How to protect your business from cyber theft and payment fraud

ATB listens

After all the time, energy and hustle you've put into your business, you take pride in the reputation and success you've worked so hard to build. As you should!

So why allow cyber criminals to steal these from you?

The end goal of most cyber thieves today is to get their hands on money.

Your money.

If someone in your company opens a phishing email tomorrow,

do you have the right protections in place to detect a hacker who is spying on your systems?

To prevent a thief from seizing your network and demanding ransom?

To deter an embezzler from stealing your company's banking information and sending wire transfers to offshore accounts?

To prevent a crook from redirecting supplier payments to bogus accounts or stealing payroll from your employees?

On average,

1 in 4

Alberta businesses is a victim of fraud or attempted fraud.

Today, every business, every system, every device, every person is more vulnerable to cyber theft and payment fraud than they were last year. The frequency of successful cyber attacks is increasing at record speed. And with it, the value of what is being taken.

As you build your business, your customers, shareholders, employees, lenders and partners all expect your company to be reliable and secure.

The question is, how secure is it?

> “There are lots of ways businesses can protect themselves but in general they are only now starting to wake up to the seriousness of the problem.”

James Swanson
Partner, Miller Thomson LLP
2017 Calgary Technology Law Lawyer of the Year

This is no time to lose to thieves – it’s time for Alberta entrepreneurs to apply ingenuity and determination to win this race. In this white paper, the **Treasury and Payments Solutions team of ATB Financial shares timely and critical information about theft, payment fraud and other cyber threats that are harming Alberta businesses**, along with ideas and tips you can implement immediately to **protect yourself, your customers and your business**.

Organized cyber crime poses a huge threat to Alberta businesses

Someone in the company clicked in an email...

...immediately downloading spyware into the system and enabling hackers to gain administrative access. Apparently they spent some time spying on internal activities and emails.

One day, when the CEO was travelling, the cyber criminal sent a fraudulent email through the CEO's account to his assistant.

> "Please wire $200,000 immediately to this account. I'm about to board a plane so you won't be able to get hold of me. But it's urgent you do this right away."

The assistant wired the funds to the overseas account.

When the real CEO returned to the office, he knew nothing about it.

The funds were gone, and untraceable.

Cyber thieves use an entrepreneurial business model

To execute crimes, many cyber thieves use sophisticated business models – similar to those of entrepreneurs.

In fact, organized crime is the most prevalent type of cyber crime today, making it the most significant threat to Alberta businesses.

