to justify taking kickbacks and telling lies. While greed is usually a key factor, other key drivers of corporate crime include excessive risk-taking behaviors, such as a desire to beat the system, and pressure from external bad actors.

Financial difficulties, competition in the market, the rising cost of living, or personal situations can create a sense of desperation. Individuals may resort to criminal activities because they believe it is the only way to solve their problems.

While less frequent, crimes committed by business owners and/or senior executives are significantly more damaging from an economic standpoint than those committed by middle managers and lower-ranking employees.

Level of authority

Most occupational frauds are commited by employee-level or manager-level personnel. But frauds by owners/executives are much more harmful.



Fraud triangle

The driving factors behind a fraudulent act

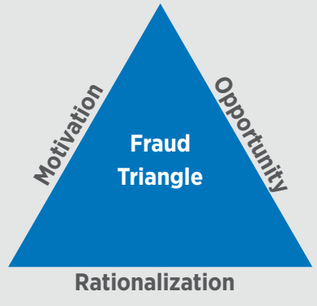
The fraud triangle is a concept used in forensic accounting and fraud investigation to explain the factors contributing to criminal behavior. The term was coined by criminologist and sociologist Donald Cressey and consists of three elements: motivation, opportunity, and rationalization.[8]

Motivation: Motivation plays a crucial role in driving individuals to commit fraud. To identify motivations, anti-fraud professionals often look for financial incentives. When organizations or employees feel pressure to meet financial targets or beat their competitors, they may engage in dishonest activities.

An economic crisis adds a further dimension. In the early 2000s, driven by their motivation to maintain high stock prices and secure personal financial gain, executives at Enron infamously manipulated financial statements to inflate profits and hide losses.[9]

Opportunity: Weak internal controls, lack of oversight, or holding a position of trust within an organization can make it easier for fraudsters to cheat the system and get away with it. A lack of robust oversight enables wrongdoing. This is a common theme in many high-profile frauds.

Rationalization: Fraudsters often convince themselves that their dishonest actions were necessary and justifiable.



Fraud cases rise, but still massively underreported

Insider fraud is more common than many might think.[5] Accounting abuses, egregious business practices, vendor favoritism, bribery, and corruption are just some of the wrongdoings that have come to light over the course of 2023, amid ongoing economic uncertainty.

Yet while corporate fraud cases are on the rise, the percentage of those reported has declined in recent years.[6]

Among the trends to watch out for in 2024 is the growing sophistication of AI-leveraged social engineering attacks, and rise in supply chain and ESG-related fraud. "We will see more social engineering and business email compromise-type losses over the coming year, and a downturn in the economy could give rise to more instances of staff embezzlement," notes DesPain. "Both insider and outsider fraud are on the uptick."

Meanwhile, regulatory pressures are growing. Supervisors are introducing new rules, with a greater onus on companies to tackle crime within their midst. There is more scrutiny of senior managers and an expectation they will take concrete steps to improve and uphold internal controls so that organizations can spot red flags and act before misdeeds become fully-blown scandals.

Fraud and the broader economy

There is a strong correlation between the incidence of corporate fraud and the relative health of the broader economy. During a downturn, when jobs are under threat and company finances under pressure, there is likely to be more motivation to commit financial crime. Executives may feel incentivized to hide investment losses from investors and shareholders, or accept bribes.

At the same time, studies suggest fraudulent behavior is more likely to come to light during more challenging economic periods. It is less easy to hide when balance sheets are stretched.

The Association of Certified Fraud Examiners conducted a study on the effects of the downturn during the 2008-2009 economic recession. It found the financial pressures caused by the Global Financial Crisis had resulted in an uptick in fraud.[10] Executives under pressure to meet financial targets may feel more motivated to participate in nefarious activities, or to turn a blind eye to bribery and corruption, for instance, if there is a perceived benefit in doing so.

"We are likely to see corporate fraud during tougher economic times," says Steve Bear, Head of Sales & Distribution — D&O, Gallagher. "Humans are complex, though, and the motivation isn't always financial and personal gain."

