US perspectives on fraud and economic crime

The results of this year’s Global Economic Crime and Fraud Survey are dramatic. Reported economic crime—in the US and globally—reached the highest rate in the Survey’s 20-year history. The rich data and insights from 7,228 global organizations across 123 countries offer a snapshot of how the pervasive threat of fraud impacts a broad range of companies. The US shows a breakaway from global trends on several fronts including fraud rates, who the fraudsters are, and internal prevention methods.

Every organization, of every size, in every industry—no matter how vigilant—is vulnerable to blind spots. What actions can companies take today to pull fraud out of the shadows and better prepare, respond and emerge stronger?
How is economic crime impacting US companies?

Fraud is more public, more detectable and more visible than ever before—but are we seeing all of it?

For the first time in our Survey, more than half (53%) of US respondents reported being victims of economic crime in the previous 24 months—a 40% increase relative to 2016’s result. Globally, the reported rate of 49% was also a historic high for the Survey.

Yet these figures only reflect the fraud that has been identified. Economic crime professionals know that fraud hides in the shadows and it stands to reason that virtually all organizations are targets. This leads to a critical question: What about companies that did not discover incidents of fraud? Were they lucky enough to escape fraud—or do they just not know about it? Shining a light onto these potential blind spots and taking a proactive stance can advance opportunities for big improvements in your fraud-fighting efforts.

53% of US respondents reported being victims of economic crime in the previous 24 months

Record-high experiences of fraud

Has your organization experienced any fraud and/or economic crime within the last 24 months? Respondents that answered ‘yes’.

Industries showing the highest reported rates of fraud in the US:
- Manufacturing
- Energy, utilities and mining
- Entertainment & media
- Financial services

Source: PwC’s 2018 Global Economic Crime and Fraud Survey
Fraud is hitting the wallets—and within the walls—of organizations

The economic crimes reported by our US respondents were more financially impactful than ever, with over a third (37%) of respondents reporting losses from the most disruptive fraud greater than $1 million. These US figures also dwarfed the aggregate results: globally, only 18% reached that range, with most falling below the $1 million threshold.

With an eye on the scale of losses that can occur, it’s no surprise that in the past 24 months, 52% of US organizations increased or significantly increased the amount of funds used to combat fraud and 42% plan to do so in the next 24 months.

The jury of public opinion can’t be overruled

Damage from economic crime goes far beyond financial loss. Today, there’s amplified danger of damage to a company’s reputation. With public expectations of companies and their business partners at an all-time high, even a small matter can blow up into a large and consequential issue in the public eye.

The fallout doesn’t stop there. When a company’s reputation takes a hit, so do its people. Four in ten (43%) US respondents described employee morale as being damaged by the most serious fraud.

US organizations also cited that business relations (42%), reputation/brand strength (38%) and relations with regulators (37%) suffered significant impact from the crime.
What types of fraud are disrupting organizations?

Fraud types have diversified

Fraud is an ever-changing adversary—so we tweaked our definitions in this Survey to reflect as precisely as possible the latest forms of fraud. This year we introduced two new categories—fraud committed by the consumer and business misconduct—which immediately were ranked in third and fourth place among the 53% of respondents who reported fraud in the last two years. The high response in the business misconduct category may be partially correlated to a new awareness of the risks of corporate malfeasance, in light of high-profile corporate frauds that took place over the Survey period.

Interestingly, we know the word “cyber” tends to incite a strong reaction both inside and outside company walls. But from a fraud prevention point of view, our analysis found that the actual crime was not the intrusion—it’s what was taken, and how. It is critical that companies distinguish between the two. Case in point: 32% of US respondents reported that asset misappropriation was the theft facilitated via a cyber-attack, and 23% suffered intellectual property theft.

Bribery and corruption are not new—and corruption may be one of the biggest issues facing society today. Against this backdrop, it’s not surprising that the share of US respondents who said they were asked to pay a bribe more than quadrupled, from 7% to 31%. Similarly, the percentage of US organizations who believed they lost an opportunity to a competitor who paid a bribe more than tripled, from 8% to 29%. But our analysis into further company experiences showed that bribery and corruption detection methods are not keeping pace: only 37% of our US respondents said they performed a bribery and corruption risk assessment in the last 24 months; and just half had specific policies that address bribery and corruption.

