



PwC's Global Economic Crime and  
Fraud Survey 2022

Protecting the perimeter:

The rise of

external fraud



**pwc**

Canadian insights





## New vulnerabilities and threats

On the global stage, and right here in Canada, rising environmental, geopolitical, financial and social pressures are creating a risk landscape that is more volatile than ever. This volatility complicates the challenge of preventing fraud and other economic crimes. Even as organizations act quickly to navigate change, bad actors look to exploit the potentially widening cracks in fraud defences. In fact, almost two-thirds of organizations we surveyed in Canada have experienced fraud in the past year.

As a business leader, you must ask yourself: Are sufficient controls in place for the myriad new business processes and digital technologies being deployed? Are we adequately managing risks related to a sustained hybrid work environment? Has our organization implemented the appropriate policies and incentives, as businesses around the world emerge from the pandemic into an uncertain economy? What is the most pressing fraud risk that our company faces today?

Years of effort to combat fraud through policies, training, internal controls and monitoring have helped businesses clamp down on internally driven misconduct, even in a volatile risk environment. At the same time, however, new, more impactful threats have been brewing. This year's [Global Economic Crime and Fraud Survey](#) conducted by PwC shows that organizations' perimeters are increasingly vulnerable, and external fraudsters are emerging as a bigger threat. Let's take a closer look at what this all means, particularly for companies doing business in Canada.

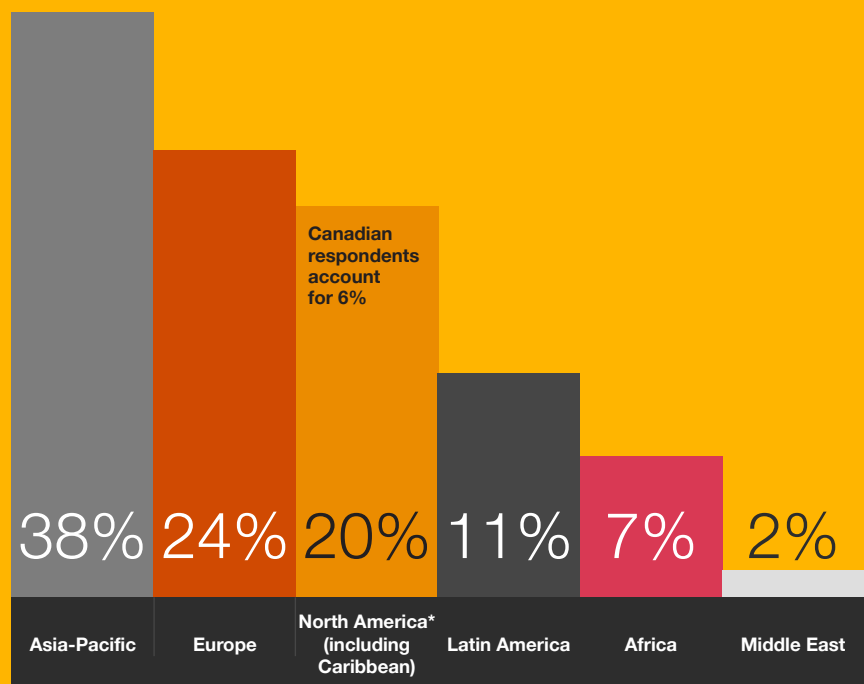
1



## About the survey

The 2022 Global Economic Crime and Fraud Survey examined organizations' attitudes toward fraud and financial and economic crime in the current environment, with polls being conducted at two different times (May and June 2022), in total surveying 2,319 people in 68 countries. This report combines that research, homing in on fraud trends and conduct risk.

