Managing fraud in our current environment

Discussion on fraud trends, response strategies, and results from KPMG's 2022 Fraud Outlook Survey

March 23, 2023

Your facilitator

Pete Bradford
Managing Director Advisory
Forensic Services
pbradford@kpmg.com

Session objectives

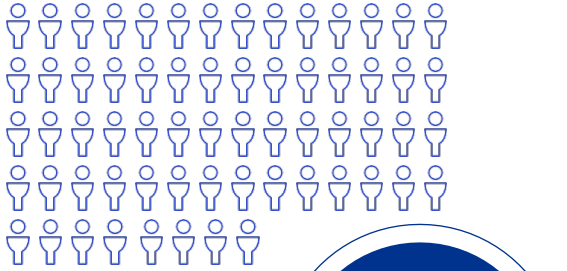
After completing this course, you should be able to:

- Describe the current threats organizations are facing and the future outlook of the fraud environment (as based on KPMG's 2022 Fraud Outlook Survey)
- Identify current fraud trends and potential response strategies to mitigate these trends
- Explain the impacts of Covid-19 on the fraud environment
- Identify red flags for financial statement fraud

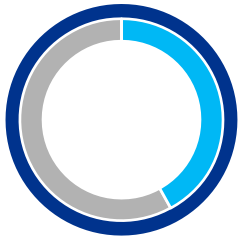
KPMG 2022 Fraud Outlook

About the research

This study is based on a survey of 642 executives:



642



58%
Latin America

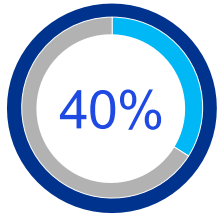
42%
North America

They are roughly evenly divided across seven industries:

- Industrial manufacturing
- Consumer products and retail
- Energy and natural resources
- Financial services
- Insurance
- Life sciences and pharmaceutical
- Telecoms, media and entertainment and technology

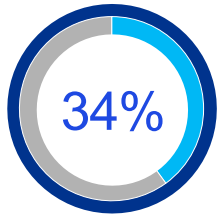
The sample is predominantly composed of senior leadership: **more than half of respondents are board members, members of the C-suite, or heads of departments.**

Their companies are a range of sizes:



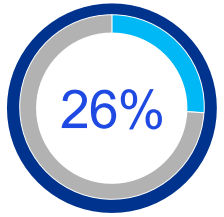
40%

have annual revenues of **less than US$1 billion**



34%

have annual revenues of between **US$1 billion and US$10 billion**



26%

have annual revenues of **more than US$10 billion**

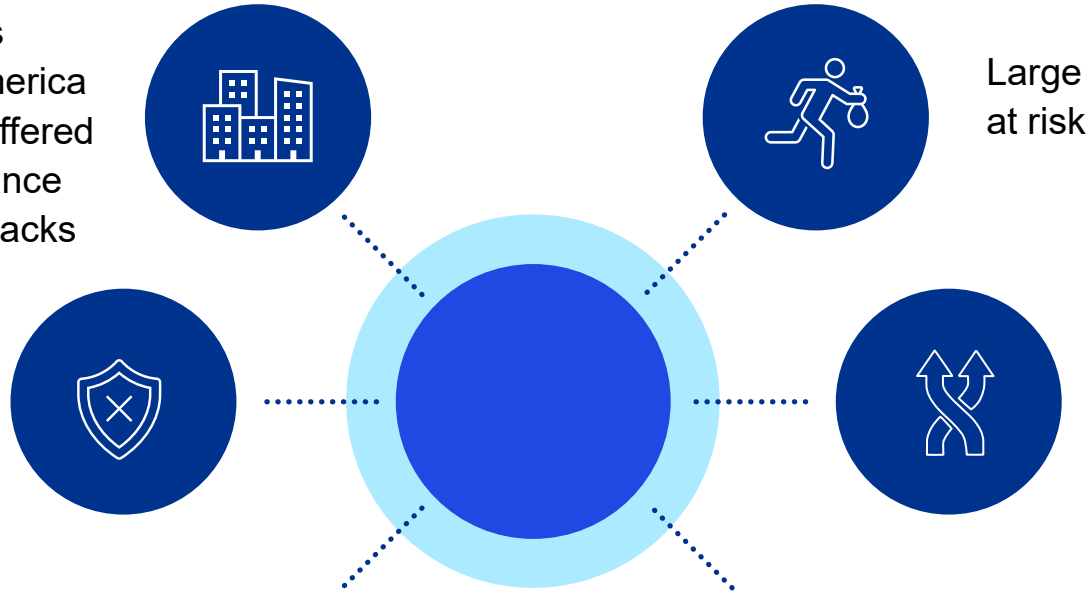
Executive summary

Our survey reveals that fraud, compliance concerns and cyber attacks are common, have increased in severity, and are expected to become more frequent.