What types of fraud have organizations experienced in the last 24 months?

<table>
<thead>
<tr>
<th>Type</th>
<th>US</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset misappropriation</td>
<td>48%</td>
<td>45%</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>31%</td>
<td>49%</td>
</tr>
<tr>
<td>Fraud committed by the consumer</td>
<td>28%</td>
<td>29%</td>
</tr>
<tr>
<td>Business conduct/misconduct</td>
<td>29%</td>
<td>28%</td>
</tr>
<tr>
<td>Bribery and corruption</td>
<td>16%</td>
<td>25%</td>
</tr>
</tbody>
</table>

Frauds committed by the consumer and business misconduct, making their first appearance in the survey in 2018, already reached the top of most commonly reported types of economic crime.

Source: PwC’s 2018 Global Economic Crime and Fraud Survey
Bribery and corruption continues to grow in frequency and intensity and the focus of the Department of Justice (DOJ) has not waned. Propelled by the new Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, the DOJ continues to focus on both self-disclosure and civil and criminal prosecution of individuals, as well as companies.

**Who is committing economic crime?**

The percentage of fraud committed by internal actors—especially senior management—is up sharply

The gap between internal (43%) and external perpetrators (48%) is shrinking among US respondents. Alarming, the share of internal fraudsters swelled from 29% in 2016 to 43% this year. In the US, the majority of internal perpetrators were involved with marketing and sales (21%), which could potentially be related to high-profile corporate crimes involving sales practices in the US—and may further reflect the need to tighten up internal ethics and compliance programs.

Another noteworthy fact: the share of internal fraud committed by senior management in the US doubled (18% to 36%) in only two years. Senior management became the most likely internal perpetrator of fraud in the US. Globally, they were the least likely.

Of course, these findings represent only those who were caught. Considering that senior managers are often in a position to override controls—and that controls often can’t prevent the possibility of C-Suite crime—there is a strong possibility that actual fraudulent activity was even higher than reported.

---

Adding to the risk posed by senior employees is the fact that the longer their tenure, and the more they are trusted, the more likely they are to be in a position to commit the fraud.

While there is some evidence\(^3\) that boards, institutional investors, governments and the media are holding CEOs to a higher level of accountability for ethical lapses than in the past, our Survey results suggest that, at least at the level of senior management, more scrutiny could help move the needle in preventing fraud.

Pay attention to those that you trust

Even external frauds are being perpetrated by the “devil that you know”. Collectively, third parties (vendors, agents/intermediaries and shared service providers) topped the list of external perpetrators. The customer was the most common individual external perpetrator. What will you do if the people and entities with whom you do business defraud you? Forewarned is forearmed: Survey results show that businesses should be vigilant about who is given access to their systems and processes.
Why does fraud happen?

The fraud triangle

For fraud to occur, there must be three elements in place—an incentive or pressure; an opportunity; and a rationalization. Fraud practitioners refer to these as the “fraud triangle”—and in examining these relative drivers of fraud in the US we found some notable divergences from the global results.

The opportunity to commit a fraud is cited as the most influential factor contributing to internal fraud as ranked by 48% of US and 59% of global respondents. The opportunity is usually addressed by internal controls, and 59% of US respondents said they made a high level of effort to use business processes to combat internal fraud. But the data still showed that there is room to improve detection methods—this despite a plethora of advanced tools available around data analytics and other rapidly maturing technologies.

When looking to incentive or pressure, 37% of US respondents cited this as the main driver of internal fraud—in contrast to the global response of 21%. This could reflect dissatisfaction with compensation structures or strong internal sales pressures.

Finally, rationalization—the feeling of being entitled to steal, and that doing so would be a “victimless crime”—is often a function of corporate culture. Twelve percent of US respondents reported this as the primary trigger of internal fraud, close to the 11% that said so globally. It’s also the hardest factor to control, because rationalization is fundamentally a psychological construct. Perhaps this is why promotion and verification of individual employee ethical decision-making was given too little attention. Only 38% of US respondents put a high level of effort towards this method, and 22% gave it low effort, or none at all.

So where are US executives putting efforts to combat fraud?

US awareness of fraud is up. The financial impact of fraud is up. Internal fraud is up. And yet, key fraud prevention measures such as whistleblowers, internal reviews, and external consultants were down—both compared to global and 2016 results.

Faced with growing fraud risks, many organizations pour more money into technology. Unfortunately, in the fight against fraud, especially internal fraud, technology investments can reach a point of diminishing returns—as well as offer a false sense of security. That’s because, as the fraud triangle illustrates, fraud is the product of a complex mix of conditions and motivations, only some of which can be tackled by machines.

Corporate culture can promote people-driven detection methods as beneficial—including whistleblower hotlines, fraud risk assessments, and periodic internal reviews; however, US companies reported spending less time and resources on these proven methods of prevention and detection. This is notable because on the world stage, these prevention methods were all up.

Whose problem is it, anyway?

With one spotlight on the changing global environment that organizations operate in, and another on the marked increase in internal fraud, it’s fair to ask…whose problem is it, anyway?

Among US respondents, primary responsibility for ethics and compliance programs resided with the Chief Compliance Officer and General Counsel (GC); in other countries the CEO was more likely than the GC to take on that role.
Still, most organizations are hamstrung by silos among internal departments such as ethics, compliance, legal and risk management—to the point where definitions of fraud may vary across functions, and fraud can more easily seep in through cracks. Eleven percent of US organizations still did not have—or didn’t know if they had—a formal business ethics and compliance program.

One thing is clear: The preponderance of internal crime—and of senior management as perpetrators of fraud—points to the need for boards to get more closely involved with the organization’s fraud prevention efforts.

The Board must take the pulse of the organization and ensure the audit committee gets the real-time information—including whistleblower alerts—it needs. Fundamentally, boards and the C-Suite are responsible for ensuring there is a credible, effective ethics and compliance program across the organization—and for monitoring it.
Summary

Shining a light on how companies manage the threat of economic crime—across the US and around the globe, spanning industries and sizes—can help chart a course for how you may improve your fraud-fighting efforts.

It is critical to have a clear understanding of what constitutes fraud and where its tentacles take hold to begin to unlock significant opportunities to fight it. Globally, we took a lens to how organizations can recognize fraud, take a dynamic approach, harness the protective power of technology, and invest in people. Then, we dug further into US experiences to see trends that breakaway from the global direction; and what that means to organizations today.

Leaders should examine current and expected business threats, prioritize opportunities and risks, and set an outlook for new strategies and practices to consider. Are you prepared to face fraud and economic crime and respond with a strong organization and robust processes? Are you positioned to emerge stronger?

Where do you start?

As you consider the current landscape of fraud and fraud prevention, here are some practical questions to ask:

- Have you conducted a company-wide fraud risk assessment to learn your unique risk landscape and to address potential vulnerabilities to fraud?
- In the fight against fraud, are you focusing only on external crime?
- Are your fraud mitigating activities taking into account the roles of senior management positions and the potential risks associated with their ability to override existing internal controls?
- Do you have an integrated compliance and business ethics program that includes fraud and anti-bribery and anti-corruption procedures? How does your program compare to those of your peers?
- How does your organization embrace training to reinforce the importance of your compliance and business ethics program with all employees around the globe?
- Are you finding the right balance between your technology and people investments? Our Survey results suggest the return on investment of people measures can exceed that of expensive technologies.
- Did you reduce your number of internal reviews, or scale back resources that were previously dedicated to fraud prevention programs?
- How involved are your Board and/or your audit committee in overseeing the company's fraud detection activities? Are they asking the right questions? Are your whistleblower hotline calls up or down? How are you reacting to allegations of fraudulent activity?
- How are you testing the strength of your investigations procedures? In a crisis, do you know what difficult decisions will need to be made—and who will make them?
- Do you know the public perception of your company's brand and where potential threats may lie?
Contacts

Chris Rohn
Global Economic Crime and Fraud Survey Leader, US Territory
chris.rohn@pwc.com

Didier Lavion
Global Economic Crime and Fraud Survey Leader
didier.lavion@pwc.com

Dyan Decker
US Forensic Services Leader
dyan.a.decker@pwc.com

Kristin Rivera
Global Forensic Services Leader
kristin.d.rivera@pwc.com

Brian Castelli
Principal
brian.castelli@pwc.com

Tania Fabiani
Principal
tania.m.fabiani@pwc.com

Beth Savage
Director
beth.a.savage@pwc.com

pwc.com/us/fraudsurvey
pwc.com/us/forensics