"People could be doing things just to elevate their sales figures in order to boost how they and their performance is perceived in the workplace. Or they could be concerned about the organization heading towards insolvency. The higher up you go in an organization, the more that sort of behavior becomes relevant."

"There's an immense amount of pride in many businesses and the directors or owners will sometimes do anything, including breaking a lot of rules, to avoid the company going to the wall," continues Bear. "That's where issues like insolvent trading come into play and where executives may be more likely to allow or even encourage employees to bend the rules if it artificially boosts the numbers and helps keep the company afloat."

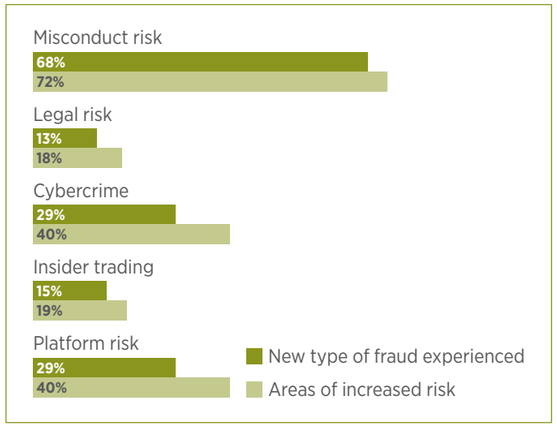
Rising cost of living

The cost-of-living crisis is an additional stressor. Even where salaries or employment status have not changed, inflation has left many individuals feeling the pinch over the past two years. The struggle to make ends meet in such an environment is a driver for some staff to steal from their employers or to accept bribes to better secure their financial circumstances.

According to PWC, 70% of businesses encountering fraud between 2020 and 2022 experienced new incidents as a result of disruption and financial uncertainty brought about by the pandemic.[11] Put simply, there was more opportunity during this period as controls were less rigorous. The shift to remote work reduced certain elements of oversight, and as the corporate world adjusted to new ways of working, it was — at least initially — easier for dishonest employees to hide.

In the UK, for instance, it is thought that around £4.5 billion of government fiscal stimulus money was lost to fraud and error through the coronavirus support schemes,[12] with up to a third of employers[13] accepting furlough funding they were not entitled to.

Types of fraud experienced during pandemic[14]



Regulators on the offensive

Regulators continue to flex their muscles in an effort to combat fraud and corruption, maintain market integrity, and improve standards of corporate governance. This includes making it more difficult for organizations to claim they had no knowledge of wrongdoing, especially where misdeeds benefited the company's bottom line.

With the latest Economic Crime and Corporate Transparency Bill, the UK government is strengthening its anti-money laundering powers, enabling better information sharing on suspected money laundering, fraud, and other economic crimes.[15] Meanwhile, the EU is preparing to strengthen and expand the anti-corruption laws of member states.

For its part, the US Department of Justice (DOJ) is stepping up into corporate criminal enforcement. Under a new adjustment, companies must disclose all non-privileged information about individual wrongdoing and will also consider all prior misconduct, not just misconduct like that in the current case.[16]

Failure to prevent fraud

One of the notable points of the UK bill is the "failure to prevent fraud" offense, which gives the Serious Fraud Office (SFO) the power to hold organizations to account if it is found they have profited from acts of fraud committed by their employees.[17] Under the offense, an organization will be held liable where criminal activity has been carried out for the organization's benefit, and where adequate fraud prevention procedures were not in place.

The law also expands the basis upon which companies may be held liable. Whereas once it had to be proven that offenses were committed by a "directing mind and will," the new framework expands this scope to include "senior managers" if they are acting within the scope of their authority.

"Turning a blind eye to the frauds will not benefit an organization," says Steve Bear. "Even a small fraud by an employee can lead to a disjointed chain of benefits. A fraudulent activity to boost sales figures, to get a bigger bonus, or improve the company's overall performance can result in the organization and its senior executives being held accountable for the fraud committed."