The majority of companies across North and Latin America reported that they have suffered losses from fraud, compliance breaches, and/or cyber attacks

Large companies are more at risk of fraud

Not enough companies are completely on top of fraud controls, compliance and cyber security



Fraud threats differ between North and Latin America

Businesses expect fraud, compliance risk and cyber attacks to rise

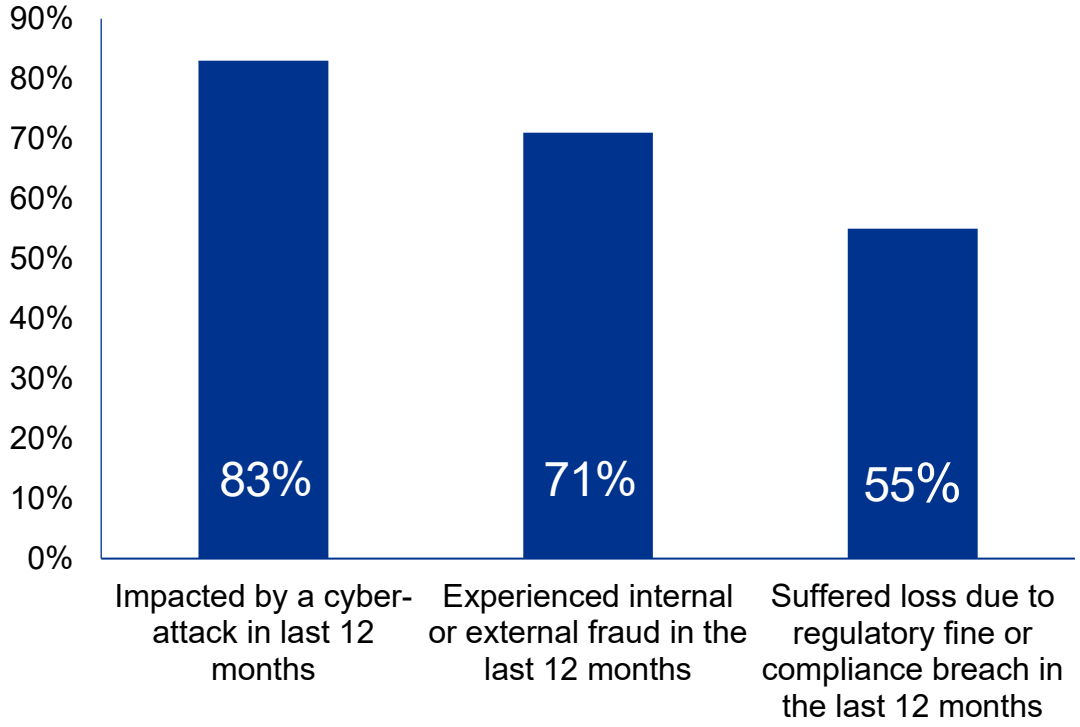
The COVID-19 pandemic has made things worse

Fraud, non-compliance and cyber breaches are the costly norm

Of the risks that we examined; respondents indicated that their companies are most likely to have experienced cyber attacks.

