2020

Fighting fraud: A never-ending battle

PwC's Global Economic Crime and Fraud Survey

www.pwc.com/fraudsurvey

pwc

Turn on the news or leaf through a newspaper and chances are you'll find a story about economic crime or fraud.

Bribery suspected in building collapse…Medical records and financial data of millions hacked… Corporate malfeasance to blame in product failure…Share price plummets as whistleblower alleges fraudulent accounting practices…

Fraud and economic crime rates remain at record highs, impacting more companies in more diverse ways than ever before. With this in mind, businesses should be asking:

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

These are some of the provocative questions that lie at the heart of the findings in this year's Global Economic Crime and Fraud Survey. With fraud a greater – and more costly – threat than ever, it's essential to assess your readiness, deploy effective fraud-fighting measures, and act quickly once its uncovered.

Fraud

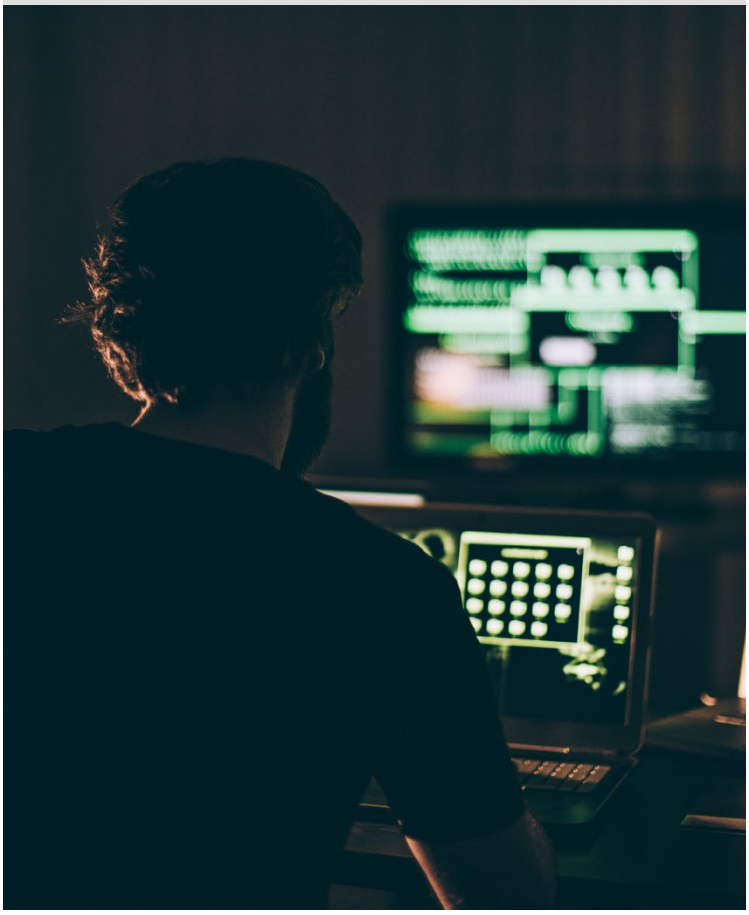
For over 20 years PwC's Global Economic Crime and Fraud Survey looked at a number of crimes, including:

- Accounting/Financial Statement Fraud
- Anti-Competition/Antitrust Law Infringement
- Asset Misappropriation
- Bribery and Corruption
- Customer Fraud
- Cybercrime
- Deceptive business practices
- Human Resources Fraud
- Insider/Unauthorised Trading
- Intellectual Property (IP) Theft IP
- Money Laundering and Sanctions
- Procurement Fraud
- Tax Fraud

Our survey findings

When fraud strikes: **Incidents of fraud**

With nearly half of the more than 5,000 respondents reporting a fraud in the past 24 months, we have timely insights on what types of frauds are occurring, who's perpetrating the crimes, and what successful companies are doing to come out ahead.