**63% of Canadian survey respondents sit in the C-suite**  
**72% of Canadian respondents' organizations have annual revenues greater than US\$100 million**



Source: PwC's Global Economic Crime and Fraud Survey 2022 - combined poll results



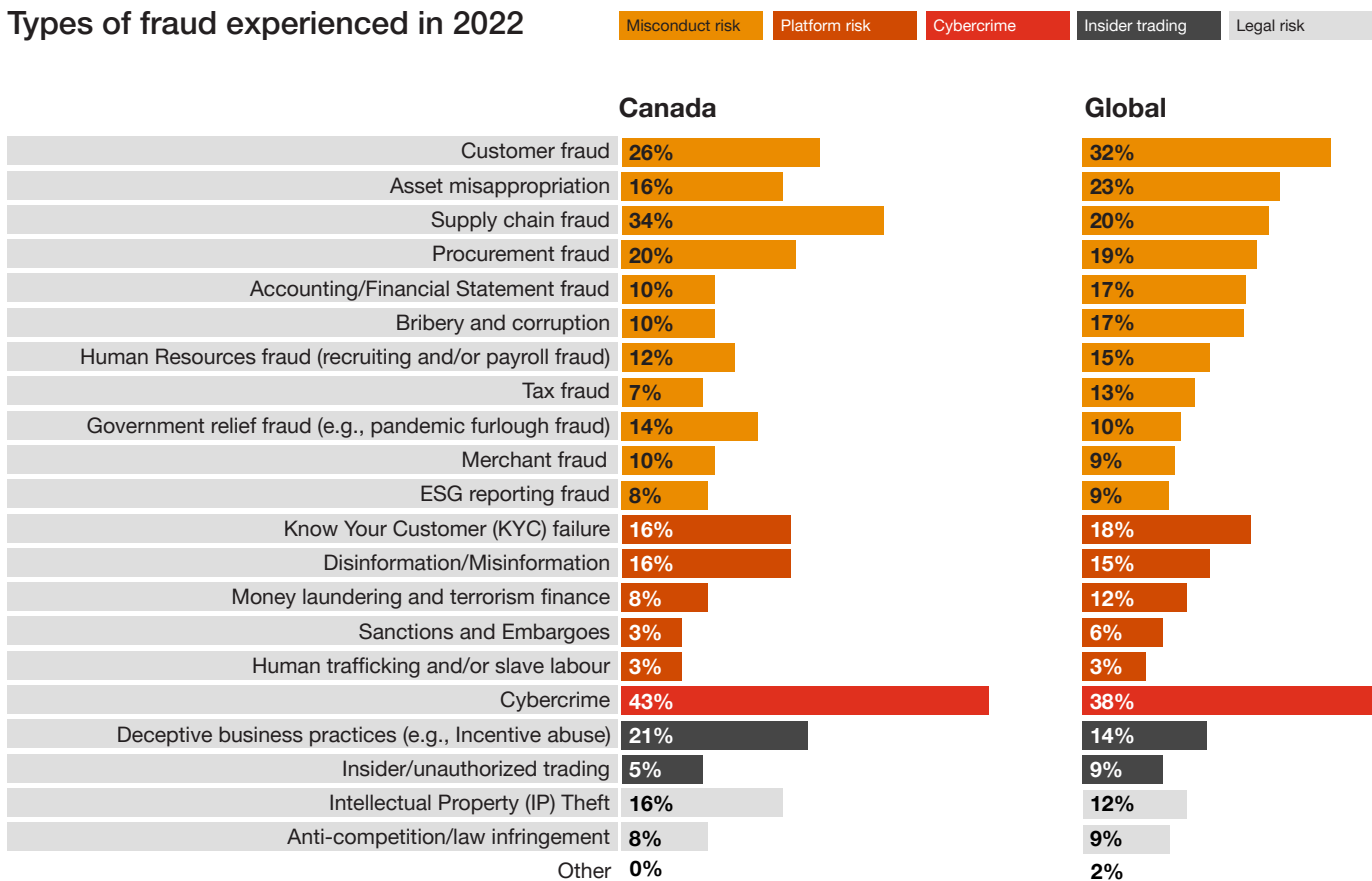
### Key survey finding: New risks emerge related to supply chain disruptions and ESG