- 83% say that their companies have suffered at least one cyber attack over the past 12 months
- 71% of respondents report that their companies uncovered fraud over the past 12 months
- 55% of respondents acknowledge that their businesses have paid regulatory fines or suffered financially due to compliance violations in the past year

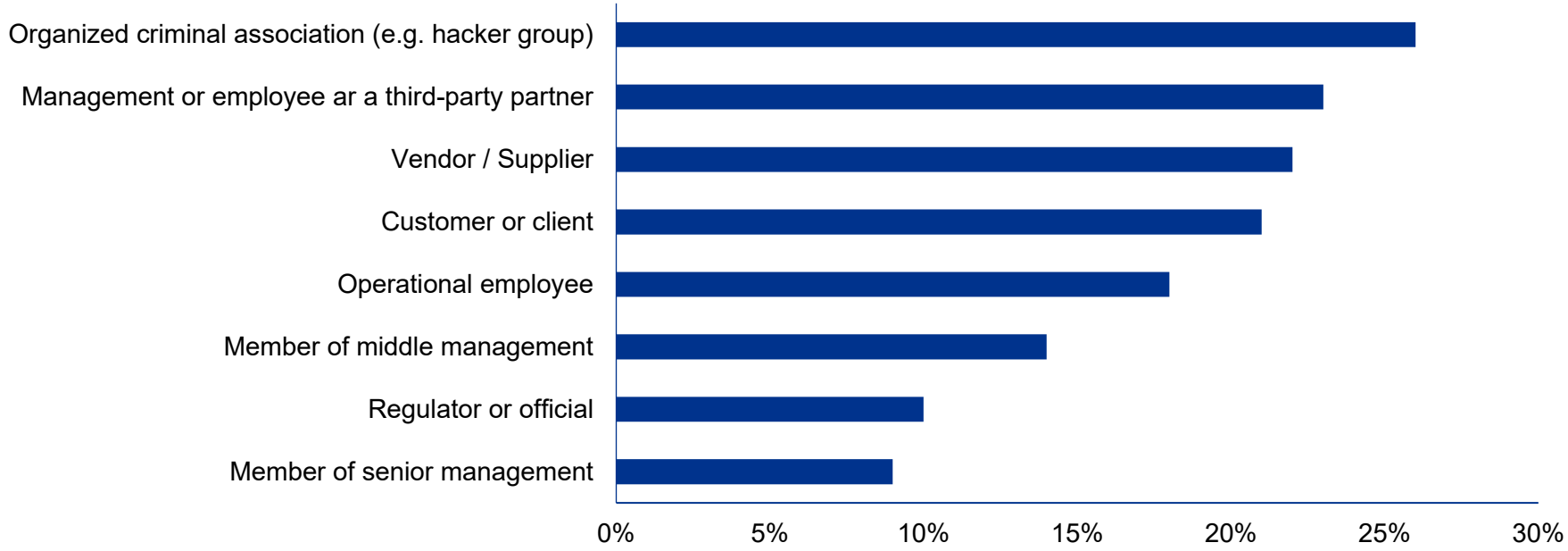
The reality of the triple threat



Respondents told us that, the average combined loss from fraud, compliance issues and regulatory fines was 1 percent of their profits.

Profile of the fraudster

Which of the following types of individuals are known to have been involved in fraud or misconduct (either alone it in collusion) at your company during the past 12 months?

