



The Cost of Fraud

How business owners are tackling risks and challenges

September 2024

CFIB
CANADIAN FEDERATION
OF INDEPENDENT BUSINESS.



Introduction

In the current business landscape, small and medium-sized businesses (SMEs) across Canada are increasingly worried about the threat of fraud. These challenges have the potential to not only disrupt daily operations and undermine business stability but also have broader economic implications for the country.

Fraud against businesses occurs when an individual or group manipulates or deceives a business often through a 'scam' — a deceptive scheme designed to steal money, goods, services, or valuable information such as personal or banking data. Common examples include email phishing, spyware, fraudulent advertising, office supply scams, and fraudulent payments. It's important to note that direct theft, where no deceit is involved, is not considered fraud.

Insights from CFIB's August *Your Voice* survey reveal that in the past 12 months half of small business owners have encountered fraud, either through attempted scams or by falling victim to it. While scams like email phishing, phone calls, and text messages are common, businesses are particularly susceptible to more damaging forms of fraud, such as fraudulent payments and chargebacks. The average cost to small businesses victimized by fraud in the past 12 months is \$7,800, covering direct costs such as financial losses, legal fees, and equipment replacement. Beyond financial losses, fraud also consumes time, reduces productivity, and negatively impacts staff morale due to increased stress. Business owners' concerns are further heightened by the rise of artificial intelligence, with many fearing that AI will enable more sophisticated and harder-to-detect fraud attempts.

This report explores the challenges faced by small businesses as a result of fraud, identifies the prevention measures currently in use, and offers recommendations to enhance resilience against these evolving threats.

Highlights

Small businesses' experience with fraud

- In the past 12 months, half of business owners (50%) have experienced either attempted or successful fraud.
 - Sectors most impacted by fraud attempts include transportation (61%), finance, insurance, real estate, and leasing (59%), and arts, recreation, and information (57%).
 - The likelihood of experiencing fraud attempts increases with business size.
- Four in five businesses feel more worried about fraud than ever before.
- Nine in ten business owners fear artificial intelligence will fuel more sophisticated fraud.
- Despite these concerns, many business owners (68%) are still confident in their defenses.

Common types of fraud experienced by small businesses

- Although email scams and phishing (85%), text scams (77%), and phone call scams (76%) are the most prevalent methods of attack, SMEs are more likely to fall victim to fraudulent payments (18%) and chargebacks (17%).
- Hospitality, retail, transportation, personal services, and arts, recreation, and information are the sectors most affected by chargebacks and fraudulent payments.

The impact of fraud and scams on small businesses

- 36% of businesses that experienced fraud suffered losses within the past year, with an average financial cost of \$7,800
- Beyond financial losses, businesses experiencing fraud report significant impacts, including time wasted dealing with the situation (76%), negative emotional impact (51%) and decreased staff morale (23%).

Fraud prevention practices used by small businesses

- To combat fraud, businesses are prioritizing stricter payment verification processes (50%), increased cybersecurity investments (36%), and enhanced employee training (32%).