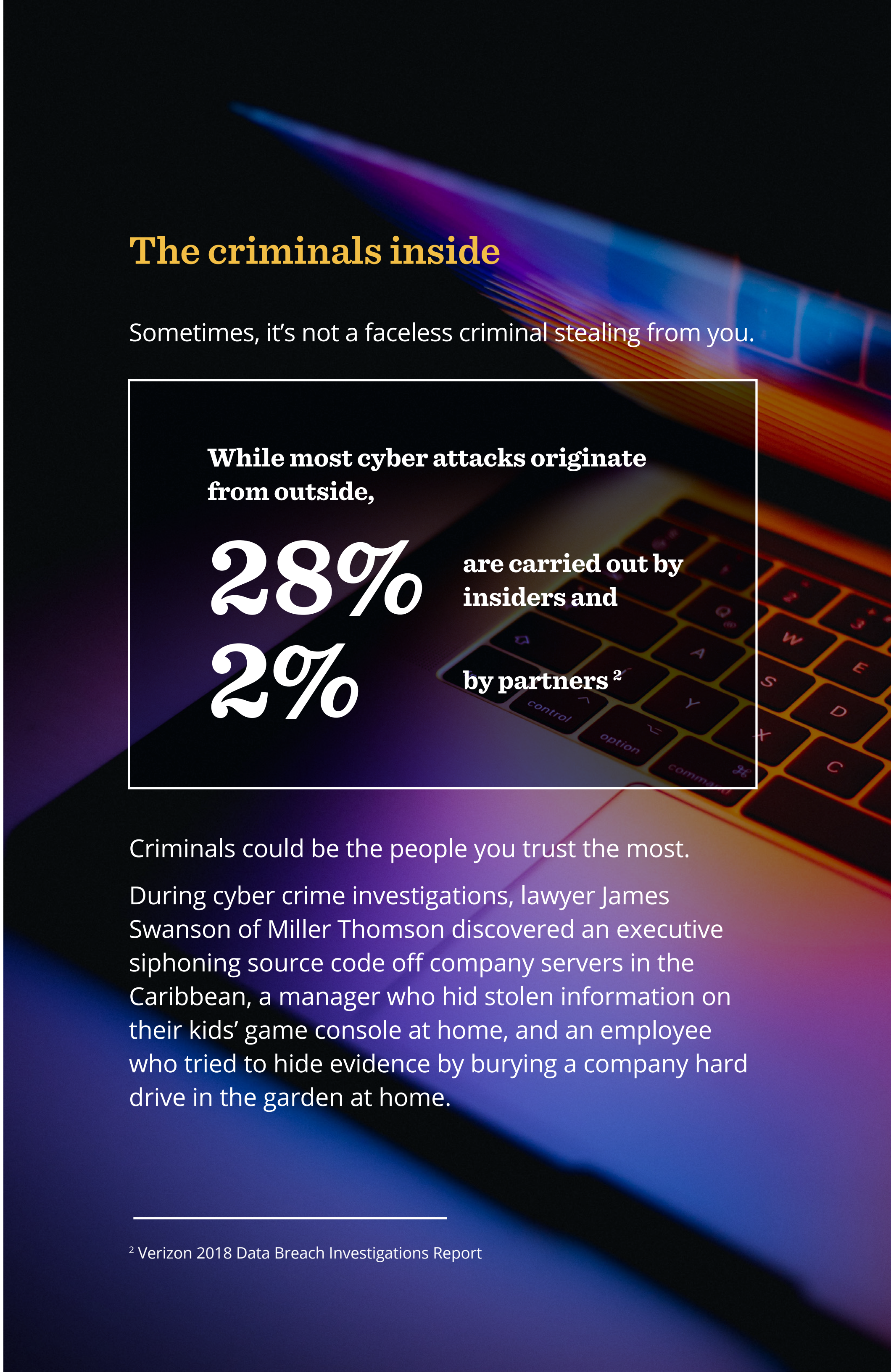
While casual attackers and nation states represent other significant types of external attackers, organized criminal networks accounted for 50% of all breaches in 2017.[1]

[1] Verizon 2018 Data Breach Investigations Report

Focused on "following the money," like entrepreneurs, they look for ways to increase revenue and maximize profits. Unlike traditional entrepreneurs, they do this by stealing from individuals and organizations.

Like their legal counterparts, criminals build their business models to achieve competitive advantage through specialization, innovation, quality or customer service. Many integrate divisions ranging from research and development, to sales and marketing, to finance and accounting.

These businesses are usually connected with sophisticated criminal networks. Within the underground marketplace, or dark web, these networks include salespeople who sell stolen data and exploit kits (hacking toolkits for cyber criminals to distribute malware or perform malicious activities by exploiting vulnerabilities in systems/devices), middlemen who facilitate criminal transactions and specialists who provide help desk support.



The criminals inside

Sometimes, it's not a faceless criminal stealing from you.

While most cyber attacks originate from outside,

28% **are carried out by insiders and**

2% **by partners**[2]

Criminals could be the people you trust the most.

During cyber crime investigations, lawyer James Swanson of Miller Thomson discovered an executive siphoning source code off company servers in the Caribbean, a manager who hid stolen information on their kids' game console at home, and an employee who tried to hide evidence by burying a company hard drive in the garden at home.

[2] Verizon 2018 Data Breach Investigations Report

What thieves want from your business

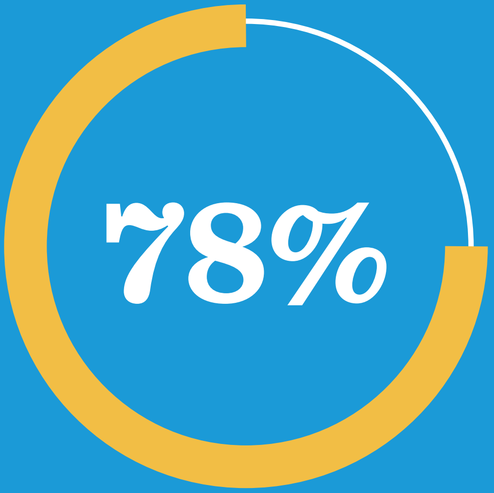
The 2018 edition of the globally respected Verizon Data Breach Investigations Report found that

76% of breaches were financially motivated

while gaining strategic advantage (espionage) was the motivation for **13%**

So money is usually the goal, and payments are especially vulnerable.