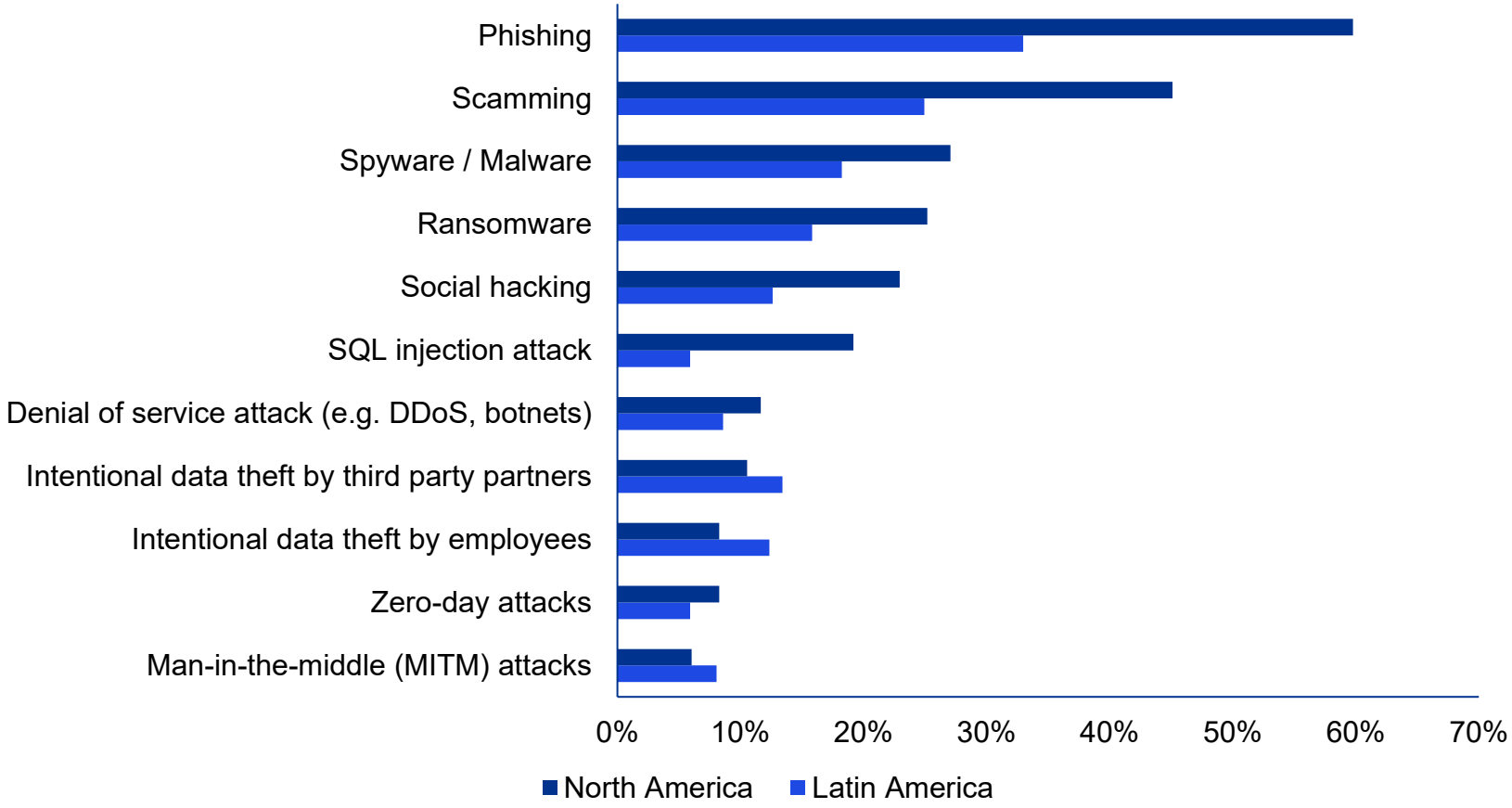


- Among North American respondents, 43% cite occurrences of fraud perpetrated by an outside criminal organization (such as a hacker group), compared to just 14% in Latin America – consistent with the higher levels of cyber crime in North America
- Conversely, 36% of Latin American respondents say that their companies experienced internal fraud, compared to just 23 % of North American respondents

Covid-19 and the impact on the risk environment

- Cyber crime increased in volume during the pandemic and has not abated
- As the chart shows, companies surveyed for this report are reporting rises in frequency of various kinds of attack
- Overall, **79 percent** of respondents saw growth in at least one of the types of attack covered in the survey
- **69 percent** of those surveyed say that remote work has been a major cyber security challenge for their businesses

