Safeguard®

GUIDE TO PROTECTING YOUR BUSINESS

VT44GPBW

As a small business owner, fraud is a significant threat to your business. According to a 2012 study by the Association of Certified Fraud Examiners, the smallest organizations suffered the largest median losses. Small businesses typically employ fewer anti-fraud controls than their larger counterparts, which increases their vulnerability to fraud. The following questions and answers should help you protect your business from fraud.

"Over 1.2 billion fraudulent cheques are written every day."

1. DO YOUR CHEQUES HAVE HIGH-SECURITY FEATURES SUCH AS HOLOGRAMS OR HEAT-SENSITIVE INK?

They should, because over 1.2 billion fraudulent cheques are written every day. More than one-fourth of all small business fraud involves cheque tampering, making it a much more common method of fraud than in larger organizations. The good news is, there are precautions. Take Safeguard Premium Secure cheques, for example. Affordable and easy to use, they are designed specifically to protect your business transactions and assets from fraud. Our high-security cheques are equipped with the latest technology and make it virtually impossible to alter cheques through washing or counterfeiting. Here are more actions you can take to avoid cheque fraud:

- Choose "signature required" when receiving new cheques to avoid them being intercepted
- Always store your cheques in a safe, secure location
- Destroy unused cheques from closed accounts immediately
- Control access to your company's accounts payable areas and systems
- Require secure password processes for employees who write and issue cheques
- Balance your accounts daily to detect abnormalities in a timely manner
- Use a 12-point or larger font for printed cheques and a security pen for handwritten cheques

2. DO YOU KEEP ALL HARD COPIES FOR YOUR BUSINESS UNDER LOCK AND KEY?

All of your company information, records and unused cheques should be safely tucked away in a secure, locked location. Only trusted employees should have access to the keys. Copies of critical documents should be duplicated with one copy in a separate location.

3. DO YOU KNOW YOUR BANK'S POLICY REGARDING DISTRIBUTION OF FUNDS AND UNDERSTAND YOUR LIABILITY IN THE CASE OF CHEQUE FRAUD?

If you're running a business, it's vitally important to read and understand your bank contracts regarding liability for fraud under the Uniform Commercial Code. This is not always easy to find, so be sure to look at the fine print of your deposit account agreement. In particular, focus on your bank's policy about making the funds available to you that might be subject to a fraud hold. For instance, let's say you are a victim of cheque fraud totaling $50,000. Some banks release the funds immediately so you can continue to use them for your business. Other banks freeze the funds until the investigation is complete, which can take up to 120 days. Depending on the amount of fraud, this could have a disastrous effect on your cash flow. Here are a couple of things you can do to protect yourself:

"Fraud against bank deposit accounts cost the industry $1.744 billion in losses in 2012."

- Look into efficient, easy-to-use security protection services like EZShield®. Regardless of your bank's policy, this service provides you with a security expert if you fall victim to cheque fraud and helps you restore your business to pre-theft status. When you order Premium Secure cheques from Safeguard, EZShield Premium Cheque Fraud Protection is automatically included, at no additional charge.
- Reduce your chances of fraud by using high-security cheques. In a 2012 ABA Deposit Account Survey Report, 16.3% of banks required businesses to use high-security cheques — and this number will continue to grow.

You should also understand how and when your bank alerts you about unusual activity on your account. Fraud against bank deposit accounts cost the industry $1.744 billion in losses in 2012, according to ABA estimates. Debit card fraud accounted for more than half of 2012 losses: 54%, followed by cheque fraud: 37%. Here are some helpful tips for preventing online fraud:

- Beware of sophisticated banking Trojan programs that creep onto your computers, steal bank logins and drain your bank accounts.
- Monitor bank accounts constantly. The faster you spot inconsistencies, the better.
- Get your bank to help. Most provide free instant alerts to warn you about unusual account activity.