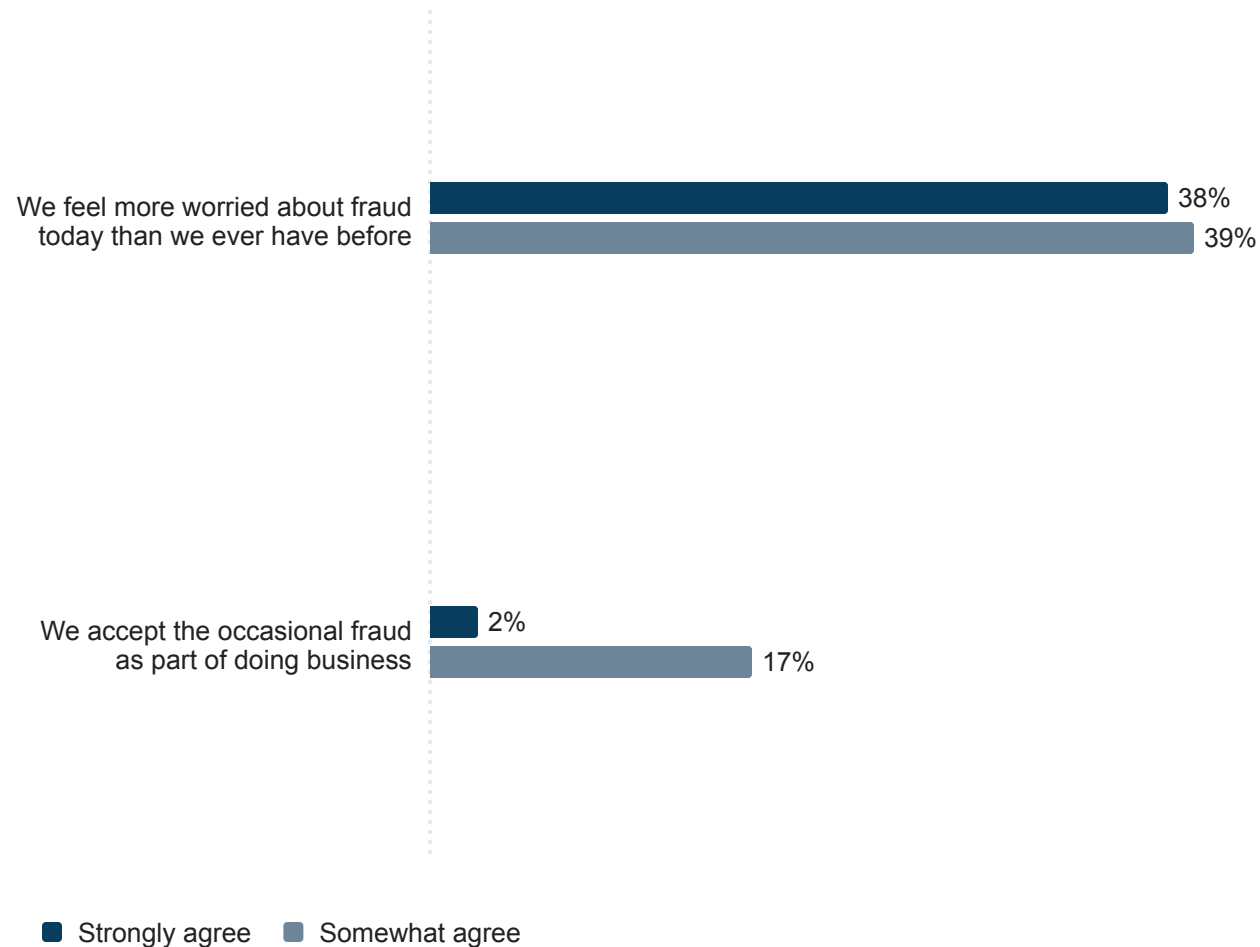
Small businesses' experience with fraud

“It's really devastating to go through a situation like this. With a small business like mine, a single scam can be the difference between having an open sign or a for sale sign.”

Retail business, ON

”

Fraud is a serious concern for small businesses: Close to four in five businesses **feel more worried** about fraud than ever before, and one in five **accept fraud as a part of doing business**.



In today's increasingly complex business environment, small businesses are feeling a heightened threat from fraud, which poses significant risks to their operations and stability. While already operating on tight margins, small businesses cannot afford financial losses from fraud.

With **four in five** (77%) small business owners expressing greater concern about fraud today than ever before, and **one in five** (19%) accepting occasional fraud as part of doing business, these results highlight the significance of this issue for SMEs.

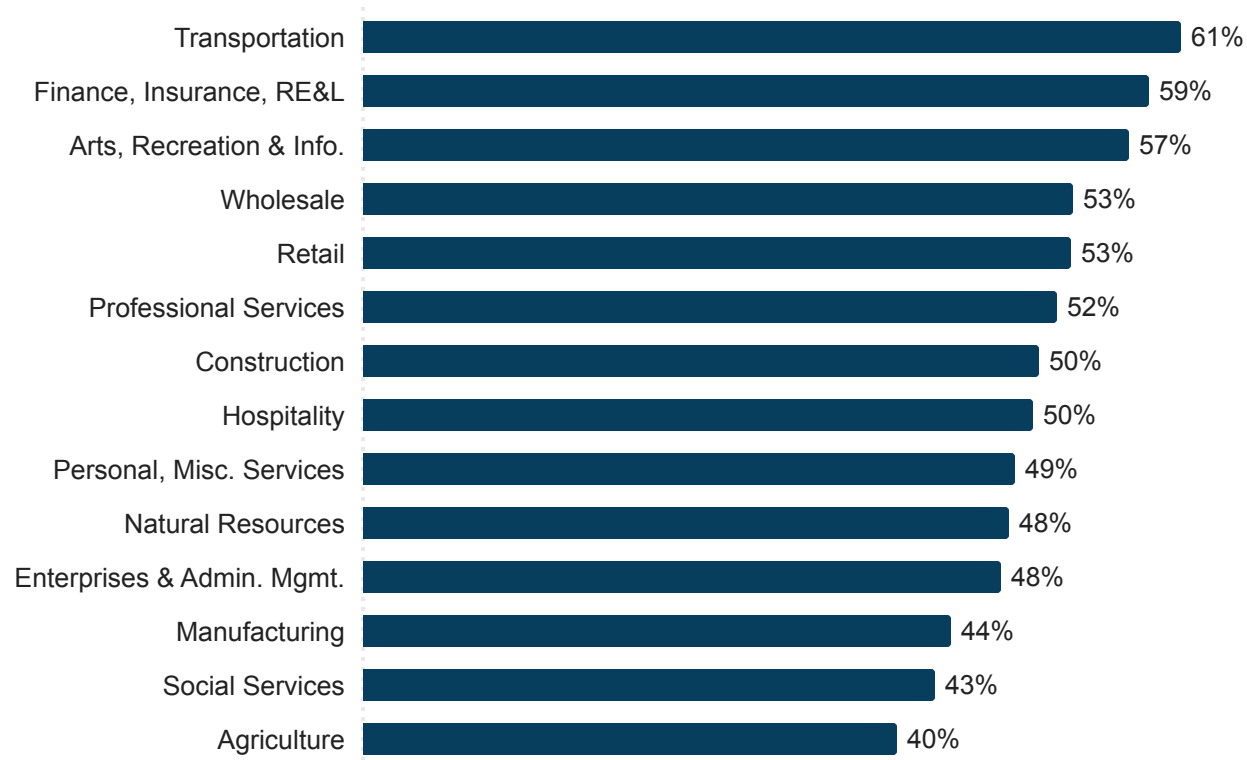
Source: CFIB, Your Voice – August 2024 survey, n = 1,945.

Question: To what extent do you agree or disagree with the following statements regarding business fraud?
(Select one for each line)

Fraud impacts half of small businesses and affects a broad spectrum of industries

1 in 2 small businesses experienced fraud in the past year

Fraud experienced, by sector



Source: CFIB, Your Voice – August 2024 survey, n = 1,990.