5,000+ respondents

62% of respondents were C-suite

72% have US$10M+ in global revenue

99 territories

US$42B in losses

47%

told us **they had experienced fraud in the past 24 months.** This is the **second highest** reported level of incidents **in the past 20 years.**

6 incidents of fraud

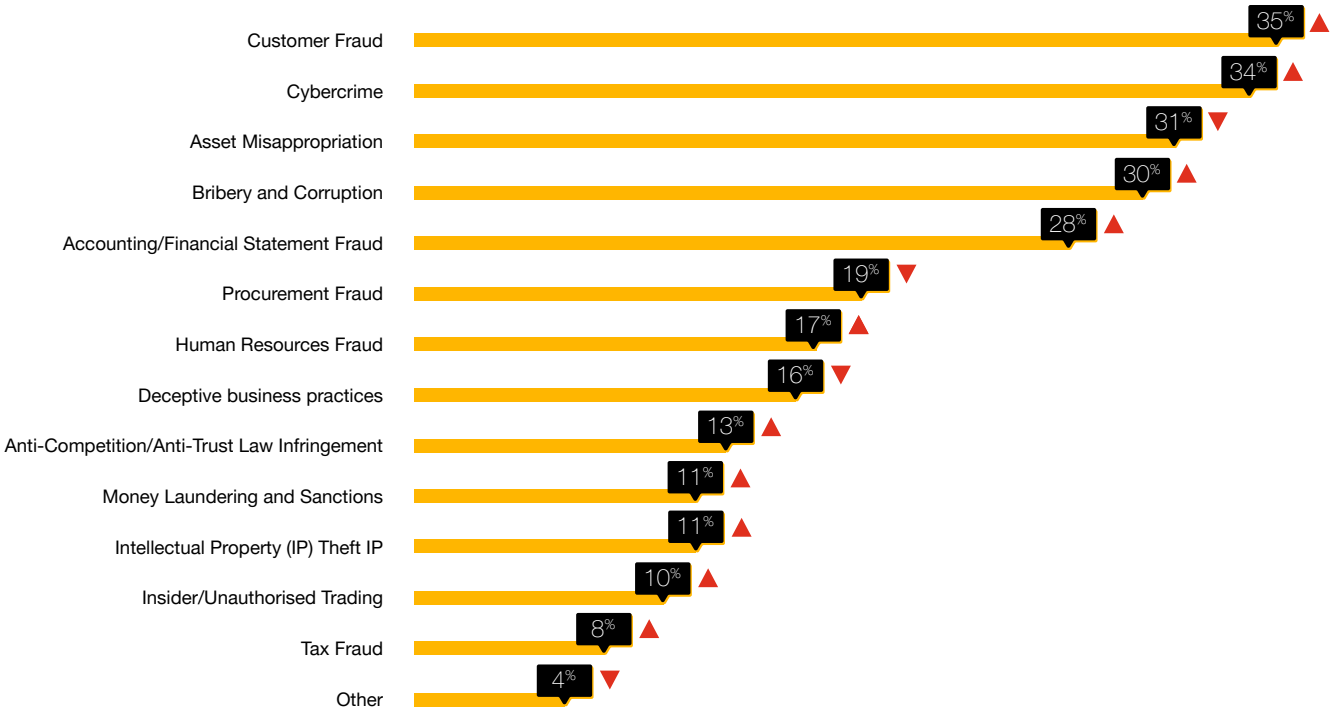
On average, companies reportedly experienced 6 incidents **in the last 24 months.**

Top 4 types of fraud

1. **Customer Fraud**
2. Cybercrime
3. Asset Misappropriation
4. Bribery and Corruption

Reported incidents of fraud committed by customers, accounting fraud, anti-trust, human resources fraud, and bribery and corruption — saw big increases this year.