Across jurisdictions, supervisors are stepping up to improve fraud prevention practices and close loopholes that have historically allowed organizations and their directors to avoid prosecution. Proactive initiatives across borders could be instrumental in bringing awareness and driving a culture change towards improved fraud prevention procedures in organizations. Since the GFC, global regulators have been stepping up their cooperation to secure convictions.

Supply chain fraud

At times when corporate finances are being stretched, companies may be more likely to choose to work with questionable vendors or purchase substandard products to cut costs. This increases their risk and provides more opportunities for fraudsters to exploit supplier weaknesses.

Because of their complex and hyper-connected infrastructure, supply chain operations provide ample opportunities to the fraudsters. There are opportunities to manipulate records or disrupt operations throughout all stages of the supply chain, from the sourcing of raw materials to the processing of inventory returns. Hybrid fraud schemes, where employees collude with external parties, can be particularly difficult to detect.

In one example, a London-based distributor supplied thousands of counterfeit engine components with doctored documentation.[18] According to a PwC Global Economic Crime and Fraud Survey 2022 report, one in eight organizations experienced new incidents of supply chain fraud as a result of the disruption caused by the COVID-19 pandemic, and one in five sees supply chain fraud as an area of increased risk as a result of the pandemic.[19]

Supply chain fraud remains a threat in 2024. Many companies are relying on fragile supply chains that have not fully recovered from the disruption which reached its height during the pandemic. Meanwhile, modern supply chains are becoming more complex and challenging to monitor beyond the first and second tiers, particularly as supply chains are redrawn as a result of trends such as nearshoring and onshoring, adding a further layer of uncertainty.

ESG fraud

In situations where companies are under pressure to improve their ESG performance, employees may be motivated to resort to overstating the organization's credentials to create a positive impression around its sustainability or inclusion and diversity initiatives, for instance, even if these efforts don't fully meet the stated claims.

As there is currently no standard ESG assessment and reporting framework globally, it is harder to detect exaggerations or outright untruths. But ESG criteria are increasingly being factored into business and investment decisions, and as a result, false representation is a serious matter with legal, reputational, and potentially regulatory implications. If senior executives knowingly sign off on deceptive marketing strategies, it can also become a D&O issue.

ESG fraud is a classic example of corporate fraud where motivation, opportunity, and rationalization — the conditions of the fraud triangle — are all present. There is both pressure to meet expectations and the opportunity to commit fraud in the current ESG landscape. ESG is also a value proposition which is increasingly monetized by many organizations.

As awareness of ESG metrics and reporting is in a development stage in most countries, fraudsters are likely to continue to exploit this. "Like greenwashing, ESG frauds are happening more and more frequently where companies, for instance, promise to drive forward initiatives on diversity, sustainability, equity, and inclusion but are not able to back them up with concrete results, says Susan Friedman, Area Senior Vice President and General Counsel in Gallagher's Executive and Financial Risk Practice.

Digital tools enable more sophisticated scams

The explosion of generative AI over the past year has presented criminals and fraudsters with a new range of tools. While organizations can also benefit by using large language models, machine learning, and other tools to better detect and prevent fraud, inevitably the criminals are already one step ahead.[20]

For instance, rogue employees can use generative AI to create synthetic data, including fake customer accounts or fraudulent transactions, while automating such processes. And they can manipulate data to camouflage irregular financial transactions or create fraudulent documents to carry forward their motives.

As we have seen within the cyber threat arena, social engineering attacks are becoming more and more sophisticated. This year will undoubtedly see a surge in 'deep fake' attacks. This is where videos or audio recordings are used to impersonate executives, either to bypass biometric verifications and/or convince employees to make what they think are genuine payments authorized by individuals higher up in the organization (the classic 'CEO fraud').