Question: In the past 12 months, has your business experienced any attempts or been a victim of actual fraud or scams? (Select one)

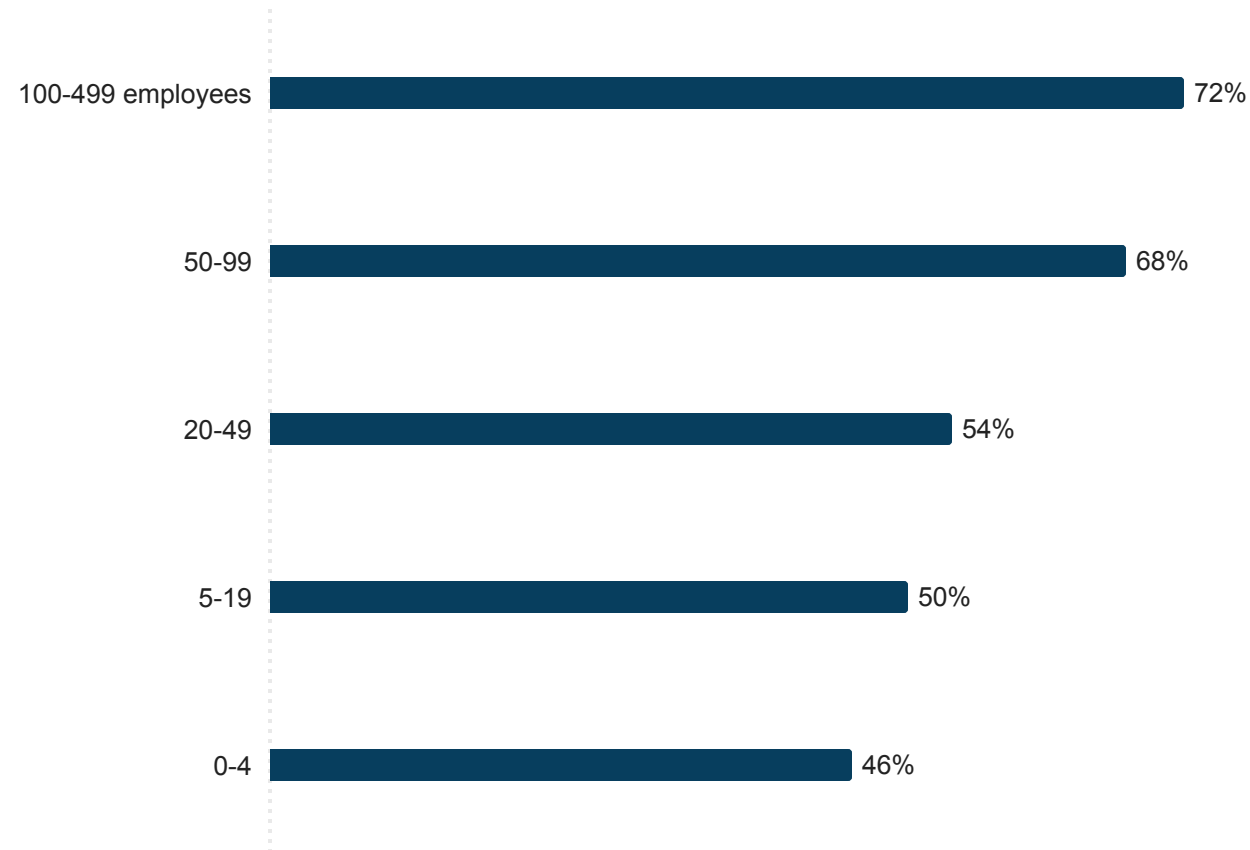
In the past 12 months, **half of small business owners** (50%) have faced attempted fraud or fallen victim to it.

Fraud impacts a broad spectrum of industries, but the level of risk varies across sectors—with those in transportation (61%), finance, insurance, real estate, and leasing (59%), and arts, recreation, and information (57%), wholesale (53%), and retail (53%), reporting the highest incidences of fraud. These sectors are particularly vulnerable due to the nature of their operations, which can involve high transaction volumes and sensitive information, making them attractive targets for fraudsters.

While other sectors may be less frequently targeted or may have operational characteristics that make fraud less prevalent, the impact is still substantial enough to warrant attention.

Larger businesses face a higher risk of experiencing fraud, though smaller businesses are also significantly affected.

Fraud experienced, by business size



While all businesses are vulnerable to fraud, the risk increases with business size. For example, 72% of larger businesses (100-499 employees) have encountered fraud, compared to nearly half (46%) of smaller businesses, including those with fewer than five employees.

Larger businesses might be more attractive targets due to their scale, resources, and potentially larger digital footprints. Smaller businesses, while less frequently targeted, still face substantial risks, underscoring the importance of fraud prevention measures across all business sizes.

Source: CFIB, Your Voice – August 2024 survey, n = 1,990.

Question: Fraud In the past 12 months, has your business experienced any attempts or been a victim of actual fraud/scam(s)? (Select one)

