BBB® STUDY:

How impostors, stolen data and fake services cost businesses billions

BBB

ISSUED: JUNE 2025

INTRODUCTION

Every day, businesses juggle dozens of tasks. From supervising employees to balancing books, days are jam-packed with details large and small.

Since 2022, Better Business Bureau (BBB) received over 3,600 reports from businesses encountering scams in the course of everyday business. Stories ranged from light nuisances, such as incessant spam emails, to complete disruption, like scammers holding data for ransom. In nearly every report, fraudsters show little regard for how their schemes could affect the livelihood of countless business owners and their employees.

And the cost is high. Federal agencies report that billions of dollars are lost annually, and the methods used grow in sophistication and number each year. Many businesses expressed dismay when encountering scams, especially those that cost them significant amounts of money. However, there are ways to fight back against scammers.

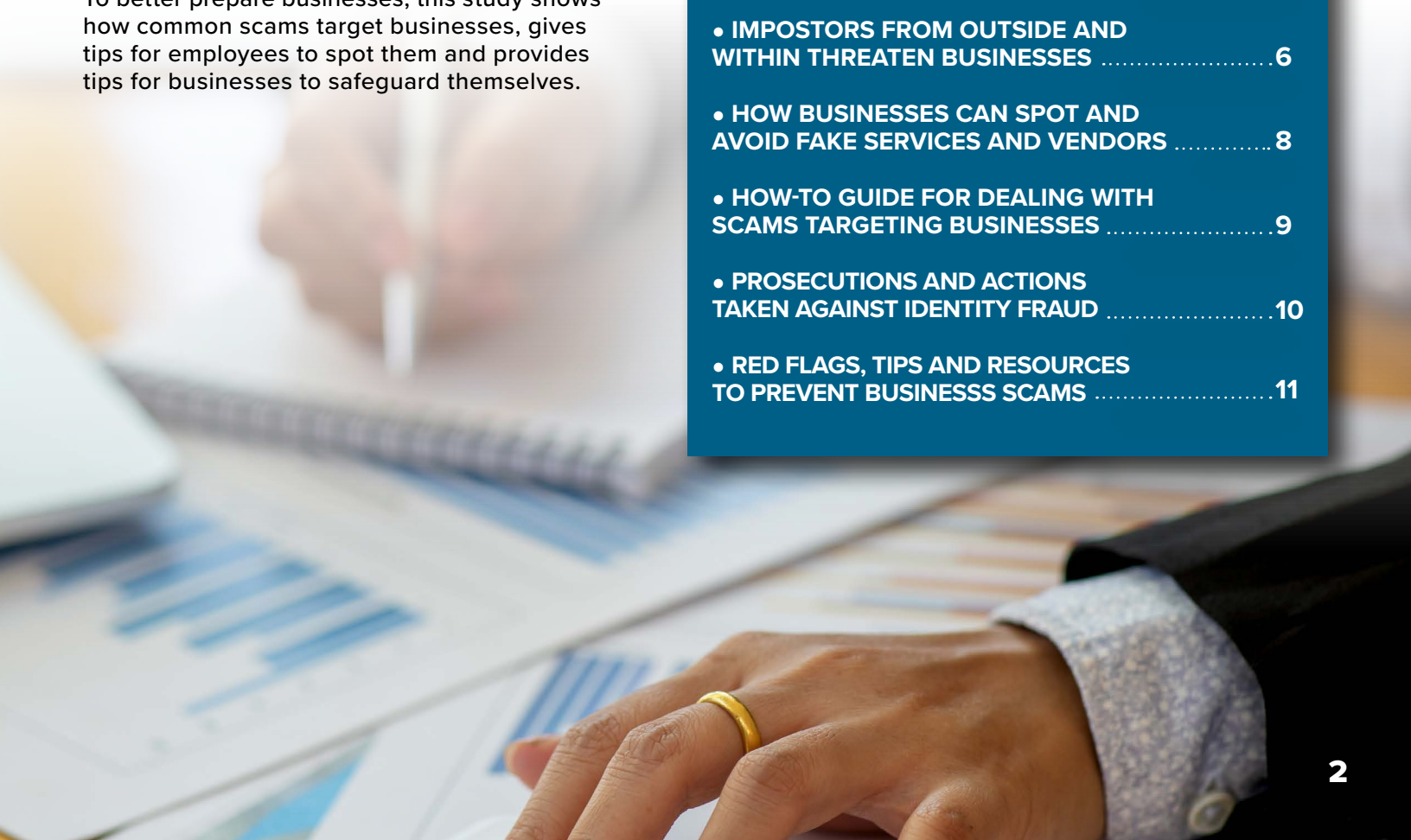
To better prepare businesses, this study shows how common scams target businesses, gives tips for employees to spot them and provides tips for businesses to safeguard themselves.