The rise of more convincing modes of social engineering creates significant challenges for businesses. According to a recent survey conducted by identity verification firm Regula, 37% of organizations have already experienced deepfake voice fraud, with 29% falling victim to deepfake videos.[21]

Frauds that changed the world

Bernie Madoff

American financier Bernie Madoff orchestrated one of the largest and most infamous Ponzi schemes in history. Starting in the 1990s, Madoff promised high returns to investors through his investment advisory firm. However, instead of investing the money, he used new investors' funds to pay off earlier investors, creating the illusion of consistent returns. The scheme collapsed in 2008 when the financial crisis hit, and investors demanded their money back. In 2009, he was sentenced to 150 years in prison for securities fraud, investment advisor fraud, and other charges.[22]

Fake accounts scandal

A US bank faced a major scandal in 2016 when it was revealed that employees had engaged in fraud which involved the creation of millions of unauthorized bank and credit card accounts in order to meet aggressive sales targets. Staff opened the accounts without the consent of customers, ultimately leading to significant financial penalties and the resignation of top executives.[23]

Enron

Enron, an energy company once considered a major player in the industry, collapsed in 2001 due to a massive accounting fraud. Executives manipulated financial statements, hiding debt, and inflating profits, to deceive investors and maintain the illusion of success. The fraud involved complex schemes and off-balance-sheet entities. When the truth was revealed, Enron filed for bankruptcy, resulting in significant financial losses for investors and employees.[24] Several senior executives received jail sentences for their part in the corrupt dealings.

FTX

In one of the biggest financial frauds in US history, Sam Bankman-Fried, the founder of cryptocurrency exchange FTX scammed investors and siphoned money from FTX to hedge funds. In 2023, the Manhattan Federal Court convicted Bankman-Fried for duping customers and investors through wire fraud, conspiracy, and money laundering, with a maximum sentence of 110 years. FTX filed for bankruptcy protection in the US in November 2022.[25]

Fraud prevention: No cutting corners

During times of economic distress, some companies may be tempted to weaken or disregard their internal controls. They may also try to avoid certain checks in their operations. However, a lack of robust oversight creates opportunities for insider sabotage.

A critical aspect of risk management is having an effective internal control system and a system to prevent, detect, and investigate fraud. One of the simplest ways to reduce the risk of fraud is to carry out adequate background checks on new staff. Segregation of duties, consistent monitoring, and documentation are other essential components.

Technology is becoming a critical tool to prevent occupational fraud by providing advanced solutions to detect and mitigate suspicious activities. Advanced analytics and generative AI technologies can analyze large volumes of data to identify patterns, anomalies, and potential fraud indicators.

Companies can make use of dedicated fraud detection software to monitor transactions, financial records, and other data sources. Meanwhile, monitoring tools can track employee activities, such as computer usage, internet browsing, or email communications, to identify suspicious behavior or policy violations.

There is a lot that employers can do to remove the opportunity to commit fraud. Principles such as 'least privilege' restrict access to sensitive parts of the business and removes temptation. Meanwhile, biometric authentication technologies, such as fingerprint or facial recognition, can enhance security and prevent identity theft or unauthorized access. However, companies must set adequate policies and guidelines before collecting and storing such data.

In addition to using this technology, organizations need to conduct employee awareness sessions and build a culture of integrity within the organization. Training staff on whistleblowing procedures and telling them what red flags to watch out for makes it more likely that concerns will be raised in a timely fashion.

"The callback verification to avoid social engineering is still one of the best risk mitigation tools," says Miranda DesPain. "It may not always work, but the fact you attempted it often will afford you coverage under a policy."

"For employee theft overall, vendor management is absolutely critical," she continues. "It's not enough to say that you have policies and procedures in place, you need to make sure they are followed and that people and trained and required to execute those transactions following that protocol."

New and emerging regulatory initiatives will further compel companies to strengthen corporate governance. Building a positive culture that encourages employees and executives to stay on the right path and alert to suspicious activity will remain imperative over the next 12 months as the threat landscape — driven by cybercrime, market liquidity, geopolitical unrest, and technology among other factors — continues to evolve.

Even the most sophisticated fraud prevention frameworks can be exploited. Employers should ensure they tackle all three elements of the fraud triangle — motivation, opportunity, and rationalization — to ensure the proper controls are in place. Continuous focus on policies, training, and a holistic effort across departments can give companies an upper hand in the fight against fraud.