Common types of fraud experienced by small businesses

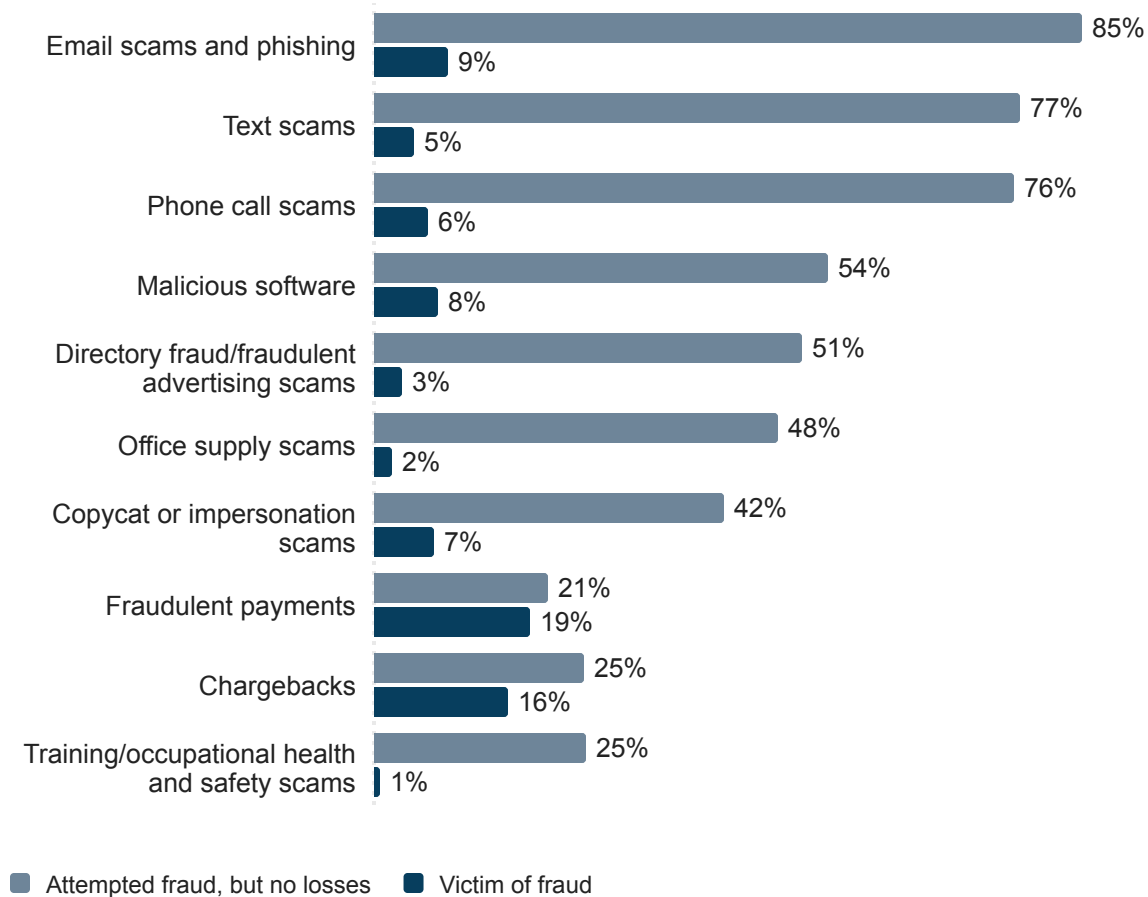
“For me, the biggest issue with fraud is the constant phone calls about refused payments with a bank or Amazon. It's unbelievable how many of these I receive—several times a day on some days. It's absolutely unacceptable that this type of crime is occurring openly every day.”

Retail business, AB

”

Common **fraud tactics** include email, text, and phone scams, although payments and chargebacks typically result in greater financial losses

Types of fraud experienced by small businesses*



Source: CFIB, Your Voice – August 2024 survey, n = 982.

Question: How has each of the following types of scams impacted your business? Please select the option that best describes each type.

Note*: Includes responses from businesses that encountered fraud within the past 12 months.

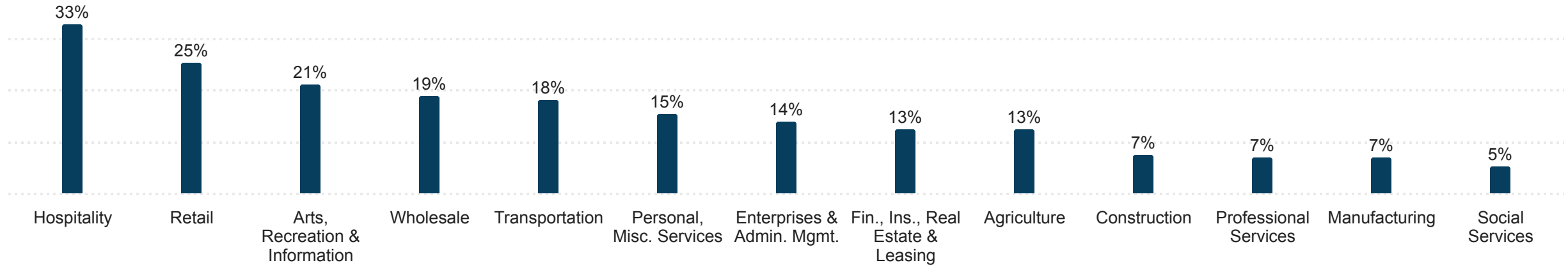
Businesses are affected by fraud in two ways. First is fraud which results in a loss of money, goods/services or valuable information. Second is attempted fraud, which targets a business but does not result in any loss.

The most common types of attempted fraud include email scams and phishing (85%), text scams (77%) and phone call scams (76%). However, businesses are less likely to fall victim to them, suggesting they are better equipped to spot or mitigate the risks of these types of fraud.