ABOUT THIS STUDY

This work focuses on patterns of reports from the public about scams they have encountered. Through an analysis of the reports, BBB studies are intended to give consumers, businesses, news media, researchers and regulatory agencies an in-depth understanding of:

- **How these scams work**
- **How to avoid them**
- **What is being done to help curb fraud**

CONTENTS



HOW COMMON ARE BUSINESS SCAMS?

Business scams are becoming ubiquitous. Almost 80% of companies dealt with attempted fraud in 2024, according to one report.

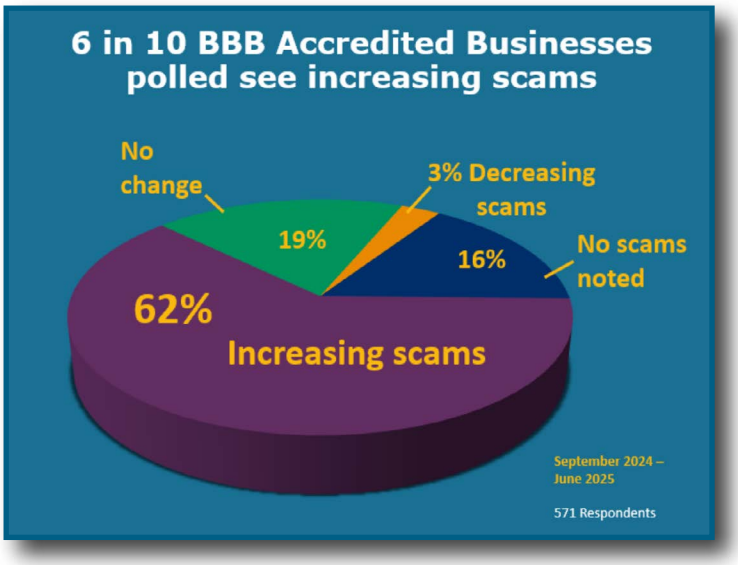
Due to the wide variety of methods and ruses scammers use, savvy companies need to be on the lookout for various types of scams. The variety of frauds makes it hard to track the true scale of business scams in North America.

BBB Scam Tracker℠ reports showed tactics involving the impersonation of executives, data breaches, ransomware, fake consultants, vendor impersonations and many more. These frauds reach into every aspect of a business, putting each employee and executive at risk of falling for a scammer's ruse.

While there were several thousand cases reported to BBB, those numbers are likely a vast undercount, according to one study using FTC data. Available cases do indicate a rise in reports since 2022, however, and business owners told BBB the crippling effects fraud can have on their lives.

One **wholesale food seller** in **Connecticut** reported to BBB about a scam in April, in which their company sent nearly $390,000 worth of product to a known client and reputable company. When the wholesaler didn't receive payment, they reached out to their client. It turned out that their client's business identity had been stolen, and the orders were fraudulent. The ruse was elaborate. Scammers used the client's invoice documents, company logos and important non-public contact details.

The theft didn't stop there. The wholesaler said they were surprised to learn the scammers used fraudulent transcations to steal their information as well. The criminals were now impersonating both the wholesaler and their clients to other companies.



"We have our local law enforcement, and the Federal Bureau of Investigation (FBI) involved because this person or persons is still perpetuating the scam under our name now as well as many other produce and food establishments," said the owner.