On a global scale, just 51%\* of the organizations that PwC surveyed reported experiencing some form of fraud or other economic crime within the last 24 months. But in Canada, that number was higher, at 60%. And although many Canadian organizations have invested large amounts of resources to fight financial crimes and prevent and detect fraud, new threats and perpetrators continue to emerge. Canadian respondents reported experiencing new types of fraud and financial misconduct in the last two years—especially related to the pandemic and government relief programs, as well as to supply chain issues and environmental, social and governance (ESG) programs.

### Fraud rates and financial impact among large and small organizations

**73%**  
of Canadian respondents said that as a result of the disruption caused by COVID-19, their organization has experienced increased risk

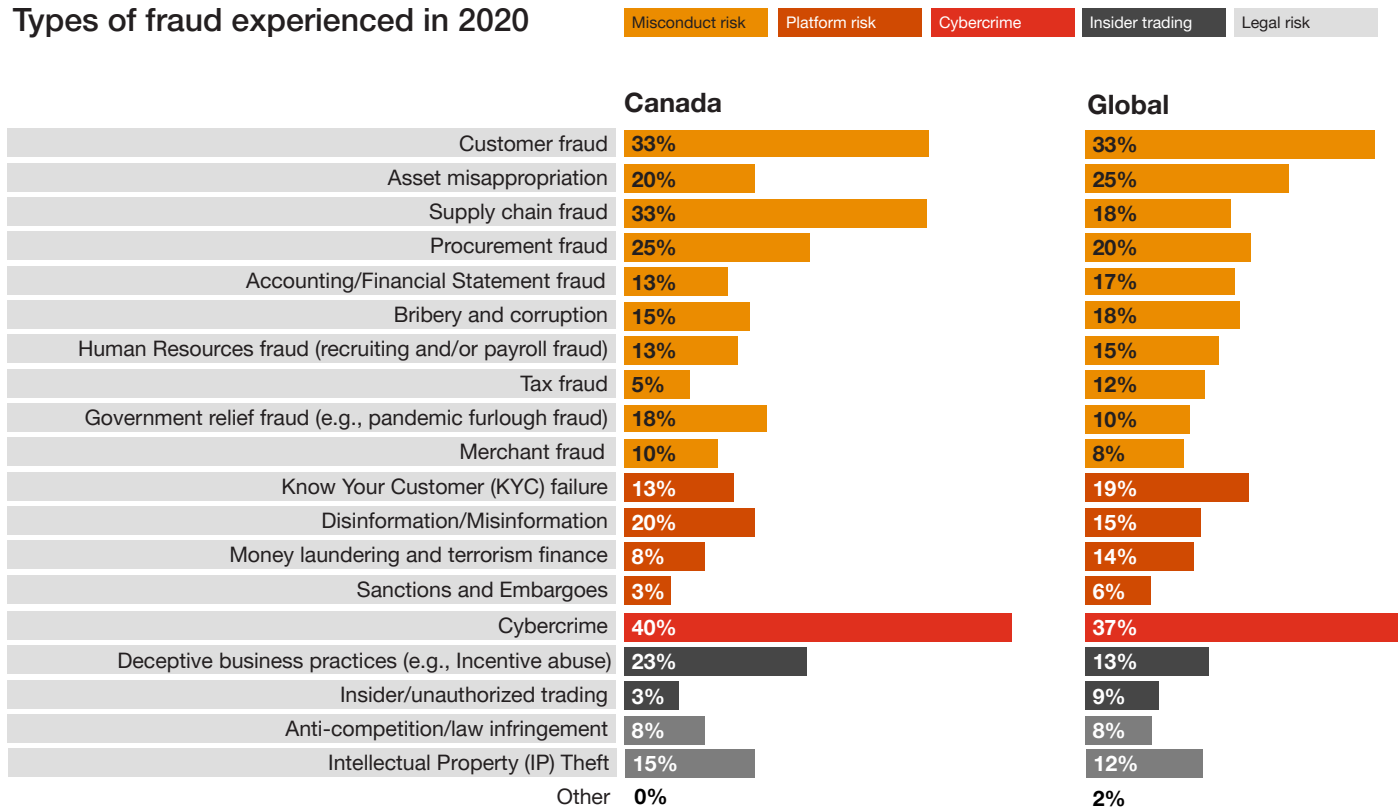
### Types of fraud experienced in 2022







## Types of fraud experienced in 2020



In addition to experiencing new kinds of fraud, Canadian organizations that suffered losses from fraud that were higher than US\$1 million increased by 20%, comparing data in 2022 with data from 2020. That increase of 20% means that, overall, fraud in 2022 caused more losses than in 2020.