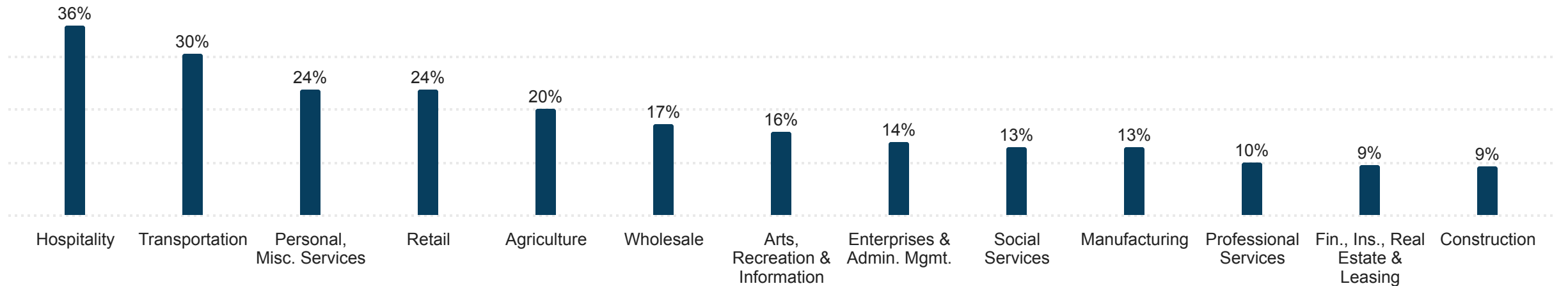
In contrast, fraudulent payments and chargebacks, though less common, are more likely to result in business losses. Fraudulent payments can involve the use of stolen credit card information or the manipulation of point-of-sale terminals for unauthorized transactions. Fraudulent chargebacks occur when customers falsely dispute legitimate transactions.

The **hospitality sector is the most affected** by chargebacks (33%) and fraudulent payments (36%), likely driven by high transaction volumes and the frequent use of credit/debit card payments, increasing the risk for disputes and fraud.

Victim of chargebacks (fraudulent customer disputes resulting in the reversal of a sale transaction)*



Victim of fraudulent payments (e.g. using stolen credit/debit cards or cheques, counterfeit currency to pay your business)*



Source: CFIB, Your Voice – August 2024 survey ,n = 939.

Question: How has each of the following types of scams impacted your business? Please select the option that best describes each type.

Note*: Includes responses from businesses that encountered fraud within the past 12 months.

The impact of fraud on small businesses

“[Regarding the cost of fraud] there is a cost to train staff, to pay for cyberinsurance and to meet the requirements to be insurable, as well as the stress of constant awareness.”

Wholesale business, ON

”

36%

of businesses that experienced fraud within the past year suffered losses, with an average financial cost of

\$7,800

During the past year, 36% of businesses that experienced fraud suffered losses at an average financial cost of \$7,800.^{[1][2]} This estimate captures not only the direct losses but also broader expenses such as the value of lost goods or services, legal fees, and computer replacement costs. This is a conservative estimate, as it does not account for lost productivity, missed sales or business opportunities, which can further amplify the true cost of fraud.

Approximately three-quarters of victims reported costs below the average. This trend may be attributed to the tendency of fraudsters to target smaller amounts, which are less likely to be detected and are subject to more lenient penalties in Canada. Fraud under \$5,000 carries a maximum prison sentence of up to two years, while fraud exceeding this threshold can result in sentences of up to 14 years.^[3]

[1] Source: CFIB, Your Voice – August 2024 survey, Preliminary results.

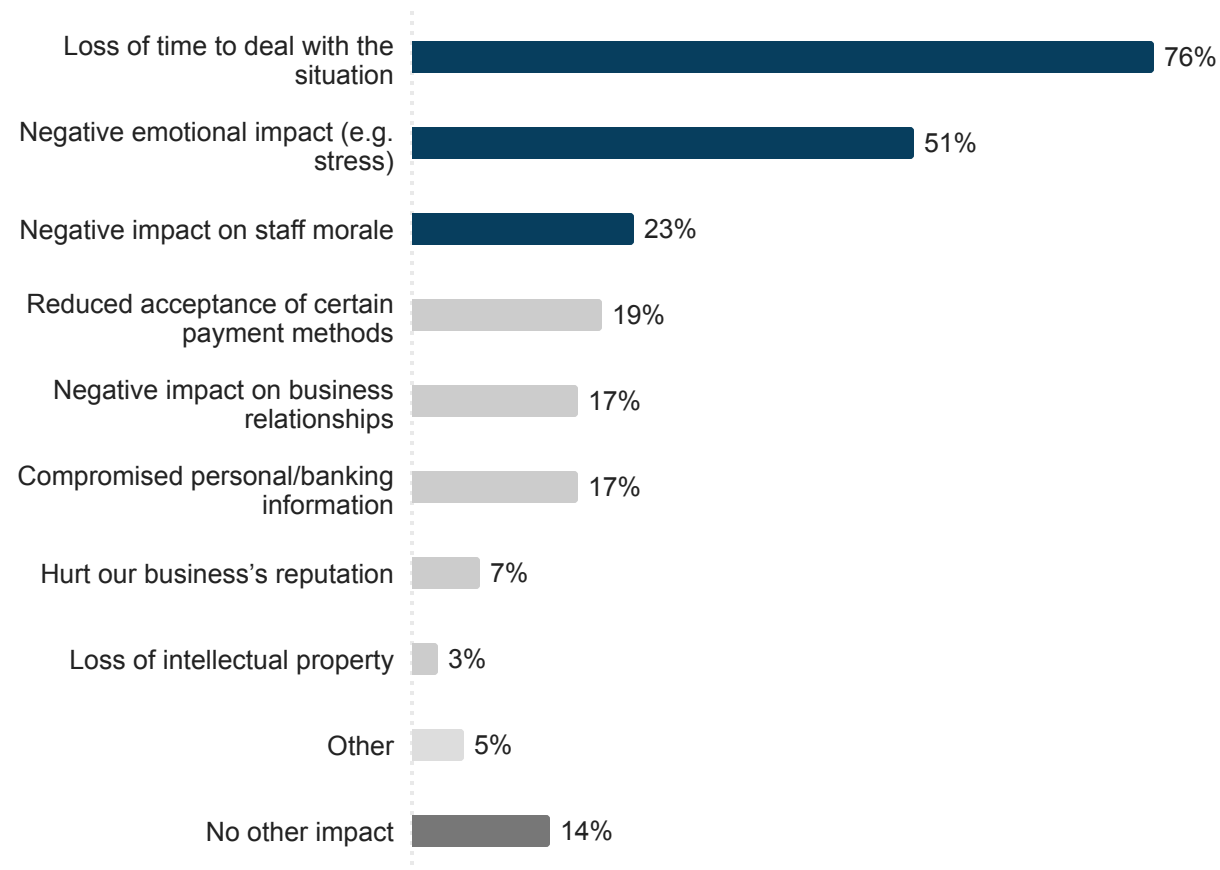
Question: What were the approximate financial costs your business incurred as a direct result of the scam(s) during the past twelve months (including money lost, value of goods/services lost, legal costs, computer replacement, etc.)? (Please indicate amount; enter \$0 if you did not incur any financial costs)