4. DO YOU DESTROY ALL EXPIRED COMPANY DOCUMENTS WITH A CROSS-CUT SHREDDER?

Experts often recommend that you shred bills, tax documents, credit card and bank account statements, and other items that could easily be used by thieves to commit fraud or identity theft. Even recycling bins are not reliable sources of security, so just to be safe, you might want to institute a shred-all policy. And, if you're a business traveler, you should be careful not to leave sensitive documents in garbage cans, hotel rooms, airplanes or conference areas. More and more hotels are providing shredder services from third-party security vendors. If not, you can always take your sensitive documents to a location where you can properly destroy them.

You should always use a cross-cut shredder. Strip-cut shredders are the least secure. They use rotating knives to cut narrow strips as long as the original sheet of paper, which can be reassembled by a determined and patient thief. Cross-cut or confetti-cut shredders cut rectangular or other small-shaped shreds. This makes reconstruction exponentially more difficult, if not impossible.

5. DO YOU CHANGE PASSWORDS ON A REGULAR BASIS AND HAVE A POLICY THAT PREVENTS MULTIPLE PEOPLE FROM USING THE SAME USER NAME AND PASSWORD?

Password protection is essential in today's online world. Make passwords long and strong. Combine capital letters with numbers and symbols. Have separate passwords for each account, and change them often — at least every 60 days.

6. DO YOU MONITOR YOUR CREDIT AT LEAST ONE TIME PER YEAR?

It makes good sense to stay on top of your credit. Checking your credit history will alert you to unusual activity, which may be your first warning that your business is under attack. With that in mind, you can get a free credit report from either TransUnion or Equifax, by calling 1.800.465.7166, or by mailing your request form and photocopies of your required identification to:

TransUnion
Correspondence in English
TransUnion Consumer Relations Department
P.O. Box 338, LCD1
Hamilton, ON L8L 7W2

Correspondence in French
Centre de relations aux consommateurs TransUnion
CP 1433 Succ. St- Martin
Laval, QC H7V 3P7

Equifax
National Consumer Relations
P.O. Box 190, Station Jean-Talon
Montreal, QC H1S 2Z2
Fax: 514.355.8502

7. DO YOU HAVE A SOCIAL MEDIA POLICY THAT IDENTIFIES WHAT COMPANY INFORMATION EMPLOYEES CAN AND CANNOT SHARE ON FACEBOOK, TWITTER OR OTHER SOCIAL MEDIA?

"Identity thieves, hackers, business competitors and other predators are always on the lookout for easy prey."

If you allow employees to access social media sites such as Facebook and Twitter during work, make sure they keep their personal life separate from their work life. Why? Because anything posted to social media is "out there," so to speak. It's not private anymore. In fact, the more they reveal, the more vulnerable they — and possibly your company — become. No matter how safe a particular social medium seems, information can still be compromised, whether it be through their friends or the site itself.

Another concern is online attacks. Identity thieves, hackers, business competitors and other predators are always on the lookout for easy prey. With enough background material, they can impersonate anyone online and trick friends and followers into compromising company information. They can also gain access to restricted sites, inside and outside your business.

Make sure employees are careful about what they say and do online. Educate employees about how their online behaviour could impact the company.

8. DO YOU HAVE UP-TO-DATE ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE IN PLACE?

According to McAfee's *State of Security* Report, almost a third of small businesses have yet to purchase or implement many of the next-generation security technologies available in today's market. If this is true for your company, do it now — and when you do, be sure to get auto-updating security software.

9. IS YOUR DATA ENCRYPTED, AND DO YOU USE A SECURE CONNECTION FOR RECEIVING OR TRANSMITTING CREDIT CARD INFORMATION ACROSS THE INTERNET?

Many small businesses can't afford IT and security talent, which makes them very vulnerable. There are some simple steps you can take to protect yourself:

- Use anti-virus software and encrypted connections when transferring sensitive data. Look for https:// in the URL to know that it is safe.
- Keep your most sensitive data on the fewest number of computers and, if possible, segregate it from other data.
- Review your general liability insurance policy. Does it cover exposure related to cyber liabilities? There are now cyber-insurance policies available.