Canadian organizations, however, are getting better at detection. In Canada, the rate of fraud detected through advanced data analytics is 9% higher than the global average. Suspicious activity monitoring detection rate is 7% higher than the global average. And external audits are 6% higher than the global average.

So what's ahead for Canadian business leaders? These are the three main areas to focus on when it comes to fraud: (1) continue with ongoing prevention, (2) change how we protect against new threats and (3) consider new ripple effects at the enterprise-wide level that emerge from ongoing digital systems and collaboration (i.e. platform risk). We consider each in greater detail below.

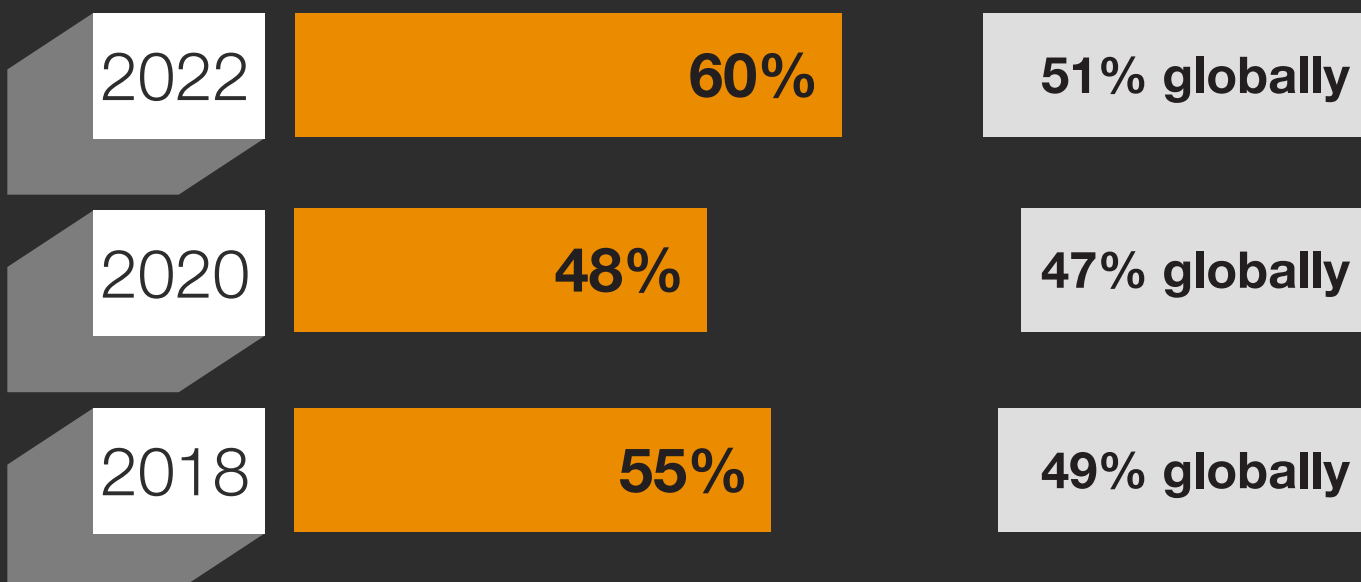
## Takeaway #1: Fraud prevention measures work

Despite the rising risks—from the pandemic, supply chain issues, environmental and geopolitical instability, an uncertain economy and a talent shortage—on the global stage, no significant increase has appeared in fraud, corruption and economic crime rates since 2018.