[2] Includes responses from businesses were victims of fraud in the past 12 months.

[3] Government of Canada. *Criminal Code (R.S.C., 1985, c. C-46). Section 380.* [Web] Accessed on August 29, 2024: <http://laws-lois.justice.gc.ca/eng/acts/C-46/page-82.html?txthl=engud>

Hidden cost of fraud: Businesses impacted by fraud experience significant consequences beyond financial losses.

Impacts of fraud experienced by small businesses beyond financial losses*



Source: CFIB, Your Voice – August 2024 survey, n = 979.

Question: What impacts, other than the financial costs, did the scam(s) have on you or your business? (Select all that apply)

Note*: Includes responses from businesses were victims of fraud in the past 12 months.

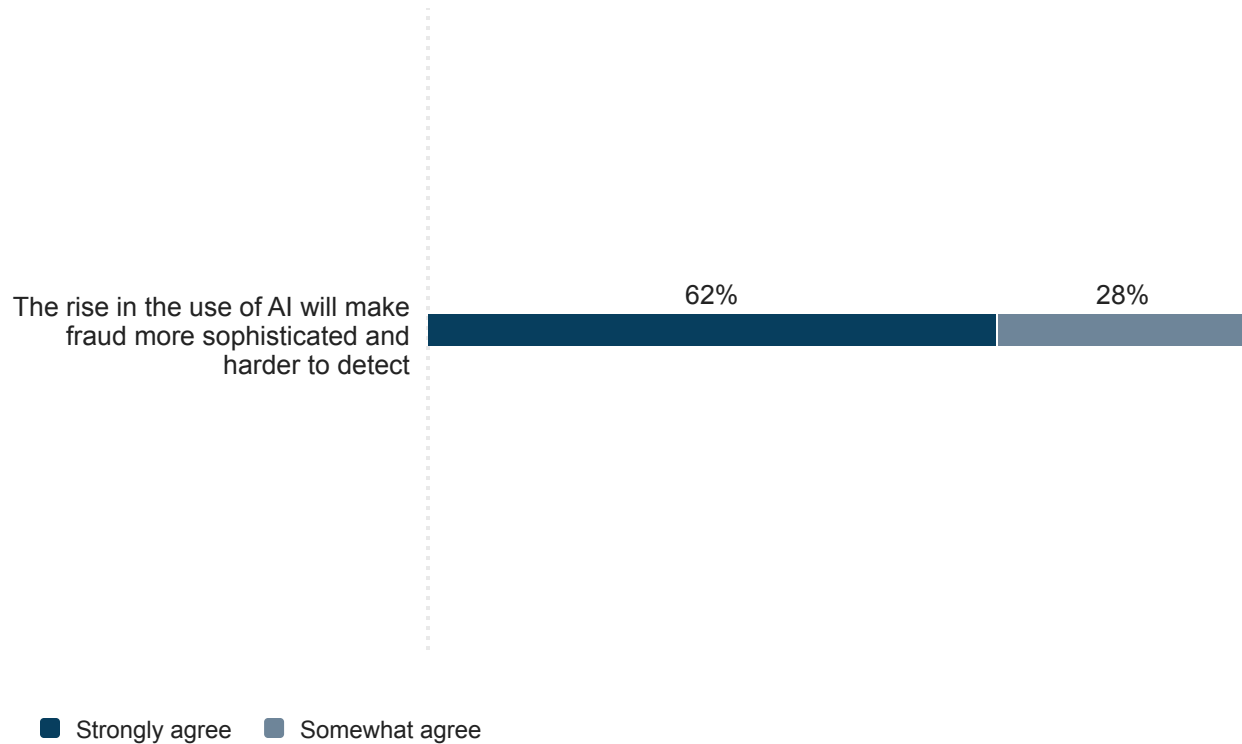
Fraud causes more than just financial losses; it extends into several critical areas that significantly impact business operations. For businesses, the most substantial non-financial costs include the time required to manage the situation (76%) which diverts resources from essential business tasks.

Moreover, dealing with fraud has a negative emotional impact (51%) which can create a challenging work environment, adversely affecting decision-making and workplace morale (23%). The resulting decline in staff morale is particularly concerning, as it can reduce employee engagement and productivity.

Additionally, other non-financial impacts include a reduced acceptance of payment methods (e.g. credit cards and large bills) and strained relationships with suppliers or clients.

Rising fears: 90% of business owners see **artificial intelligence** as a game-changer for more sophisticated fraud

Business owners' perspectives on AI-driven fraud



Source: CFIB, Your Voice – August 2024 survey, n = 1,945.