While corporate fraud cases are on the rise, the percentage of those reported has declined in recent years.

There is an expectation on senior managers to improve and uphold internal controls so the company can spot red flags and act before misdeeds become fully blown scandals.

Citations

1 Dyck, I. J. Alexander et al. "How Pervasive Is Corporate Fraud?," SSRN, 2 Oct. 2023.
2 Egan, Matt. "US Government Fines Wells Fargo $3 Billion For Its 'Staggering' Fake-Accounts Scandal," CNN. 24 Feb. 2020.
3 DesPain, Miranda. "Market Conditions 2023: Crime Insurance," Gallagher, Jan. 2023.
4 Dyck, I. J. Alexander et al. "How Pervasive Is Corporate Fraud?," SSRN, 2 Oct. 2023.
5 Dyck, I. J. Alexander et al. "How pervasive is corporate fraud?," Springer Link, 5 Jan. 2023.
6 Tsipursky, Gleb. "The Hidden Epidemic of Corporate Fraud," Forbes. 11 Apr. 2023.
7 "Occupational Fraud 2022. A Report to the Nations," ACFE, 2022.
8 "The Fraud Triangle," NWC.
9 Hayes, Adam. "What Was Enron? What Happened and Who Was Responsible," Investopedia, 28 Mar. 2023.
10 "Impact of Recession on Fraud," ACFE, 2009.
11 "PwC's Global Economic Crime and Fraud Survey 2022," PwC, 2022.
12 "Delivery of Employment Support Schemes in Response to the Covid-19 Pandemic," National Audit Office, 13 Oct. 2023.
13 "A Third of Employers Complicit in Furlough Fraud," Crossland.
14 "PwC's Global Economic Crime and Fraud Survey 2022," PwC, 2022.
15 "Factsheet: Economic Crime and Corporate Transparency Bill Overarching," Gov.UK, 26 Oct. 2023.
16 Meister, David and Lelogeais, Isabelle. "DOJ Steps Up Corporate Criminal Enforcement, Looks More Broadly at Past Misconduct," Skadden. 19 Jan, 2022.
17 "Factsheet: Failure To Prevent Fraud Offence," Gov.UK, 26 Oct. 2023.
18 Johnsson, Julie et al. "Fake Spare Parts Were Supplied to Fix Top-Selling Jet Engine," Bloomberg, 31 Aug. 2023 .
19 "PwC's Global Economic Crime and Fraud Survey 2022," PwC, 2022.
20 "AI: Keeping Pace With the Cybercriminals," Gallagher, Nov. 2023.
21 "Regula Survey: a Third of Businesses Hit by Deepfake Fraud," Regula, 1 May 2023.
22 Hayes, Adam. "Bernie Madoff: Who He Was, How His Ponzi Scheme Worked," Investopedia, 31 Oct. 2023.
23 Wilowski, Mack."Timeline: Wells Fargo's Biggest Legal Settlements," Investopedia, 16 May 2023.
24 Hayes, Adam. "What Was Enron? What Happened and Who Was Responsible," Investopedia, 28 Mar. 2023.
25 Cohen, Luc and Godoy, Jody. "Sam Bankman-Fried Convicted of Multi-Billion-Dollar FTX fraud," Reuters, 3 Nov. 2023.
26 "Principle of Least Privilege," CyberArk.

Spotlight

Gallagher

Welcome to Spotlight — presenting insights, shifting perspectives, and reframing evolving global trends.

Presenting the issues, opportunities, and risks that are transforming the way we do business, from industry hot topics and emerging growth markets through to perspectives on the big questions shaping our world today, this article provides actionable insights and analysis to inform strategic decision-making and power onward growth plans.

The Spotlight content series is designed for company executives, risk managers, industry operators, and business owners looking to reframe pressing issues, shape strategy, and pursue their future ambitions with confidence.

AJG.com/insights

AJG.com **The Gallagher Way.** Since 1927.