In Canada, however, the rates of fraud have risen, and it's important for business leaders to remember that fraud is expensive. It hits the bottom line, leaving less money to redistribute to stakeholders, improve employee conditions or invest in innovation. In the future, it will be wise for organizations not to underestimate the cost of fraud versus the cost of investing in better controls to prevent and detect fraud.



### Share of Canadian organizations experiencing fraud, corruption or other types of economic crime



We found a notable increase in such economic crimes in Canada over the past two years. What might account for the higher number of companies experiencing fraud in Canada compared with the global experience? One possible explanation is that more Canadian companies digitized their activities in the past two years in response to COVID-19 lockdowns, and that may have led to new sources of threats. As organizations changed their ways of doing business, enabling many more people to work from home, for example, that likely had an impact on processes and internal controls as well.





### Breakdown of direct loss suffered by Canadian organizations in the last 24 months through the most disruptive fraud

Less than 50,000 US dollars	8%
50,000 to 100,000 US dollars	14%
100,000 to < 1 million US dollars	14%
1 million to < 5 million US dollars	19%
5 million to < 50 million US dollars	8%
50 million to < 100 million US dollars	8%
100 million US dollars or more	7%
Immeasurable (solely non-tangible loss)	9%
Don't know	13%

### Cybercrime, customer fraud and supply chain fraud are top concerns in Canada

Unsurprisingly, given the rapid acceleration of digitization over the past several years, cybercrime still accounts for the majority of economic crime: 43% of respondents have been victims of it in 2022, and [CEOs cite it as a top risk](#). However, our survey results show that cybercrime has actually gone down 5% from our previous survey in 2020.

We also note a decline in cybercrime since 2018. This general decline may seem counterintuitive given the increase in online applications and processes. But companies have simultaneously been investing in more prevention measures. In Canada, organizations adapted their IT security and protected themselves more efficiently as they digitized operations. This increased security seems to have worked and resulted in a lower impact of cybercrimes in 2022.

Following cybercrime, according to our survey, the largest types of fraud reported in Canada were customer fraud and supply chain fraud, with 33% of respondents reporting that they had been a victim of misconduct in the last 24 months.

Comparing the Canadian data with the global data, we see that Canada reported more misconduct risk, potentially due to supply chain fraud (34% vs. 20% for global), more government relief fraud (18% vs. 10% for global) and more procurement fraud (14% vs. 10% for global). As Canada quickly implemented several government assistance programs during COVID-19, varying controls—given the speed of implementation of these measures—may have led to an increase in opportunities to commit fraud.

## IN FOCUS

## Fraud in a downturn

The pandemic created unsettling vulnerabilities as organizations accelerated the shift to digital operations. One bright spot is that asset misappropriation, although still a top category of fraud, was down in the last 24 months—perhaps, in part, because more employees are now working remotely, with limited access to company assets. At the same time, remote working increased risks beyond just digital security. For example, some companies experienced increased risks to employee safety; there was a heightened risk of blackmail or physical harm to employees working from home with access to valuable corporate data. Additionally, the rate of organizations experiencing disinformation fraud (e.g. social media spreading fake news) in the past 24 months was 15%, suggesting companies need to increase their awareness of this emerging risk.

Past downturns, such as the 2007–09 recession, offer valuable lessons for organizations navigating volatility as they begin to emerge from the pandemic. History shows that fraud trends in times of turmoil don't emerge immediately. Often, it takes 18–24 months for these events to become known. However, inflection points, such as the shift from a shrinking to an expanding economy, can be beacons for internal fraud identification.