Question: To what extent do you agree or disagree with the following statements regarding business fraud? (Select one for each line)

Business owners are increasingly concerned about the evolving threat of AI-driven fraud, with an overwhelming majority (90%) fearing that AI will make fraud more sophisticated and harder to detect.

AI-driven fraud has the potential to evolve rapidly, making it more challenging for businesses to keep up with the latest threats. For example, fraudsters can leverage AI to personalize their schemes — such as generating fake emails, creating deepfake videos, and executing targeted phishing schemes — further exacerbating the risk of businesses falling victim to fraud and amplifying potential financial losses.

Fraud prevention practices used by small businesses

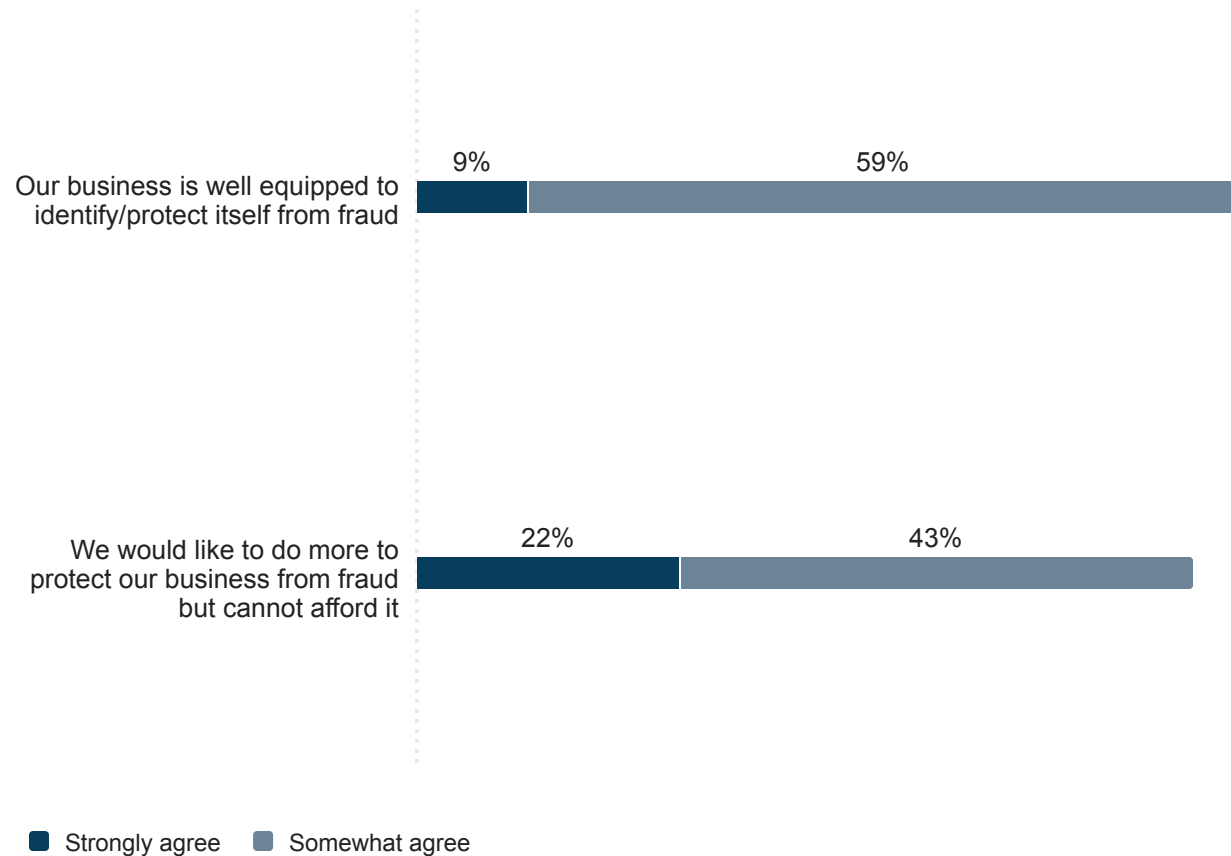
“We no longer mail cheques [to vendors from our outgoing mailbox due to past fraud incidents where cheques were stolen and cashed by third parties]. We take all cheques to the post office, resulting in additional tasks and loss of productivity.”

Professional services business, ON

”

Confidence in fraud prevention practices is moderate, resource constraints limit further action