Over 60% of businesses reported being targeted by scammers, according to a poll of over 500 BBB Accredited Businesses (above). The majority said scam attempts had increased in recent years.

An Identity Theft Research Center report showed nearly three-quarters of scam reports indicated losses of $250,000 or more in 2024. For some types of scams, the amounts were lower but still caused harm.

The cost of an average data breach in the United States in 2024 was estimated to cost a business $4.9 million, according to IBM.

BBB SCAM TRACKER℠ REPORTS

YEAR	REPORTS	MEDIAN LOSS	SUSCEPTIBILITY
2023	1,346	$1,250	27%
2024	1,796	$1,200	29%
2025 (through May)	505	$838	32%

HOW COMMON ARE BUSINESS SCAMS?

The U.S. Chamber of Commerce's Small Business Index survey revealed that 60% of small business owners — who mostly run companies with fewer than 100 employees — said cybersecurity threats are a top concern.

A report from Mastercard found, "These businesses are often too small to hire IT or cybersecurity specialists, and business owners wear too many hats to keep track of the latest updates or research the best network monitoring software."

American Bankers Association President and CEO Rob Nichols called for stronger national protections against fraud this year at a summit in Washington, saying fraud presented an "insidious threat." He suggested a coordinated, national strategy that includes government and private businesses.

"They need to stop scammers from reaching vulnerable consumers through fake social media profiles, spam calls, text messages and emails," Nichols said. "Right now, it's still too easy for the bad guys to spoof a bank name on a caller ID, email or text."

Securing customers' data is imperative for businesses. Not only does it increase trust among consumers, but a patchwork of federal requirements for certain industries and additional state laws makes protecting data a legal mandate. At least 20 states have rules and regulations outside of the federal government, and companies must continually educate themselves to stay compliant.

"Many companies keep sensitive personal information about customers or employees in their files or on their network," according to the Federal Trade Commission (FTC). "Having a sound security plan in place to collect only what you need, keep it safe, and dispose of it securely can help you meet your legal obligations to protect that sensitive data."

Understanding the different ways scammers target businesses can be difficult, so BBB broke down the vast array of scams into three separate categories: stolen data, impersonation, fake services.

HOW DATA BREACHES AND STOLEN INFORMATION COST BUSINESSES

When data is stolen from a business, the results are costly. One of the most common types of scams is when fraudsters "break into" a company's data storage system. This is called a data breach.

A breach operates in two parts. First, the information is stolen. After that, scammers leverage it to commit various types of fraud, like business identity theft, or they use it to outright steal funds by breaking into accounts.

Over the last three years, the Federal Bureau of Investigation (FBI) reported nearly $1.4 billion in losses related to data breaches across the United States. North America experienced several significant instances in 2024.

In May, a hacker associated with the cybercrime group ShinyHunter told a news organization that telecommunications company AT&T paid over $300,000 to recover stolen phone records after the hackers breached an unsecured cloud storage system. The group struck again in June, when Ticketmaster informed 560 million customers their information had possibly been compromised. ShinyHunters again claimed to hold the data, putting it up for sale for $500,000. Later investigations revealed the thefts were made possible by a chain of data security failures across several companies.

In Canada last summer, hackers infiltrated the system of Suncor, one of the country's largest energy companies. They perpetrated what is known as a ransomware attack, where scammers enter a company's computer system and lock it from use until a company has paid a ransom.

Government agencies aren't safe from breaches either. In October, the Canada Revenue Agency was hacked, and 28,000 Social Insurance Numbers were exposed. One report showed scammers using the stolen numbers to file fraudulent tax returns under the names of the victims.

FBI INTERNET CRIME COMPLAINT CENTER DATA BREACH STATISTICS

YEAR	REPORTS	TOTAL LOSSES
2022	2,795	$459 million
2023	3,727	$534 million
2024	3,204	$365 million

IMPOSTORS FROM OUTSIDE AND WITHIN THREATEN BUSINESSES

Deception is a major factor in all business scams, especially those involving impersonation. Ruses come in several forms, but they can neatly be divided into two categories: external and internal impersonation. **External scams** involved fraudsters pretending to be known and unknown vendors, government agencies, compliance agents and internet service companies. In these cases, the scammers want to fool a business owner or employee into handing over important information or cash before their disguise is figured out.

Several reports to BBB involved the impersonation of a government certification service sent through the mail to new and existing business owners.

Elise in **Fort Lauderdale, Florida**, told BBB she received a deceptive letter in the mail shortly after starting her business.

"The letter came shortly after registering our new business with the state of Florida. They attempted to solicit us for a Certificate of Status which we had already purchased through the official government agency and were waiting for."

One **business** in **Virginia** told BBB it was approached by a trademark protection company, which said the business's name was at risk of being taken over by another party. To stop this, the business paid nearly $24,000 over two-and-a-half years to the trademark protection company. Eventually, the business owner realized it was a scam and tried to cut off contact by blocking the scammers' numbers. "The phone numbers continuously change," the business owner said. "They currently tell me I owe them $1,800."

BBB received over 120 reports related to trademark scams, a common and costly fraud.

Phishing scams often provide information for scammers to use in deceptions as well. When a fraudster identifies a company which focuses on business-to-business transactions, they will trawl through their email and phone contacts and attempt to scam the associated companies through fake contracts and hijacked payment systems.

BBB received over 300 reports of impersonations, many involving vendor fraud.

Jaclyn in **Seattle, Washington**, told BBB a scammer impersonated one of her company's subcontractors. The spoof was convincing, she said, mirroring both the contractor's email and invoices.

"It was a very elaborate scam with little to no spelling or grammar errors. They followed up on the request as well and even provided the ACH information they wanted us to send the money to," she said.

Business identity fraud is widespread. BBB wrote in February about impostor scams where fraudsters stole the information of car sellers across the country and used it to scam consumers. BBB Wisconsin tracked a case where a scammer stole the information of a luggage and travel gear website, cloning their listings on a separate website, offering the products at extreme discounts and stealing money from consumers once it was sent.

CANADIAN ANTI-FRAUD CENTRE REPORTS

YEAR	VENDOR FRAUD REPORTS	TOTAL LOSSES	SPEARPHISHING REPORTS	TOTAL LOSSES
2022	3,273	$3.5 milion	1,575	$58 million
2023	1,461	$4 million	1,275	$59 million
2024	760	$8.3 million	937	$67 million

IMPOSTORS FROM OUTSIDE AND WITHIN THREATEN BUSINESSES

When hackers gain access to a company's file or communications systems and pretend to be employees, these **internal impersonations** can be costly.

The most common scam type businesses encountered last year, according to the Association of Financial Professionals (AFP), was business email compromise (BEC). This scam, where the perpetrators use a company's email system to impersonate executives or other high-ranking employees, made up 65% of the reports to AFP.

The FBI reported a staggering amount of monetary loss from 2022-2024, with reports showing $8.4 billion stolen through BEC scams.

The Royal Canadian Mounted Police (RCMP) warned businesses in Canada about BEC scams as well.

"By leveraging existing business relationships between the person receiving the email and the person sending it, the criminal, pretending to be the trusted sender, will use various means to convince the recipient to send money or share financial information. BEC is one of the most financially damaging online crimes," the RCMP said.

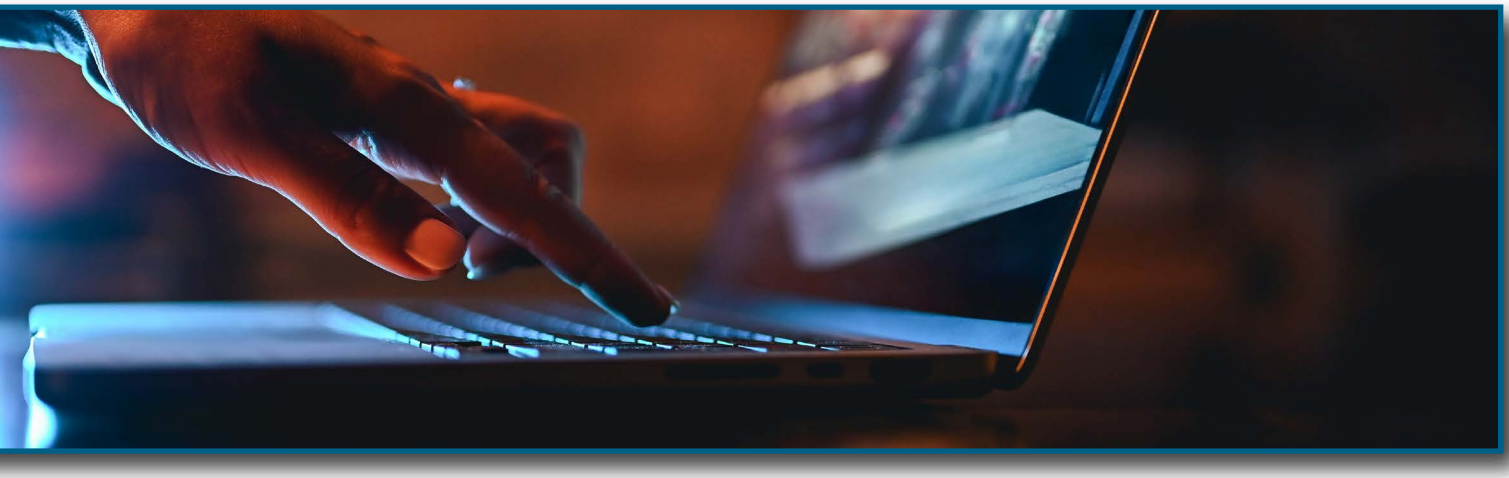
Several reports from Canadian businesses in British Columbia and Saskatchewan reveal no organization is immune from impersonation.

It is vital to provide tips to the public and business owners if your organization has ever been impersonated. BBB has extensive resources online to combat these scams.

The Better Business Bureau is not immune to being victims of impostor scams. Some impostors falsely act as BBB to steal information and money from businesses.

FBI INTERNET CRIME COMPLAINT CENTER BEC STATISTICS

YEAR	REPORTS	TOTAL LOSSES
2022	21,832	$2.7 billion
2023	21,489	$2.9 billion
2024	21,442	$2.8 billion



HOW BUSINESSES CAN SPOT AND AVOID FAKE SERVICES AND VENDORS

With so many aspects of a business to juggle, many owners look for ways to simplify their lives. Scammers know this, and they now offer a multitude of fake services. As nearly every business now has a website, scammers have keyed into the domain registration process. Over 40 reports to BBB show a barrage of fake letters, emails and outreach where scammers attempt to sell fake domains to businesses.

Casey in **Owosso, Michigan**, told BBB he received an offer for a domain for his business. The only issue? He already owned it.

"Initially, I thought someone was trying to 'sell' my domain to me or renew my domain. It just struck me as very predatory and, if sent to the wrong person, very confusing since it is presented like a bill or late notice."

Another report involved a **wedding and event planner** in **Mechanicsville, Virginia**. She told BBB a company reached out to her, saying she owed them for online advertising. But the business owner had never contacted any company for advertising.

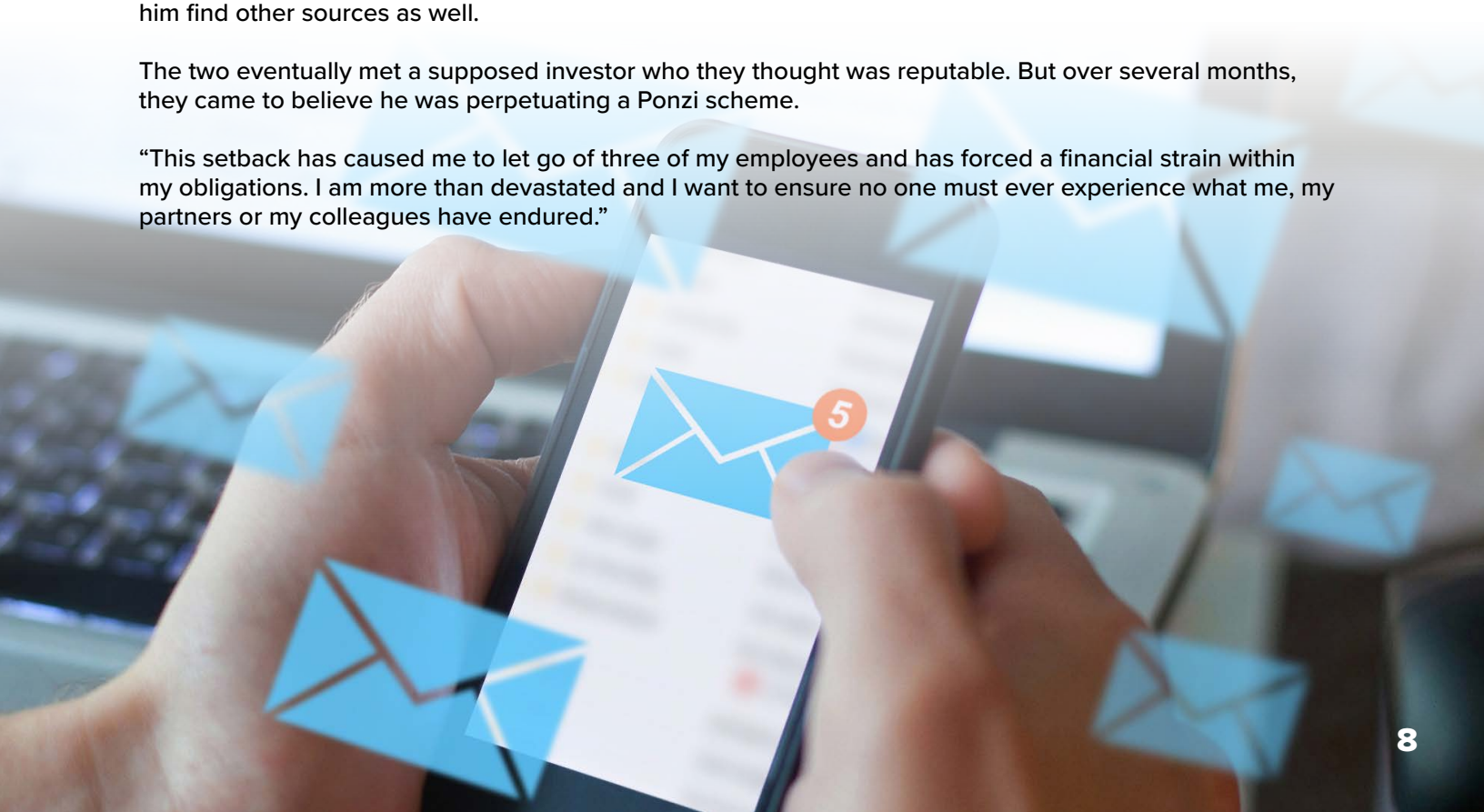
"I ignored several emails from them. They sent another reminder email. I found out through looking them up on Facebook and Instagram that this has happened to hundreds of other small businesses throughout the U.S. and Canada."

When fake services are convincing enough, the effects of their schemes can devastate the finances of a business, sometimes before ever launching.

One **accountant and business advisor** in **Atlanta, Georgia**, told BBB she worked with fledgling business owners to get off the ground. She talked with a veteran who hoped to get funding for his business, and they approached their city's government. The city couldn't commit to funding but supported the idea and asked them to find investors. The advisor decided to invest $150,000 in the company herself, while helping him find other sources as well.

The two eventually met a supposed investor who they thought was reputable. But over several months, they came to believe he was perpetuating a Ponzi scheme.

"This setback has caused me to let go of three of my employees and has forced a financial strain within my obligations. I am more than devastated and I want to ensure no one must ever experience what me, my partners or my colleagues have endured."



HOW-TO GUIDE FOR DEALING WITH SCAMS TARGETING BUSINESSES

To protect from scams

Stolen Data

- Train employees to use strong password protection
- Require the use of multifactor authentication
- Install security measures on individual devices and across IT network
- Consider hiring IT specialists or consultants

Impersonation

- Don't trust caller ID
- Verify invoices over the phone or in-person whenever possible
- Never pay with cryptocurrency or person-to-person payment services
- Know that government groups never use intimidating tactics
- Avoid grants that require payment to access

Fake Services

- Use WHOIS and other website verification tools
- Make sure websites are secure
- Never give out company information for "free" services

If your business has been subject to a scam

Stolen Data

- Move quickly to avoid further damage
- Secure systems and fix vulnerabilities
- Hire an independent forensics team
- Consult with legal counsel

Impersonation

- Contact your financial institution if money has been exchanged
- Reach out to the impersonated business/ government group
- Report to authorities
- If found through advertisement, flag them on the platform
- Contact your website hosts if yours was stolen
- Recover phone numbers, emails and any other stolen information from scammers
- Contact customers to inform them of impersonation of your business

Fake Services

- Contact your financial institution if money has been exchanged
- Report to authorities
- If found through advertisement, flag them on the platform

PROSECUTIONS AND REGULATORY ACTIONS

The Department of Justice (DOJ) and the FBI work to disrupt and stop business scammers, saving millions in the process.

In February, the DOJ announced charges against two Russian nationals that allegedly operated the Phobos cybercrime group. Phobos victimized over 1,000 public and private entities worldwide and extorted over $16 million in the process.

Whenever possible, the government has attempted to restore information and stolen funds.

Back in 2022, U.S. government agents pulled off an infiltration of their own to save stolen data. It began when the FBI tracked and entered into the systems of a ransomware group named Hive. The hackers, having stolen several victims' information, hid it behind encryption and demanded payment for the data. The FBI cut off that process and recovered the keys to the encryption, handing them back to the people whose data was stolen and saving over $130 million in the process.

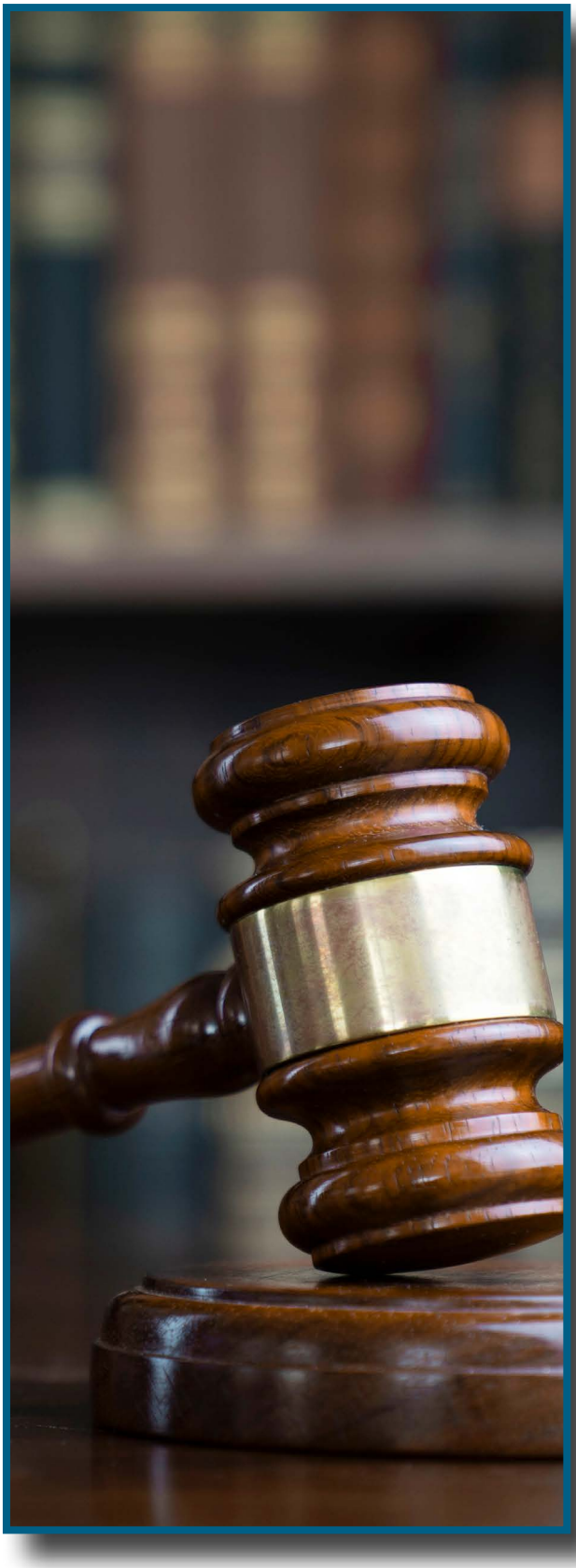
"The Justice Department will spare no resource to identify and bring to justice, anyone, anywhere, who targets the United States with a ransomware attack," said then-Attorney General Merrick B. Garland.

Companies are subject to strict regulations, especially around customer data, and the failure to adequately protect information from scammers can lead to penalties.

Last summer, two consulting companies paid over $11 million in fines for failing to adequately protect citizens applying for housing assistance during the COVID-19 pandemic. In 2023, a rideshare executive was ordered to pay $50,000 and received three years' probation for a coverup of a data breach which involved millions of customer records.

Overseas, where restrictions are even more stringent, failure to secure customer data has led to massive penalties. Ireland fined Meta $1.3 billion in 2023, and Luxemburg ordered Amazon to pay $877 million two years prior.

Government agencies can also receive penalties. As a result of the Canada Revenue Agency breach, the country launched an investigation, which is ongoing.



RED FLAGS, TIPS AND RESOURCES TO PREVENT BUSINESS SCAMS

Red flags: Learn these signs

- Unknown businesses, government agencies and big-ticket buyers
- Invoices from unexpected emails
- Odd behavior from "known" vendors or businesses
- Requests for gift card or pre-paid debit card payments
- Urgent demands to renew or file applications for trademarks
- Claims about expiring domain names
- Consultants making big promises about helping your business

BBB's tips to avoid business scams:

- Train employees to recognize scams
- Double check invoices and payments before sending
- Verify vendor contact information
- Establish payment procedures
- Avoid wire transfers, pre-paid debit cards and gift cards whenever possible
- Maintain good records to compare against fraudsters' claims
- Don't trust caller ID or names associated with emails
- Research unknown companies asking to do business
- Decide whether to sign up for a dark web scanner
- Install firewalls, multifactor authentication and other security measures
- Obtain verification on social media profiles
- Find more tips and resources at BBB's Business Scam HQ

Where to report business scams:

- Better Business Bureau Scam Tracker
- Federal Trade Commission (FTC) or call **877-FTC-Help**
- Federal Bureau of Investigation (FBI) or call **(202) 324-3000**
- Canadian Anti-Fraud Centre - or **1-888-495-8501**
- Find your state's Attorney General online

Acknowledgements

This study is a joint project of Better Business Bureaus of Chicago, Dallas, Omaha, San Francisco and St. Louis.

Contributions include data from **BBB Scam Tracker, BBB Institute for Marketplace Trust, IABBB** and various regulatory agencies.

BBB International Investigations Initiative

- BBB Chicago - bbbinfo@chicago.bbb.org
- BBB Dallas - info@nctx.bbb.org
- BBB Omaha - info@bbbinc.org
- BBB San Francisco - info@bbbemail.org
- BBB St. Louis - bbb@stlouisbbb.org

By Brian Edwards, BBB International Investigations Specialist - bedwards@bbbinc.org

Find more information about this study and other BBB scam studies at BBB.org/scamstudies.

BBB's mission is to be the leader in advancing marketplace trust. We do this by:

- Setting standards for marketplace trust
- Encouraging and supporting best practices by engaging with and educating consumers and businesses
- Celebrating marketplace role models
- Calling out and addressing substandard marketplace behavior
- Creating a community of trustworthy businesses and charities

Image Credits: Getty Images

BBB