Much initial fraud can become visible in times of transition because fraudster behaviour often lags the shift to new goals and targets. For example, corrupt employees may be taking illegal actions to achieve sales targets that leaders know are unobtainable heading into a down economy, creating suspicion. External fraudsters also capitalize on inflection points, taking advantage of market confusion, particularly with consumer-based schemes. Organized crime groups can recruit more easily in a down economy, bringing in the suddenly unemployed as new team members. And as a result, there's every reason to increase scrutiny of fraud risks in a downturn, giving special attention to those an organization may not have seen before.



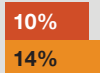
### Economic crime due to COVID-19

As the ripple effects of COVID-19 continue, combining with geopolitical risks and economic instability, companies have experienced new kinds of fraud and increased risks.

#### Misconduct risk



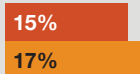
#### Legal risk



#### Cybercrime



#### Insider trading



#### Platform risk



■ New type of fraud experienced  
■ Areas of increased risk

Source: PwC's Global Economic Crime and Fraud Survey 2022 - combined poll results



# 90%

of those encountering fraud in Canada experienced new incidents of fraud as a result of disruption caused by COVID-19\*

\*Note: This is a difference of 20 percentage points from the global average of 70%.



## Takeaway #2: Threats are changing, so protecting the perimeter has to change



## The perimeter is vulnerable, and the game has changed

Our 2022 global survey identified an unsettling threat profile emerging. Dangerous new predators—external entities, including cyber threat actors and organized crime rings—that can't be controlled or easily influenced are quickly growing in strength and effectiveness. Nearly 70% of organizations surveyed around the world that reported experiencing fraud also reported that the most disruptive incident came via an external attack or collusion between external and internal sources. This is because external fraudsters (e.g. cyber threat actors) are immune to traditional fraud prevention tools such as codes of conduct, training and investigations.

Additionally, we've seen a significant rise in cybercrime and a decrease in reported organized crime rings. The impact of cyber criminals and organized crime rings, which are among the most common external perpetrators, rose substantially in the last two years. About 33% of external perpetrator cases were the result of cyber threat actors, and 28% were conducted by organized crime. Both numbers reflect increases from our 2020 survey.

### Main perpetrator of the most disruptive or serious fraud experienced in Canada



**External perpetrator**

**60%**

(53% in 2020)  
Compared with 43% for global



**Internal perpetrator**

**15%**

(28% in 2020)  
Compared with 31% for global



**Collusion between internal and external actors**

**25%**

(16% in 2020)  
Compared with 26% for global





### External threat actors are a rising risk

As more employees work remotely, and more processes become digitized, we’re seeing a rise in fraudsters acting from home, rather than in a company office, as well as seeing cyber threat actors. Additionally, as supply chains become increasingly digital, those operations present opportunities for new fraud risks to emerge.

At the same time, organized crime groups are becoming more specialized and professional, with goals, incentives and bonus structures. We expect them to continue taking advantage of vulnerabilities, and they will likely keep investing to outsmart their targets. Combatting these bad actors is unlike the effort to contain internal fraud, because companies have little ability to influence or control the perpetrators’ actions.

Several factors are converging to drive a rise in external fraud. The increased frequency of data breaches in recent years will undoubtedly continue, raising the bar considerably for companies obligated to protect the private, personally identifiable information of their customers. The breaches will also challenge the knowledge-based authentication strategies that organizations have put in place to protect against fraudsters.

Bad actors are also collaborating with one another, increasing both the volume and the sophistication of attacks.