Of which of the following have you seen an increase in the last year



Increasing focus on compliance

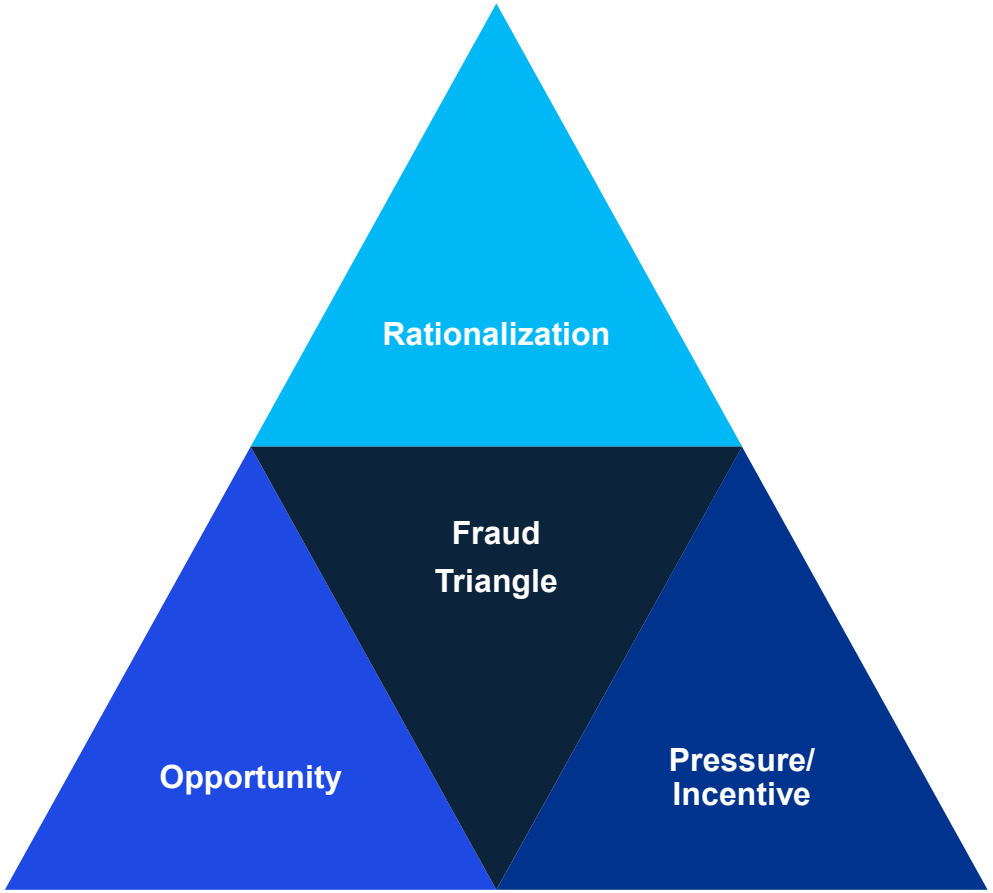
Over 70% of all respondents, and more than 80% working for large businesses, report that rigorous enforcement, increasing regulatory burdens and potential penalties increase the time and attention that their corporate leaders give to compliance issues

To what extent are the following increasing the time and attention that your company's leadership is paying to compliance issues? (Percentage answering substantially/greatly)