Business owners' perspective on their fraud prevention practices



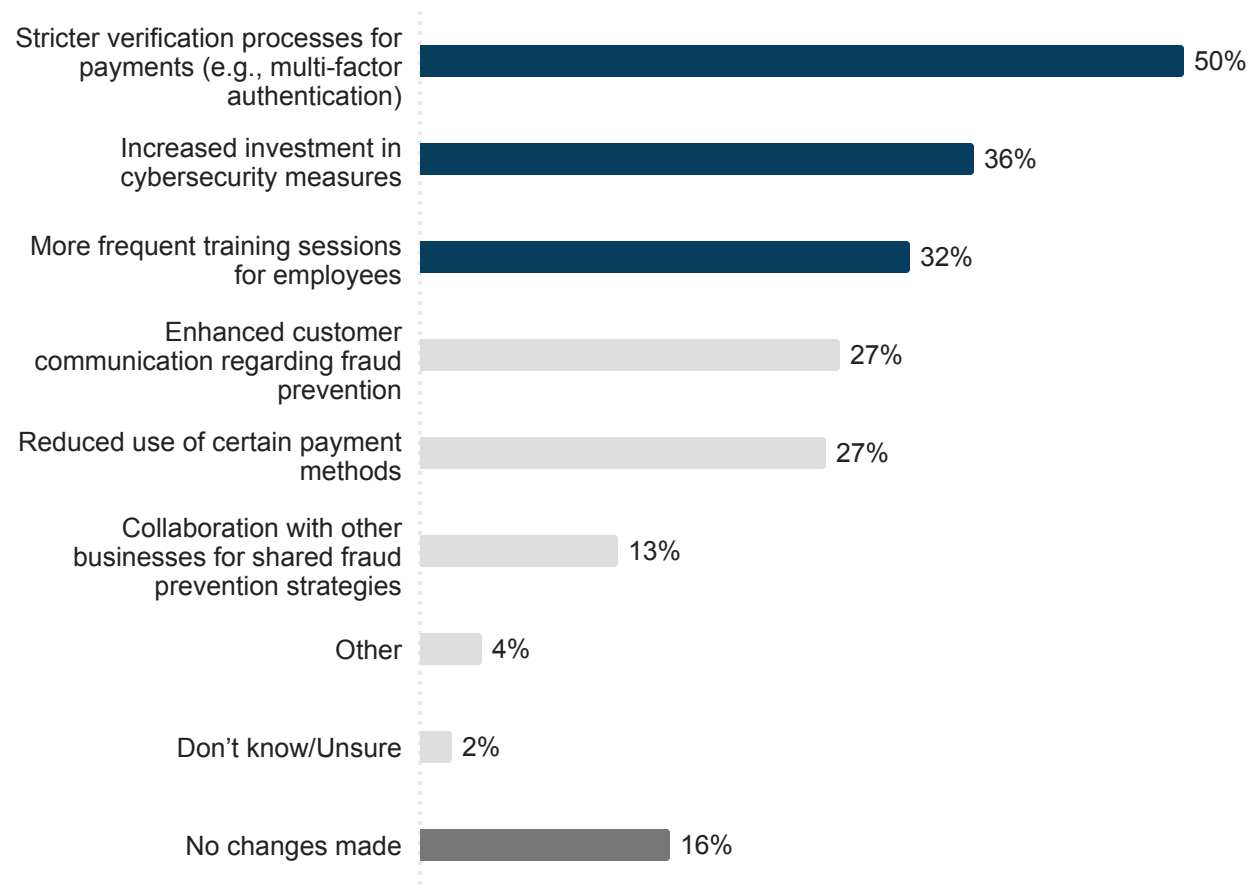
While business owners are increasingly concerned about the evolving threat of fraud, many (68%) still feel confident in their current defenses. However, there is a clear recognition that additional protective measures are necessary, though most small businesses (65%) are limited by resource constraints, preventing them from taking further action.

Source: CFIB, Your Voice – August 2024 survey, n = 1,945.

Question: To what extent do you agree or disagree with the following statements regarding business fraud?
(Select one for each line)

Majority of businesses have implemented fraud prevention measures, with varying approaches

Fraud prevention practices used by small businesses to address fraud*



Of the businesses that have encountered fraud, the majority (82%) have some measure in place to protect their business from fraud/scams.[4] Businesses are adopting a comprehensive approach to fraud prevention, with a strong emphasis on securing payment processes through stricter verification methods (50%) and bolstering cybersecurity measures (36%). Employee training (32%) plays a key role in these efforts, aiming to enhance awareness and preparedness against potential threats.

Source: CFIB, Your Voice – August 2024 survey, n = 969.

Question: Has your business made any of the following changes to its practices or policies to address fraud? (Select all that apply)

Note*: Includes responses from businesses that encountered fraud within the past 12 months.

[4] All options were multi-categorical with the exception of "No changes made" and "Don't know/Unsure." Given that 18% of respondents chose these options indicates that 82% of respondents made at least one specific change in response to fraud concerns.

Recommendations

For government

- Enhance the Code of Conduct for the Payment Card Industry in Canada ensuring accountability to merchants through a fair, transparent and competitive payment landscape in Canada. This includes implementing improvements to complaint handling processes for merchants, such as the process of challenging chargebacks.
- Making sure resources are allocated adequately to “cyber policing” and reporting yearly outcomes with specific numbers for small businesses.
- Providing small businesses with financial assistance (tax credit, grants, or low-interest loans) to help them invest in I.T. security.
- Proactively sharing information on existing resources and best practices with businesses and associations.
- Providing advice specifically tailored to SMEs on preventing cyberattacks.

For business owners

- Reach out to CFIB’s Business Advisors for assistance in addressing/preventing cyberattacks.

Call: 1-833-568-2342

E-mail: cfib@cfib.ca

- Visit [Interac.ca/fraudfighters](https://interac.ca/fraudfighters) for tips and best practices on how to protect your business and payments.
- To report fraud, contact the Canadian Anti-Fraud Centre, the RCMP or your local police department.

Methodology

The data for the analysis in this report was collected through CFIB's *Your Voice* survey conducted in August 2024.

Survey details

Type: An omnibus, controlled-access online CFIB survey.

Active dates: August 8 - 21, 2024

Participants: Results are based on responses from 2,340 CFIB members who are owners of Canadian independent businesses, from all sectors and regions of the country.

Statistical reliability: For comparison purposes, a probability samples with the same number of respondents would have a margin of error of +/-2.0%, 19 times out of 20.

Authors

Marvin Cruz

Director, Research
marvin.cruz@cfib.ca



Alchad Alegbeh

Research analyst
alchad.alegbeh@cfib.ca



Additional information

All CFIB research



cfib.ca/research



[@CFIB_FCEI_Stats](https://twitter.com/CFIB_FCEI_Stats)



research@cfib.ca