#### Type of external perpetrator

	2022	2020
Customer	38%	25%
Hacker	32%	25%
Vendor/supplier	26%	10%
Competitor	21%	12%
Agent/intermediary	15%	11%
Consultant/adviser	15%	9%
Organized crime	15%	19%
Shared service provider	12%	17%
Joint venture/alliance partner	9%	9%
Foreign state	6%	20%
Other/Don't know	3%	3%

#### Positions of perpetrators

Senior management	Operati staff	Middle management	Contract worker and/or “gig” worker	Shared service/ offshore center	Other staff	Don't know
31%	29%	24%	8%	7%	1%	1%

Source: PwC’s Global Economic Crime and Fraud Survey 2022 - combined poll results



## Takeaway #3: ESG reporting, supply chain disruptions and the rise of more connected enterprise-wide digital systems increase fraud risks



As more customers, employees, governments and other stakeholders put pressure on companies to achieve ESG targets and standardize their reporting, the risk of related manipulation and fraud is expected to rise.

# 52%

of Canadian respondents reported being relatively concerned to extremely concerned about the manipulation/fraud of ESG reporting by employees within their organization

### Greatest challenges in managing risks associated with ESG targets and reporting requirements

	Canada	Global
Intagibility to accurately monitor or report ESG of third party business partners	48%	42%
Inability to accurately monitor or report ESG metrics with my organization	42%	40%
Inability to prevent or detect misconduct related to ESG risks	49%	37%
General lack of understanding of what ESG means	32%	37%
Failure to define ESG objectives for my organization	35%	35%
Inability to manage ESG-related for my organization	27%	35%
Lack of ownership over ESG in my organization	27%	35%
Other	1%	1%
Don't know	6%	7%



In general, Canadian organizations reported slightly fewer concerns about ESG challenges, as compared with global respondents, but they all face similar challenges in this area. Canadian organizations' greatest concerns involved three issues:

- 49% of respondents reported concern about their inability to prevent or detect misconduct related to ESG risk (compared with 37% globally)
- 48% of respondents reported concern about their inability to accurately monitor or report ESG metrics of third-party business partners (compared with 42% globally)
- 42% of respondents reported concern about their inability to accurately monitor or report ESG metrics within their organization (compared with 40% globally)

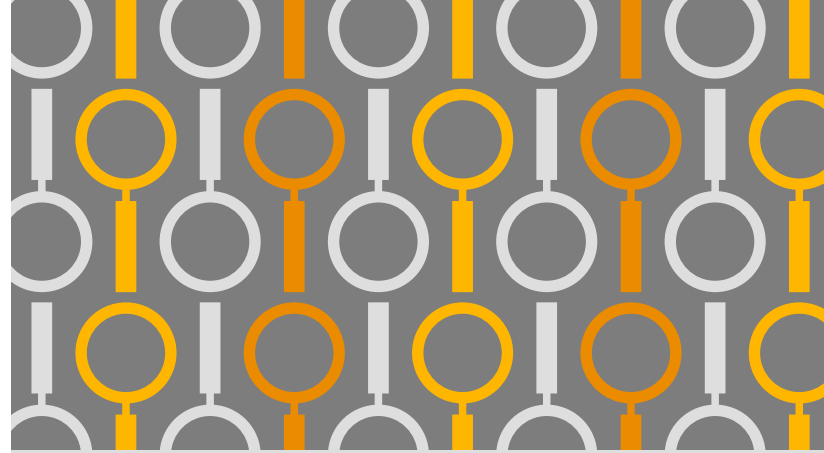
Additionally, when it comes to the future of fraud, we expect to see more risks coming from the enterprise-wide digital systems (i.e. platforms) that organizations rely on today. According to our global survey respondents, four in 10 experienced some form of fraud in the past two years connected to the digital platforms they rely on, whether that was related to know-your-customer (KYC) breaches, disinformation, money laundering, terrorism financing or anti-embargo activities. The rise of digital platforms, such as social media, e-commerce or services (for example, ride-sharing or lodging), opens the door to myriad fraud and other economic crime risks that most companies are just beginning to understand.