10. DO YOU DO BACKGROUND CHECKS ON ALL EMPLOYEES?

One study done by the Retail Council of Canada found that 87% of small and medium-sized businesses experienced some sort of theft, and nearly 50% of their theft was perpetrated by their employees. Here are easy ways you can protect your business:

- Before hiring new employees, verify their employment history, education and references, and perform criminal background checks, credit checks and drug screenings
- Create an environment of trust where employees feel comfortable stepping forward
- Consider making it easy for employees to provide information about questionable events or behaviour anonymously
- Watch for the most common types of fraud in small businesses: billing schemes, corruption involving an employee (bribery or conflicts of interest) and cheque tampering
- Conduct internal and external audits of financial statements and institute a code of conduct for employees

- Recognize red-flag behaviour of employees, such as living beyond their means, undergoing financial problems, developing an unusually close relationship with a vendor or customer, having control issues or exhibiting an unwillingness to share duties
- Implement anti-fraud controls, such as separation of duties, use of authorizations, job rotations and mandatory vacations

11. IS YOUR BUSINESS' WIRELESS NETWORK SECURED?

Wireless security is very important, as it is especially vulnerable to attacks. A hacker with a simple antenna can break into your network from a mile away. Make sure your company's wireless network is up-to-date and uses the current, standard WPA2 encryption. Add an additional layer of protection by using the MAC address filtering option in your wireless router.

"1.5 million adults become cybercrime victims every day."

According to the Xerox and McAfee Study of 2012, security is important for your printer network as well. Half of employees using a printer at work say they've copied, scanned or printed confidential information at work. Only 13% have been prompted to enter a password or code, so that might be a valuable step to implement.

12. IS YOUR SMARTPHONE SET UP WITH REMOTE TRACKING AND REMOTE WIPING TO ALLOW YOU TO ELIMINATE ALL DATA OFF YOUR PHONE IF IT IS LOST?

It should come as no surprise that mobile devices — much like personal computers and paper records — represent a potential vulnerability for our private information. More and more people use their smartphones to access banking and other financial information via the Internet. In fact, smartphones contain as much sensitive data as a laptop.

As technology continues to grow so does the risk of fraud. According to a 2012 Norton Cybercrime Report, 2/3 of the people surveyed do not use any type of security solution for their mobile device. With 1.5 million adults becoming cybercrime victims every day (that's 18 victims per second), protecting all of your devices and accounts should be your number one priority. App makers for smartphones are not making the task of stealing personal information nearly as difficult as it should be, meaning that many apps store sensitive data in unencrypted plain text. That means losing your smartphone could put you at a high risk for identity theft.

However, there are some precautions you can take, such as learning about security features and functions on your smartphone and using the strongest passcode protection available to lock your phone.

13. DO YOU HAVE A DISASTER RECOVERY PLAN IN PLACE IN THE CASE OF A NATURAL DISASTER OR CYBER ATTACK?

"According to the 2013 Javelin Strategy & Research Study, every two seconds identity fraud occurs."

According to McAfee's State of Security Report, six out of every ten large enterprises and two out of every three midsize companies have a formal disaster recovery plan. That drops to one out of every two for small businesses. Such plans are not that hard to implement: a plan can be as simple as security rules, guidelines and consequences for ignoring them. Here are some things to consider when formulating your best course of action:

- Conduct an inventory of your credit cards, employee Social Insurance numbers and customer databases. If you don't know what data you have, you can't protect it.

Preventing fraud is the key to protecting your small business. With the right tools and support in place — you can minimize the risk of fraud.

SAFEGUARD SECURE.

FIGHT FRAUD AND REDUCE RISK WITH SAFEGUARD SECURE® PRODUCTS AND SERVICES.

Contact your local Safeguard consultant for a complimentary cheque-fraud risk analysis.

To locate a consultant in your area, call 800.523.2422.