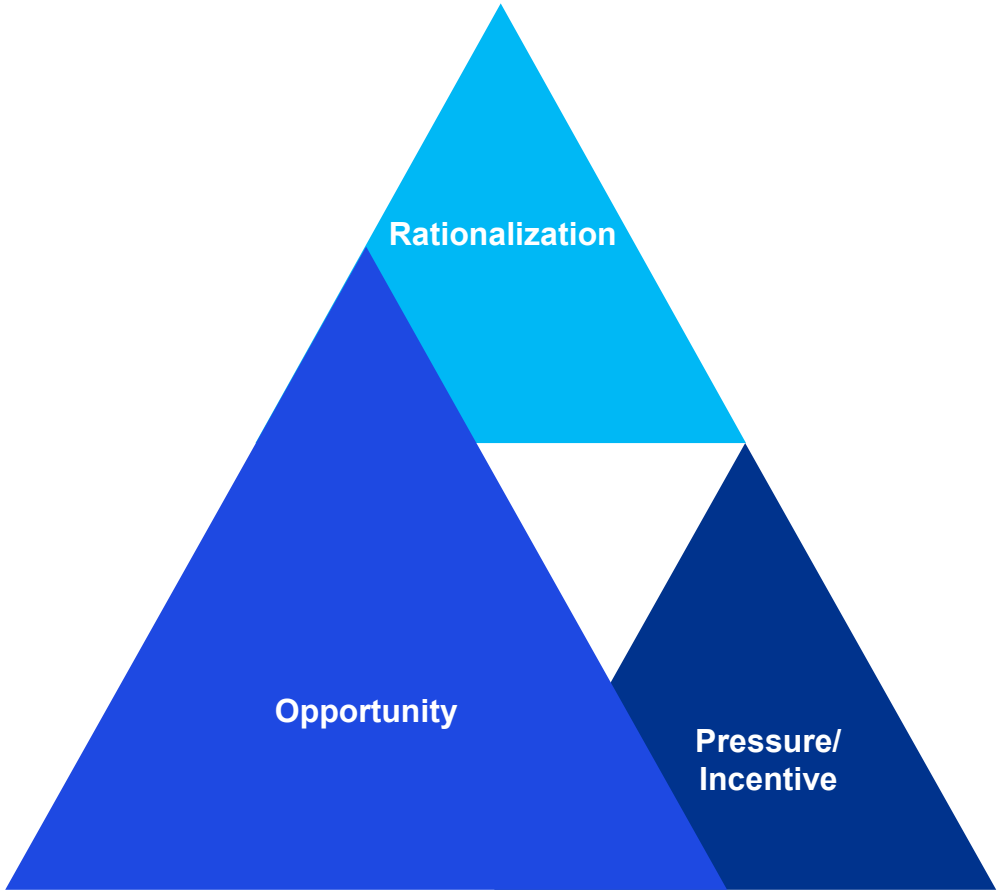
Impact of Covid-19

Covid-19 Impact to the fraud triangle

Pre-COVID 19 View

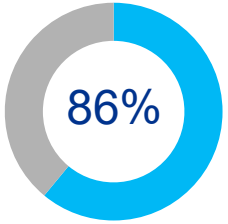


COVID 19 View

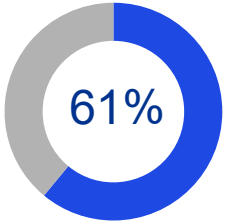


Impact of COVID-19

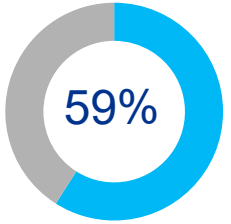
The COVID-19 pandemic and resulting lockdowns have complicated the threat environment.



Of Respondents say that working remotely has negatively affected at least one element of their company's fraud prevention, compliance, or cyber security programs



Of Respondents agree that the shift to remote working has increased the risk of fraud due to a reduced ability to monitor and control for fraudulent behavior



Of Respondents Agree the anti-fraud controls they had in place pre-pandemic have not been effectively updated to reflect the new working reality

01

Remote work has impeded management controls and supervisions. For example, many employees are millennials who share apartments with others not associated with the company, increasing challenges with ensuring that non-employees do not have access to company systems/data.

02

Amid supply chain problems, companies are more likely to circumvent existing controls (such as due diligence on third parties) to get access to materials as quickly as possible.

03

Cyber security increased in volume during the pandemic and has not abated. Companies are reporting rising frequencies in various attacks, with phishing (44%), scamming (33%), malware (22%), and ransomware (20%) growing challenges for many. Respondents tell us it takes about a month, on average, for a cyber attack to be fully contained.

Source: 2022 KPMG Fraud Outlook

Case Studies and Response Strategies

Case examples

1 Case

Allegation/Issue:

A controller used journal entries to move operating expenses onto the balance sheet (i.e., shifted expenses to pre-paid assets or long-lived assets) and deferred capitalization of construction in process assets.

How it was discovered:

- Identified by audit team doing year over year/quarter over quarter analytics
- Unsatisfactory evidence provided by company triggered an investigation

Lessons Learned/End Results:

- CFO, COO, and Controller were terminated
- Lack of appropriate oversight/review
- Financial statement manipulation is not always occurring at the C-Suite level
- This case also highlights that expense manipulation in order to achieve more favorable results has been more common than revenue manipulation in order to achieve more favorable results
- Depending on how the organization is performing, expense manipulation can also include recognizing expenses early when the organization is performing well or to incur the expenses prior to a public offering in order to have more favorable results once public

Case examples (continued)

2 Case

Allegation/Issue:

Management made public announcements about products, pre-orders, and contracts (not in line with the facts) to make them appear more attractive to investors.

How it was discovered:

The CEO was making statements in media appearances that were not true. A short seller report was released stating investors were being misled which triggered an SEC inquiry and investigation.

Lessons Learned/End Results:

- CEO and CFO were terminated
- Company was issued a subpoena and is being investigated by SEC. Chairman of the Board of Directors is currently under investigation as well
- Case highlights the concept that what is occurring should be consistent with what is being communicated. Audit team/people in general should recognize inconsistencies
- We have seen an uptick in subpoenas/information requests from regulators questioning management's non-financial communications to the street (i.e., pre-orders, where an entity is in the clinical trial phases (i.e., biopharma companies), and claims associated with what a product can do)
- We have also seen employees calling their own Company hotline as well as the KPMG hotline related to this topic

Case examples (continued)

3 Case

Allegation/Issue:

A financial services organization was spoofed via fraudulent email communication regarding bank account and wire transfer change requests, resulting in the release of fraudulent wire transfers.