Platform risks can create a ripple effect—with the impact of fraud penetrating multiple organizational silos. Because platform fraud is an enterprise-wide problem, combatting it requires an organization-wide, cross-functional effort with a diverse community of solvers.

IN FOCUS

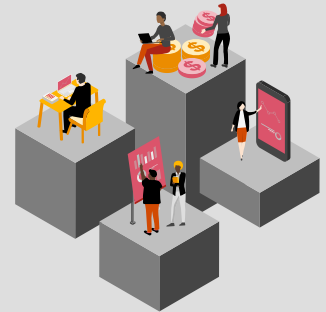
## Emerging threats

Trust has become a key lever for value creation. So a perceived or real misstep in transparency can wreak havoc on brand reputation and underlying trust. That's why, as previously discussed, with ESG responsibility growing in importance to stakeholders, accuracy in ESG reporting will be increasingly essential. A relatively low percentage of organizations reported encountering ESG reporting fraud in the last 24 months. However, we expect that risk to increase—along with the consequences. And the same is true for supply chain risks.



3%

of Canadian organizations said they experienced **anti-embargo fraud** in the last 24 months.



10%

of those organizations encountering fraud in the last 24 months experienced **ESG reporting fraud**.

23 %

of organizations experienced new incidents of **supply chain fraud** as a result of the disruption caused by COVID-19.



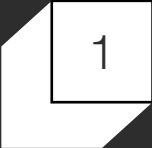






## Three actions to lower your fraud risk and increase your resiliency

Respondents to our 2022 survey indicated that they were strengthening internal controls, technical capabilities and reporting to prevent and detect fraud. However, defending against predators requires a new approach.

Here are three considerations to help you build resiliency for the future:

- 

**Understand the end-to-end life cycle of customer-facing products**  
Identify where opportunities exist for a fraudster to exploit customer-facing products and cause financial, legal or reputational damage.
- 

**Strike the proper balance between user experience and fraud controls**  
Through the right combination of fraud technology, strategy and processes, both a good user experience and effective fraud controls are achievable.
- 

**Orchestrate data**  
Consolidate data from disparate, disconnected systems into a centralized platform that can track the end-to-end life cycle of users, including fraudsters, and generate meaningful alerts.

---

## Conclusion

Looking ahead, business leaders will need to prioritize human-led, tech-powered solutions when it comes to fraud prevention and detection. Putting people at the heart of decision making is a critical way to build trust and create [culture change](#), thereby adding value across the organization and driving better business outcomes.



Want to know more about what you can do in the fight against economic crime?

Contact one of our subject matter specialists:

**National Leaders**

**Jennie Chan**

Forensic Services Leader, Partner  
+1 416 815 5057  
jennie.m.chan@pwc.com

**Edward Matley**

Partner, Crisis & Resilience  
+1 778 998 5334  
edward.matley@pwc.com

**Montréal**

**Marie-Chantal Dréau**

Partner, Forensic Services  
+1 514 205 5407  
marie-chantal.dreau@pwc.com

**Danny Garwood**

Partner, Cyber Forensic Investigations  
+1 514 205 5404  
danny.garwood@pwc.com

**Ottawa**

**Steven Malette**

Partner, Forensic Services  
+1 613 755 5979  
steven.m.malette@pwc.com

**Toronto**

**Jessica Allen**

Partner, Forensic Services  
+1 416 815 5210  
jessica.c.allen@pwc.com

**Joseph Coltson**

Leader, Cyber Forensic Investigations  
+1 416 687 8262  
joseph.coltson@pwc.com

**Sam Samod**

Partner, Financial Crime Services  
+1 416 815 5137  
sam.samod@pwc.com

**Western Canada**

**Krista Mooney**

Partner, Forensic Services  
+1 403 509 7336  
krista.a.mooney@pwc.com



<https://www.pwc.com/ca/forensics>

© 2022 PwC. All rights reserved.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.