Crimes: frequency of overall experience



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

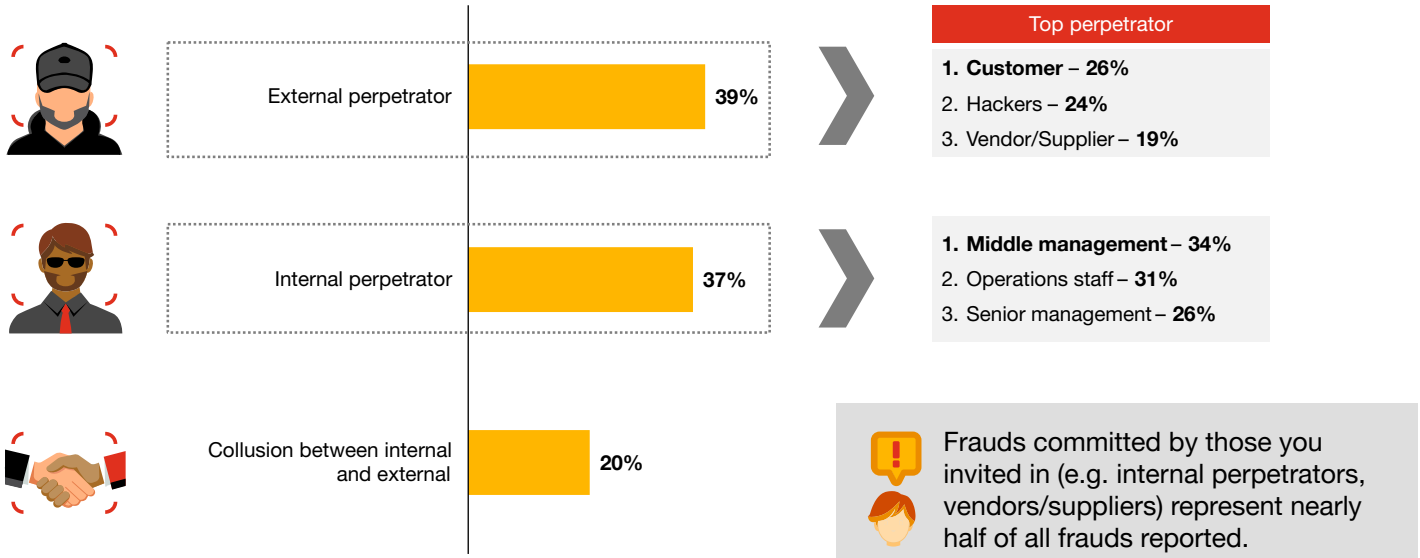
Most disruptive fraud events – by industry

	Consumer Markets	Energy, Utilities & Resources	Financial Services	Government & Public Sector	Health Industries	Industrial Products & Manufacturing	Technology, Media & Telecommunications
1	Customer Fraud **18%**	Bribery and Corruption **17%**	Customer Fraud **27%**	Cybercrime **17%**	Cybercrime **16%**	Asset Misappropriation **21%**	Cybercrime **20%**
2	Asset Misappropriation **17%**	Asset Misappropriation **16%**	Cybercrime **15%**	Accounting/ Financial Statement Fraud **17%**	Accounting/ Financial Statement Fraud **13%**	Cybercrime **15%**	Accounting/ Financial Statement Fraud **16%**
3	Cybercrime **16%**	Accounting/ Financial Statement Fraud **13%**	Accounting/ Financial Statement Fraud **14%**	Bribery and Corruption **16%**	Customer Fraud **13%**	Bribery and Corruption **14%**	Customer Fraud **13%**

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

Fraud hits companies from all angles – the perpetrator could be internal, external, or in many instances there will have been collusion. Business partners remain a risk and fraud committed by management is trending upward.

Perpetrators: external, internal and collusion between them



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

Customer Fraud (26%). Fraud committed by customers tops not only the list of external perpetrators (at 26%) for the most disruptive fraud, but also the list of all crimes experienced (at 35%, up since 2018):

- Not surprisingly, customer fraud is especially prominent in the Financial Services and consumer markets sectors. This could be significant, as more industries shift to direct-to-consumer strategies.
- The good news? It's also one of the frauds where dedicated resources, robust processes and technology have proved effective for prevention.