How it was discovered:

Actual third-party who was supposed to receive a payment asked where the payment was, causing the company to realize it made a payment to a fraudulent account.

Sent MILLIONS out the door. Got back about half of the funds back. Entire process broke down. Just Did not follow their policies. The emails they sent weren't even that good. Address was off by a letter. Actual third party asked where payment was and they realized it wen tout to the wrong entity.

Lessons Learned/End Results:

- Company sent millions of dollars to a fraudulent account. Was able to recover about half of the funds
- Note: this scenario has been **occurring across all industries**
- This case highlights the importance of change management controls and processes organizations have in place when requests are made for changes to bank account information for customers/suppliers/vendors as well as employee payroll requests to direct deposit information. There should be dual authentication processes in place that includes a pre-established set list of phone numbers and individuals to conduct a live call back verification, rather than information provided in email requests

Case examples (continued)

4 Case

Allegation/Issue:

CEO was pressuring the Chief Actuary and other accounting personnel to manipulate earnings via:

- Lowering the Claims Reserves
- Inflating accruals to release at a latter date
- Expense manipulation

How it was discovered:

The Chief Actuary raised an allegation through the company's hotline and also communicated to the external auditors.

Lessons Learned/End Results:

- Management override: Management ignored what was being told to them by experts and insisted that the reserves be lowered to hit metrics
- The CEO was not terminated, but was instructed to "stay in his own lane".
- The Company improved the transparency and key inputs were properly vetted before booking the reserve.
- At the end of the day, the overall process had more transparency.

Case examples (continued)

5 Case

Allegation/Issue:

The CEO, COO, and Controller manipulated inputs into the annual impairment calculation so that the Company would not have an impairment.

How it was discovered:

Audit team kept asking for evidence that was not provided. Specialists provided input that statements company was making did not align with market expectations. An employee eventually provided audit team a report conflicting the information provided by Management.

Lessons Learned/End Results:

- Management integrity issues – those signing management representation letters were hiding information from auditors on purpose
- Highlights manipulation of goodwill/intangible impairment calculations in order to not trigger an impairment. Again, focusing on **vetting through third party evidence any inconsistent/contradictory information identified**

Case examples (continued)

6 Case

Allegation/Issue:

A Company had a short seller report issued against it noting that the CEO of the company was charging personal expenses to the company in an extravagant manner. After the short seller report was publicized, the SEC issued a subpoena to the company.

How it was discovered:

The Board of Directors engaged outside counsel and forensic accountants to assess whether the allegations had merit.

Lessons Learned/End Results:

- The Board learned that the CEO had engaged in perquisite abuse. This included personal use of the company jet, a condo in NYC, tickets to the World Cup finals.
- The CEO's wife and children used black car services for personal trips.
- $5 million in perquisites had to be disclosed.
- The CEO was removed, as well as a significant portion of the Board.
- The now former CEO had to pay fines to the SEC.
- The CFO retired after the 10K was issued.

Other considerations

DOJ Focal points

According to a February 18, 2022 article by Russ Banham titled The DOJ Targets Fraud: 5 Things to Know*, Mr. Banham outlines enhanced DOJ focal points in relation to an October 28, 2021 address by Lisa Monaco, Deputy Attorney General, to the American Bar Association's National Institute on White Collar Crime, where Ms. Monaco explained it is the DOJ's intent to actively prosecute criminal behavior, especially as "it relates to high-level corporate officers"

Mr. Banham's article outlined the following 5 focal points based on Ms. Monaco's address:

#	Focal Points
1	"To settle a case, companies will have to name all individuals involved"
2	"Prosecutors may by more aggressive"
3	"The DOJ is taking a firmer line on repeat company offenders"
4	"The DOJ will increase the use of independent monitors"
5	"The DOJ is still gearing up"

*Source: The DOJ Targets Fraud: 5 Things to Know (cfo.com)

Questions?

Contact

Contact

Pete Bradford
Managing Director Advisory
Forensic Services

pbradford@kpmg.com

312-665-1623

Thank you

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia