Fraud and Economic Crime: A seemingly never-ending battle

How can you gain the upper hand?

US edition

pwc

pwc.com/fraudsurvey

By the numbers –

US survey findings

When fraud strikes: **Incidents of fraud**

20 years

surveying top executives

56%

told us they had experienced fraud in the past 24 months.

As compared to **47%** of those that say so globally.*

5,000+

Global respondents in 2020

400+

US respondents

Top 5 types of fraud

1. **Customer fraud**
2. **Cybercrime**
3. Accounting fraud
4. Asset misappropriation
5. Bribery & corruption

$6.5B

total losses from fraud suffered by US companies over the last 24 months

6

incidents of fraud

On average, companies reportedly experienced 6 incidents **in the last 24 months.**

of those that experienced fraud

3 in 10

US companies were also **accused** of fraud

35%

of US companies were asked to pay a bribe—a record high

37% lost an opportunity to a competitor they believe paid a bribe

Yet 74% of US companies do not have a formal bribery and corruption risk program

* US respondents total 401. For purposes of this report, "globally" or "global respondents" refers to the aggregate of all countries (including the US). Total global respondents = 5,018.

When fraud strikes: **Incidents of fraud**

The rate of fraud and economic crime remains at a record high in the US, experienced by 56% of US companies in our survey—*significantly* higher than the global aggregate of 47%. Turn on any news channel, scroll the internet, or leaf through any newspaper and chances are you'll find a story about economic crime. The disruption is impacting more companies in more diverse ways than ever before.

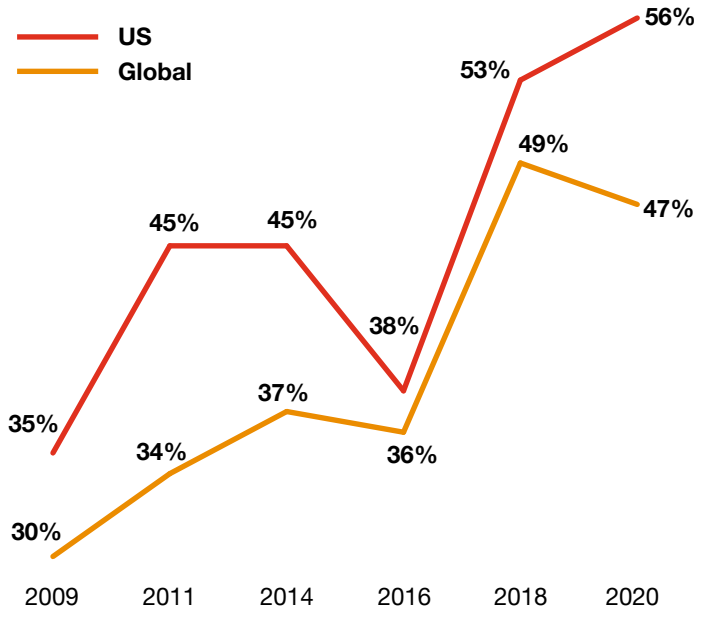
Are you assessing threats well enough…or are gaps leaving you dangerously exposed? Are the fraud-fighting technologies you've deployed providing the value you expected? When an incident occurs, are you taking the right actions?

Our US Edition of PwC's **2020 Global Economic Crime and Fraud Survey**, now in its 20th year, uncovers timely, data-driven insights into fraud trends, including the true cost of the crime, the perpetrators, and what successful companies are doing to come out ahead. We hope you can learn from the experiences of your peers and use these insights to help you better prepare for the unexpected—and protect your company's brand and reputation.

The average US organization has experienced six incidents of fraud in the last 24 months—with 10% of respondents reporting more than 10 frauds in the last 24 months.

Customer fraud, cybercrime, and accounting fraud are the top 3 types of fraud reported. The most significant increases were seen in customer fraud (from 28% in 2018 to 39% this year); accounting fraud (21% to 30%); and bribery and corruption (16% to 22%).

Percentage of respondents experiencing fraud in the last 24 months



When fraud strikes: **Who's committing fraud**

Share of fraud committed by external parties remains unchanged (49%), while the share of those who named an internal actor as perpetrator of their most disruptive fraud has decreased (from 43% to 37%). What's behind that decrease? The growing effectiveness of corporate controls, possibly, plus the addition of a third category, "collusion".

Business partners remain a serious risk. Outsourcing of non-core competencies is a trend that's not going away. But remember: any outside party you invite to act on your behalf can increase your risk significantly—so you must manage that risk carefully at every stage.

- More than 4 in 10 (42%) cite vendors/ suppliers, agents, consultants, shared service providers and other business partners as the source of their most disruptive external fraud.
- Over 80% of Foreign Corrupt Practices Act (FCPA) enforcement actions over the last 5 years have highlighted the use of third parties as conduits in the improper activity.
- Yet nearly half (45%) lack a mature third-party risk program—and 14% have no third-party due diligence and monitoring process at all.

Customer fraud is on the rise—but there's a silver lining. Outside of hackers, fraud committed by customers tops not only the list of external perpetrators (at 27%), but also the list of all crimes experienced (at 39%—up sharply since 2018). The good news? It's also one of the frauds where robust processes and the deployment of technology have proven effective.

Senior-management frauds have leveled off after a strong uptick in 2018. This may be related to a powerful trend toward transparency, the constant glare of social media, growing scrutiny by enforcement agencies, or all of the above—but it's important to stay focused. Keep an eye on internal controls. Be mindful of the connection between corporate culture and employee behavior. And watch how it is being modeled from the top down.

Perpetrators: external, internal and collusion between them*

External perpetrator

US 49%

Global 39%

Internal perpetrator

US 37%

Global 37%

Collusion between internal and external

US 12%

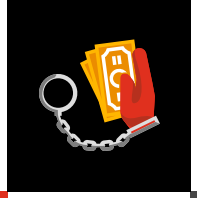
Global 20%

Top US perpetrator

1. Hacker – **34%**
2. Customer – **27%**
3. Organized crime – **17%**

1. Middle management – **42%**
2. Senior management – **26%**
3. Operations staff – **24%**

* Totals do not add up to 100%, due to those that said "Don't know". US reported "Don't know" is 2%; Global reported "Don't know" is 4%.



Feeling the impact: **The cost of fraud**

The cost of fraud—both tangible and intangible—can be staggering:

- **US monetary losses are significantly higher than global.** Roughly one quarter (23%) of respondents who experienced a fraud in the last 24 months reported losing more than $50 million across all incidents, with an average loss of $30 million. This is significantly higher than reported globally, where 13% said they'd lost more than $50 million, with an average reported financial loss of $19.6 million.
- **Were you accused of fraud?** This year, we asked respondents if their organization had been accused of perpetrating a fraud. These incidents are often more costly, with long-term challenges including penalties, fines, and reputational harm—the kinds of events that can derail your strategy. Of those that reported experiencing a fraud, 30% said they were also accused of committing one.
- **Transparency reigns.** In almost equal numbers, competitors, regulators, employees and customers were most likely to be the fraud accuser—evidence of a larger trend toward radical transparency in the face of alleged corporate malfeasance. This trend aligns with an enhanced regulatory focus and with continued whistleblower incentives.

We know from experience that losses are not limited to monetary impact. Many costs are not easily quantified—including brand damage, loss of market position, employee morale, management distraction and lost future opportunities. These can ripple outward with a long-tail effect, impacting multiple areas of the company, both internally and externally.

According to PwC's Global Crisis Survey 2019, organizations that experienced an operational crisis—like fraud—also suffered a domino effect of other events.

Operational Crisis Hits

Source: PwC's Global Crisis Survey, PwC, 2019

The impact: **Being prepared**

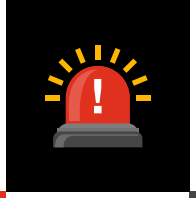
Only 7 in 10 organizations use corporate controls to detect frauds. Industries that are more heavily regulated—including financial services, technology and health-related industries—rely the most on suspicious activity monitoring. When it comes to preparedness, our survey revealed many areas where there are opportunities for improvement:

- **Two out of five US companies don't have formal or documented policies and procedures** for their overall fraud program, and 10% have no formal fraud program in place at all.
- More than a third (35%) of US companies **don't regularly test or audit controls**—nearly 10% don't even have them.
- Despite the fact that those that have been asked to pay a bribe spiked to 35%, **only one quarter of US organizations have a dedicated program to address bribery and corruption risk**. And, while most antibribery programs are focused on foreign corruption risks, three quarters of all respondents reported that accusations of bribery and corruption actually took place *within* the US.
- Surprisingly, by virtually every measure, **US companies trail the overall global group** in their use of dedicated antifraud programs.

The US trails the global aggregate when it comes to having dedicated fraud programs on many risks:

Source: PwC's Global Economic Crime and Fraud Survey 2020

Being prepared doesn't mean you can anticipate every eventuality. But it does mean staying vigilant around the specific kinds of triggers that could pose risks, aligning your fraud programs to these risks—and continuously monitoring and updating for emerging risks. It's equally important to test your controls regularly, wherever possible with independent audits and trend analyses.



Taking action: **Doing the right thing**

What will you do when hit with a fraud?

It seems self-evident, but the best way to avoid getting embroiled in a new fraud is to investigate and learn from the last one. Yet 50% of US companies did not conduct an investigation after the last major fraud. And barely one third reported it to their board.

Regulators—and, increasingly, the public—are demanding more. Reacting too slowly can not only result in more immediate damage, it can also cascade into a broader crisis.

only

50%

conducted an investigation

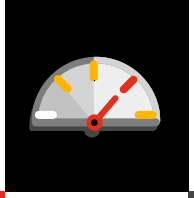
1/3

reported it to the board

What is the secret to emerging stronger after a fraud?

Some organizations emerge stronger after experiencing a fraud, while others falter. So what's the secret? We compared global organizations that self-identified as "emerging stronger" and compared them to the rest to find shared characteristics. *Please note that these figures are on a global scale.*

- **Conduct an investigation (71%).** Getting to the root of the problem is key to preventing further damage. Oftentimes, companies seek external assistance to investigate the fraud when either objectivity is crucial or they lack the resources or expertise to do it themselves.
- **Disclose the incident to government authorities (37%).** Disclosing the fraud early can sometimes result in a more favorable outcome with regulators.
- **Bolster internal controls, policies and procedures (58%).** While some policies and procedures may be easy targets, it's important to assess operations globally and identify what might be missing.
- **Take disciplinary action against employees (44%).** In line with regulatory guidance, compliance programs should apply to all, and no one should be beyond their reach. Enforcement of a compliance program is one of the keys to its effectiveness.
- **Conduct training (32%).** Training not only better informs staff of new policies and procedures, it also promotes a stronger culture around fighting fraud.



Emerging stronger: **Measuring success**

Where will you dedicate your investments? Almost half of US respondents expect to increase the amount they spend on fraud and corruption. Like a three-legged stool, an effective fraud prevention program must find the right balance between three equally robust components: *people, processes*, and *technology*.

People

While technology arguably plays a greater role than ever in fraud prevention, mitigation and investigation, people are ultimately your first and last line of defense. You need people that understand your unique risk profile and are willing to raise a hand when something doesn't seem right. It is also people that run your technology, model the algorithms and drive your monitoring programs. Yet:

- **Just 20% of US companies say they have formal fraud training** and communications that are tracked and refreshed regularly.
- **9% have no fraud training** or communications at all.
- **12% say that lack of digital skills is a top obstacle** to implementing new fraud-fighting technologies.

But there's hope. Most employees (77%) want to learn new skills—or completely retrain—now, according to *PwC's Upskilling Hopes and Fears Survey*.

Processes

Regulators today want evidence that your compliance programs are effective and that they are regularly refreshed. No one program is guaranteed to catch all improper activity and there is not one prescribed method for assessing program effectiveness. That's why compliance programs must be risk-based and right-sized. It may help to distinguish between **operational** frauds and **situational** frauds when setting up programs.

- **Operational frauds** are those that are mainly activity-driven; transactional in nature. Think of cybercrime, money laundering or customer fraud. The goal is typically to plug holes, get quick wins and achieve bottom-line savings; with methods including suspicious activity monitoring, AI and data analytics.
- **Situational frauds** can be more difficult in achieving programmatic ROI. These are mostly behavior-driven, like corruption or accounting frauds. The most effective tools here are culture- and people-based: due diligence, monitoring and investigations. The ROI may be much more complex, but the benefits to your organization can be longer lasting—better crisis preparedness, potentially lower reputational damage, and the like.

Technology

Three in ten US companies said that their most disruptive fraud highlighted a need for new technologies. Yet many are struggling to see the value, trust the effectiveness—or sometimes even understand—the new technologies they are contemplating.

- **Just 25%** strongly agree that they've been able to implement new or upgrade existing technology—citing cost, limited resources, and disparate data as obstacles.
- **38%** are using techniques such as AI and machine learning to combat fraud, but only 25% are finding value in it.

Technology requires a nuanced response—and finding the right balance is challenging. Start by seeking to extract optimal value from the technology you already have and measure its effectiveness. That can be a jumping off point for making your case to invest in new tools.

So what's next?

When it comes to evaluating fraud programs, the question isn't: "Do you have one?" It should be: "How effective is it?"

Can you measure ROI on your fraud programs?

Most people can guess that investments in compliance pay off—somehow. But now there is proof. Data shows a clear link between investments made in fraud prevention on the front end, and the cost savings gained on the back end. Companies that have a dedicated program for their most disruptive type of fraud spent less overall than those who do not have a dedicated program in place.

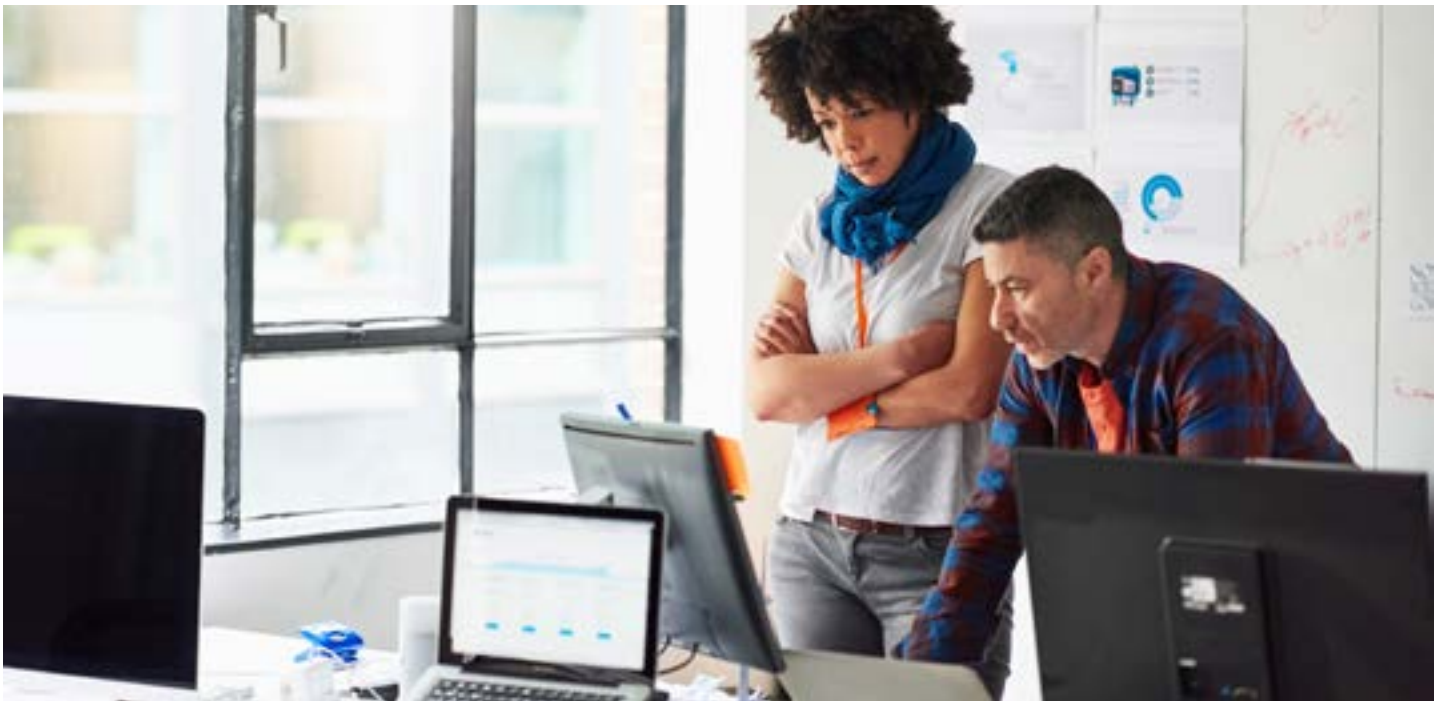
27% less on response

55% less on remediation

76% less on fines and penalties

Sometimes the ROI of fraud preparedness is measured less tangibly—but no less importantly—in terms of positive outcomes. Nearly half (45%) of all global respondents who have experienced an economic crime say they emerged *in a better place*—citing attributes such as an enhanced control environment, streamlined operations, fewer losses, and improved employee morale.

And there's another way to look at a major disruptive event: *as an inflection point*, a possible trigger to a corporate transformation. Whether that transformation is negative or positive depends on how well you prepare for it, mitigate it, and manage it.



In conclusion

Focus on taking inventory of your anti-fraud programs, benchmark your position—and then reframe whatever steps you must take as critical investments in protecting your business.

Five things you can do right now to fight fraud

Investments in preparatory and preventive measures are generally pennies on the dollar as compared to the economic, legal and reputational damage that a fraud can cause. Here are five steps you can take right now to fight the fraud risk:

1. **Look for risk markers.** Are you seeing an uptick in red flags in your activity monitoring? Are hotline calls up or down? Have enforcement patterns in your industry or geographies changed recently?

2. **Test your controls.** Check in with your internal audit team: are you up to date on your risk ecosystem—including those posed by third parties and subsidiaries—and are your controls in sync with those risks?

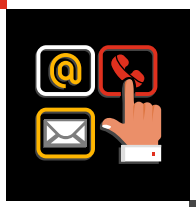
3. **Beef up your policies & procedures.** Business models and enforcement trends change over time. Not only are industries converging, regulators are digging deeper into compliance programs to assess how effective they really are in practice. Make sure yours is up to date, and test it regularly. Even if there is a compliance issue, those kinds of proactive steps can help significantly improve outcomes.

4. **Make your peace with technology.** When it comes to fighting fraud, there's no one-size-fits-all tool. It can be too easy to spend on the wrong things… and too hard to understand the value proposition of the right things. But there *is* a Goldilocks solution for every organization—including yours. Find it by focusing on matching the real risks you face with proven, effective solutions to them. Bonus: that practical approach can help you make the case for investing in the technologies you need.

5. **Change your mindset.** Nobody wants to fall victim to (or stand accused of) fraud. But if you approach it with the right mindset, you will learn a great deal—not only about your degree of preparedness, but also about your strengths (and weaknesses) as an organization. In both cases, you'll have an opportunity to emerge stronger, clearer, and better prepared than your competitors for the inevitable next incident.

To learn more

Contact us to better understand your economic crime and fraud risks and assess your programs against your peers and our global respondents.



Chris Rohn
Principal, Forensics
chris.rohn@pwc.com

Charles Hacker
Partner, Forensics
charles.r.hacker@pwc.com

Kristin Rivera
Partner, Global Forensics Leader
kristin.d.rivera@pwc.com

Denise Messemer
Director, Forensics
denise.messemer@pwc.com

pwc.com/fraudsurvey

pwc.com/us/forensics