Third parties (19%). More and more, companies outsource non-core competencies to contain costs. But these business partners can be fraught with risk – a risk many companies have not formally addressed:

- One in five respondents cited vendors/suppliers as the source of their most disruptive external fraud.
- But half lack a mature third-party risk programme - and 21% have no third-party due diligence or monitoring programme at all.

Senior management (26%). These crimes are often among the most insidious because of the ability (whether through delegated authority levels, system knowledge, or influence) top executives have to override – or conspire to override – internal controls.

Accused of fraud? This year, for the first time, we asked respondents who experienced fraud if their organisation had been accused of perpetrating a fraud. Of those who reported experiencing fraud nearly 3 in 10 were also accused of committing a fraud, corruption, or other economic crime:

- In almost equal numbers, competitors, regulators, employees, and customers were most likely to point the finger.
- Enhanced regulatory focus, and in some territories, whistleblower incentives may contribute to this trend.

Nearly half of reported incidences **resulting in losses of US$100 million or more were committed by insiders.**

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

Fraud losses are complex. Some costs can be tallied: direct financial loss or costs due to fines, penalties, responses and remediation. But some costs are not easily quantified — including brand damage, loss of market position, employee morale, and lost future opportunities.

US$42B

losses reported due to fraud **in the last 24 months**

Some frauds – such as external frauds – generally strike from outside the company, are transactional in nature, lend themselves to active monitoring, and when managed properly may reduce financial impact. For other frauds like bribery and corruption, or those internally perpetrated, it's more about managing and mitigating the downside risk. They tend to be harder to predict, monitor, and result in more costly fines -- and have ancillary repercussions such as lost business or brand harm.

Roughly **13%** of respondents who experienced a fraud in the last 24 months reported **losing more than US$50 million across all incidents.**

Top 5 costliest frauds. Antitrust, insider trading, tax fraud, money laundering, and bribery and corruption were tops in terms of direct losses — some compounded by the significant cost of remediation and after-the-fact fines.

Major frauds perpetrated by insiders are potentially far more damaging than externally perpetrated crime and not just because the financial loss is likely to be higher. 43% of reported incidences resulting in losses of US$100 million or more were committed by insiders. But such crimes can often also result in civil or criminal actions against the company and those involved, reputational harm, management distraction, and loss of business.

Diving in

Bribery and corruption remain a big challenge. One-third of all respondents say they had either been asked to pay a bribe or had lost an opportunity to a competitor who they believed had paid a bribe.

Among the responses, there were a few **blind spots and surprises:**

- **6 in 10 organisations don't have a programme to address bribery and corruption risk.**
- Nearly half of all respondents either don't perform a risk assessment or only perform an informal one.
- Half of all respondents either don't perform, or perform only informal, risk-based due diligence and ongoing monitoring of third-parties.
- Fewer than **3 in 10** companies perform limited testing of the operating effectiveness of their controls, and another **12%** do no testing at all.

Taking action: **Being prepared**

What are you doing to prevent and identify fraud? Which programmes, methods and technologies are working — and which are not? What perception gaps are still standing in the way — and what opportunities for improvement are ripe to be seized?

Fighting fraud pays… but are you doing enough? On average, companies have four dedicated programmes in place to mitigate fraud risk (larger companies with more than 10,000 employees average more). While nearly two-thirds of companies reportedly have policies and procedures in place and the majority (6 in 10) include training and monitoring — **barely half of organisations are dedicating resources to risk assessment, governance, and third party management.**

So what actions are most effective?

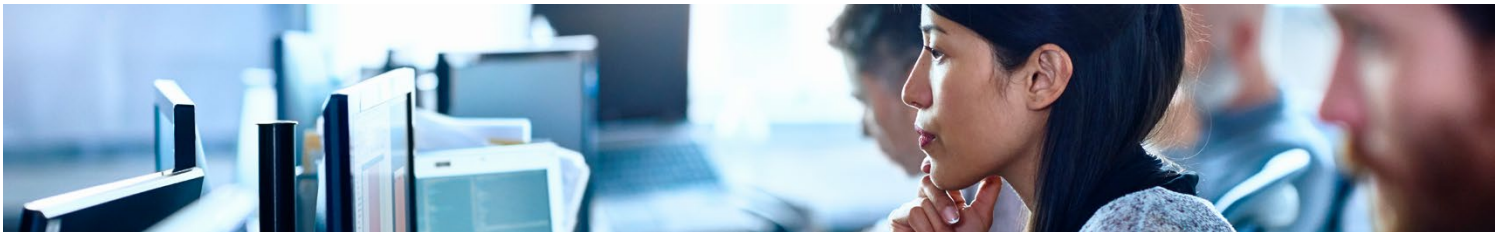
1. **Identify, rank, and address all your risks.** Companies should perform robust risk assessments, gathering internal input from stakeholders across the organisation and across geographies, to identify risks and assess mitigating factors. These assessments should also incorporate external factors. There is a wealth of information available in the public domain, and ignoring it could potentially result in a big miss. Risks should be assessed at regular intervals (not through a 'one and done' approach).
2. **Back-up your technology with the right governance, expertise, and monitoring.** Recognise that one tool won't address all frauds – and technology alone won't keep you protected. Technology is often only as good as the expert resources, data management and visibility, robust controls, and regular monitoring dedicated to it.
3. **Take notice.** The ability to react to a fraud once identified is critical and a foundational element of an effective fraud program. The ability to quickly mobilise the right combination of people, processes, and technology can limit the potential damage. Disruptive frauds often disguise a strategic inflection point – triggering the opportunity for broader organisational transformation.

Technology is just part of the answer

Large numbers of organisations have invested heavily in new tools and techniques in recent years, but many respondents revealed concerns about deploying technology:

- Fewer than **3 in 10 strongly agree** that they've been able to implement or upgrade their technology — with issues of cost, limited resources, and lack of systems cited as obstacles.
- Considering alternative technologies and techniques, only 25% are using artificial intelligence (AI) — a technology that is ever more prevalent today (however, nearly 40% of the organisations using AI are struggling to find value in it as a fraud-fighting tool).

A single tool or technology on its own will not amount to an anti-fraud programme. Are you collecting the right data with the right rules and requirements? How are you analysing that data? Are you feeding findings back into your programme to make it more robust? As companies struggle to implement new anti-fraud technologies, organisations using new tools such as artificial intelligence do find value when implemented appropriately.



What do you do when your organisation is hit by fraud? **Nearly 60% of companies who conducted an investigation ended up in a better place** — but nearly half of respondents didn't conduct an investigation at all. And one-third reported it to their board.

Regulators — and increasingly, the public — demand more. Reacting too slowly can not only cause more immediate damage, it can cascade into a broader crisis. According to PwC's Global Crisis Survey organisations with 5,000 or more employees are most likely to experience crises related specifically to **cybercrime (26%), natural disaster (22%), leadership (17%) or ethical misconduct (16%),** including fraud, corruption, and corporate malfeasance.

According to PwC's 2020 CEO Survey 58% of CEOs are concerned with their readiness to respond to a crisis

What key steps did organisations that emerged in a better place take?

Conduct an investigation (71%). Getting to the root of the problem is key to preventing further damage. Companies often seek external assistance to investigate the fraud when either objectivity is crucial or they lack the resources or expertise to do it themselves.

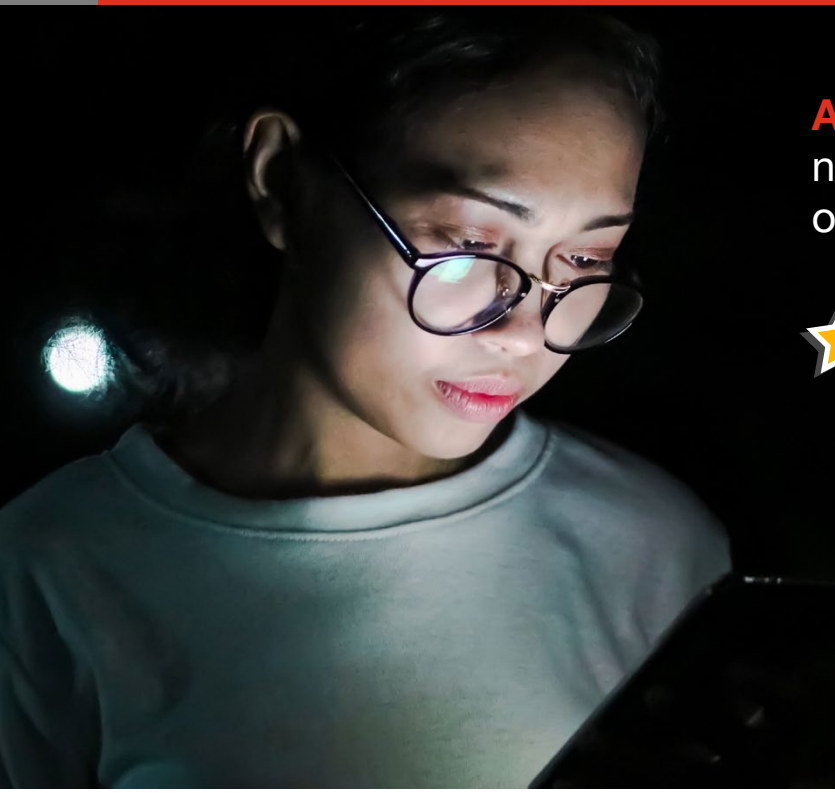
Bolster their internal controls, policies and procedures (>50%). While some policies and procedures may be easy targets, it's important to assess operations globally and identify what might be missing.

Take disciplinary action against employees (44%). In line with regulatory guidance, compliance programmes should apply to all and no-one should be beyond their reach; no person should be deemed too valuable to be disciplined. Enforcement of a compliance programme is one of the keys to its effectiveness.

Only
56%
of organisations **conducted an investigation** of their worst incident

Barely **one third reported it to the board**

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



Almost 90% said they experienced negative emotions after an incident of fraud

42%
positive feelings and emotions

89%
negative feelings and emotions

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

Disclose the incident to government authorities (37%). Disclosing the fraud early can sometimes result in a more favourable outcome with regulators.

Conduct training (32%). Training does not only better inform staff of new policies and procedures, it also promotes a stronger culture around fighting fraud.

Not surprisingly, respondents overwhelmingly **(89% to 42%)** said they experienced negative emotions after an incident of fraud. However, those who stated their organisation was in a better place post fraud stated:

- the main perpetrator was external to the organisation ('we were attacked'), rather than internal ('one of us') **(48%)**.
- companies felt strongly that they stayed true to their values, acted as a team, and prepared and followed a plan.

Taking stock

Nobody wants to fall victim to (or worse, stand accused of) fraud. But there's another way to look at a major disruptive event: as an inflection point, a possible trigger to organisational transformation. Whether that transformation is negative or positive — a full-blown crisis, or an improved market position for example — depends on how well the business was prepared and how it was managed.

The data shows that there's a significant upside to taking stock when an incident strikes. **Nearly half (45%) of all respondents who have experienced a fraud say they emerged in a better place** — citing attributes such as an enhanced control environment, streamlined operations, fewer losses, and improved employee morale. Large companies are even more likely (52%) to say they emerged better off – citing adoption of new technology and fewer repeat incidents, in addition to a better environment and streamlined operations.

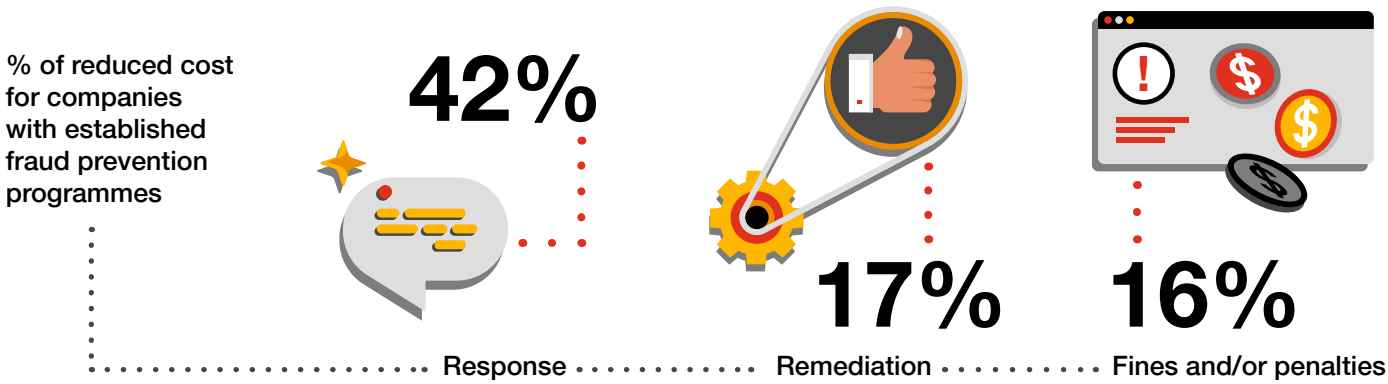
Those in fraud-related functions often find themselves fighting for increased budget to invest in new technologies, implement new programmes, or hire additional resources. **Nearly 40% of our respondents say they plan to increase their spend on fraud prevention** in the next two years. But do the measures work and will they see a return on their investment? And how do you justify the expense to your leaders?

It can be challenging to quantify the benefits of a fraud-fighting tool. It's common sense that effective fraud prevention measures reduce the quantity and magnitude of future fraud. But here's a more interesting statistic – **there is a clear link between fraud prevention investments made upfront and reduced cost when a fraud strikes.**

Companies that have a dedicated fraud programme in place generally spent less (relative to revenue) on response, remediation and fines:

- Companies with a dedicated fraud programme reportedly spent 42% less on response and 17% less on remediation costs than those companies with no programme in place.
- Where bribery or corruption was experienced, companies with a dedicated bribery and corruption programme spent 58% less on remediation than those without.

Companies who invested in fraud prevention incurred lower costs when a fraud was experienced



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

Once you have a programme in place, periodic assessment and refinement is key. Why?

- Business models are often dynamic and can evolve or change before risk programmes are established or enhanced, leaving companies exposed to unanticipated risks.
- There's increasing convergence in certain industries — for example, technology companies offering financial services, or health companies entering consumer markets —and risk management programmes need to be adapted to meet those new or evolving risks.
- A hotline call or audit finding may yield a risk previously not considered.

And perhaps most importantly, regulators are paying more attention to compliance programmes – some are starting to request companies to provide evidence showing that their compliance programmes are effective.

Many regulators recognise that compliance programmes should be risk-based and right-sized and that no programme is guaranteed to catch all improper activity. There is no cookie-cutter approach to compliance, and a programme at a large telecommunications company will no doubt look different from a programme at a small retailer. Even so, both may be adequate for addressing the particular risks faced by each organisation.

Similarly, there is no single prescribed method for assessing effectiveness. There are many scholarly articles on assessing the effectiveness of training that do provide helpful insights; however, not much is available on assessing the effectiveness of a third-party management programme, for example.

This provides an opportunity for companies to define their own meaningful assessment system, which may cover areas such as: vendor rationalisation statistics, vendor rejection statistics, participation of vendors in training programmes, vendor certifications, and/or a reduction in exception rates / findings during third-party audits. **The key is to have a defensible measurement in place that will help to demonstrate that the programme area has been tested and how it would prevent or detect problematic misconduct in the future.**

In conclusion

So where do you stand? Are you a leader in preventing, detecting, and responding to fraud? Or are there areas for improvement that you should address as a matter of urgency?

Either way, you need to act. Even the 'best' anti-fraud programmes need to be continually assessed and refined. Because as we've seen the perpetrators and methods of crime evolve, your defences must also be modified to meet the new risks.

Alternatively, if your fraud defences have blind spots or gaps, you're leaving yourself exposed to risks and the increasing costs of fraud.

Fraud is a risk to which no business is immune. And when hard questions are asked after an incident, a lack of awareness or insight is no excuse.

Now is the time to understand just how prepared you are. A customised survey allows you see how you measure against your market, industry, or global peers - and what steps you can take now to combat fraud in the future.

To learn more

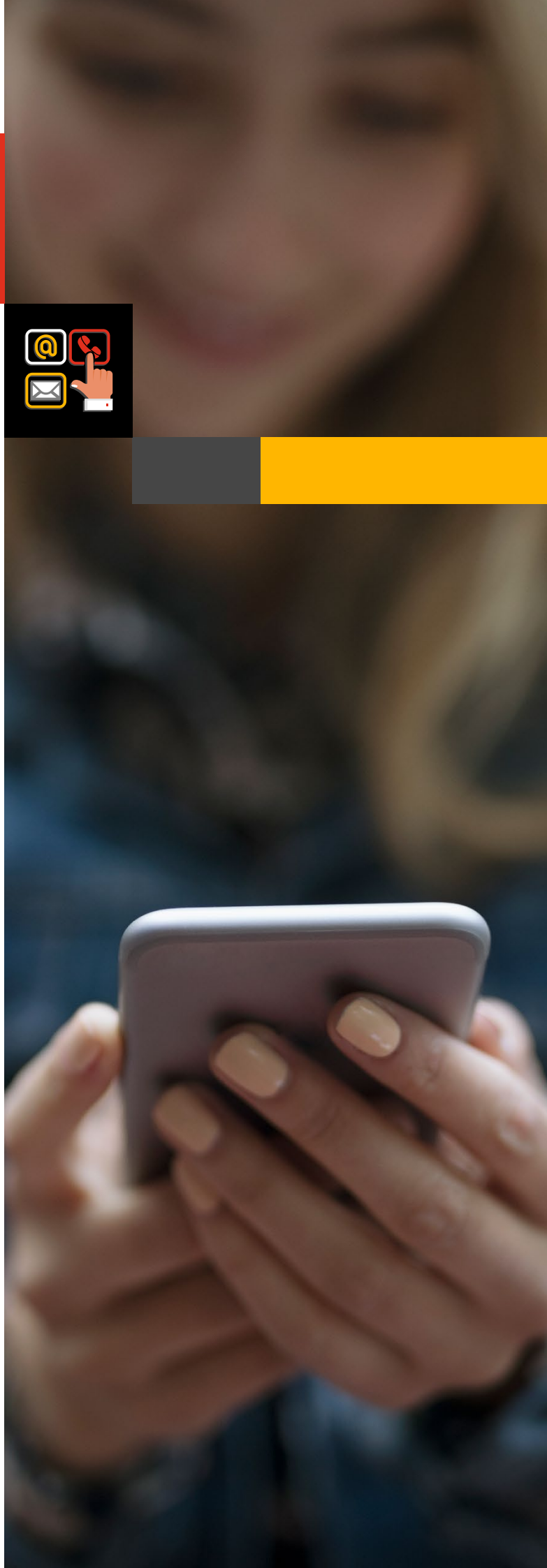
Better understand your economic crime and fraud risks and assess your programmes against your peers and our global respondents.

Kristin Rivera
Global Leader, Forensics,
PwC United States
kristin.d.rivera@pwc.com
+1 415 302 3428

Chris Rohn
Principal, Global Economic Crime and Fraud Survey 2020 Leader,
PwC United States
chris.rohn@pwc.com
+1 312 714 7463

John Donker
Partner, APA Forensics Leader,
PwC Hong Kong
john.donker@hk.pwc.com
+852 91962726

Chris Butter
Partner, EMEA Forensics Leader,
PwC U.K.
christian.butter@pwc.com
+44 7841 498581



pwc

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

WLT127074948