In its 2018 Payments Fraud and Control Survey, the Association for Financial Professionals found that



of the nearly 700 respondents said their organizations were hit by payments fraud.[3]

[3] 2018 AFP Payments Fraud Survey

The following are some of the most common types of payment fraud and cyber theft against businesses and the schemes criminals use to carry them out:

Cheque fraud is one of the oldest, and still the most common, forms of financial crime. There are many ways that thieves commit crimes with cheques:

- Duplicate cheques
- Stolen blank cheque stock
- Split deposit – fraudulent cheque deposited into victim's account and a portion requested in cash
- Forged endorsement – stolen cheques signed by someone other than the account holder
- Counterfeit – fake cheques that are not issued or authorized by legitimate account holders
- Altered – cheques that are intercepted and altered to change the beneficiary or amount
- Fictitious recipient – cheque issued to fictitious person or organization

Fraudulent vendor billing – an employee creates a shell company and pays it with company cheques

Payroll fraud – an employee accesses payroll records and simply changes their salary

Payroll system attack – a criminal steals credentials, logs in prior to a pay run and changes employees' bank details to those of fraudulent accounts

Fake invoices / invoice attacks – a hacker intercepts email correspondence, poses as a supplier and directs accounts payable to pay invoices to a new fraudulent account instead of to the supplier's genuine account

Corporate account takeover – a hacker accesses the bank or credit card accounts of a company and starts making charges

Electronic funds transfer / wire transfer fraud – an attacker gains access to a company's financial accounts and wires money to accounts they control

Extortion – hackers take over a network system and freeze it, offering to reinstate access after the company has paid a ransom

> **It's important to keep in mind that, like entrepreneurs, cyber attackers are innovative, continually evolving their techniques and tools.**

How criminals steal from your business

Many people believe maintaining the latest technology – like firewalls, hardware authentication, cloud systems – can protect an organization from intruders. But, says Justin Fong, Deloitte's Cybersecurity Leader for Western Canada, the fact is,breaches usually originate via people. Attackers are expert manipulators, able to trick people into breaking security procedures and protocols.

While employees are responsible for most cyber breaches, this is quickly changing. As more vendors and service providers touch sensitive data, third-party attacks (also called value chain or supply chain attacks) are becoming more common. Criminals are finding more ways to infiltrate systems through outside partners or providers with access to your systems and data.

Cyber attacks on supply chains increased

200%[4]

in 2017

[4] Symantec 2018 Internet Security Threat Report

These are some of the main ways that cyber thieves gain access to organizations:

Attacks can cause a lot of damage and continue for a long time.

68%

of breaches took months, or even longer to discover.[5]

[5] Verizon Data Breach Investigations Report

Hacking

- break into a computer or network

Phishing

- trick people into revealing sensitive information, like passwords and credit card numbers
- spear phishing targets specific people or departments
- whaling targets important people like company executives

Pharming

- redirect website traffic to a bogus website, usually a banking or e-commerce site

Spoofing

- impersonate another user to infiltrate systems
- email spoofing – email header that appears to be from someone the recipient knows
- IP spoofing – fake IP address that impersonates a trusted computer
- address bar spoofing – replaces legitimate address bar with a fake

Social Engineering

- gain access to systems by deceiving and manipulating people into breaking security procedures and best practices

Piggybacking

- access a network by using a legitimate user's connection, often when they don't log out

The cyber criminal's arsenal

Ransomware

malicious software (malware) that demands a ransom fee be paid after the software is installed on a computer system

Viruses

malicious code that replicates when people send it through emails, messages or attachments, and spreads to other computers by attaching itself to other computer files

Worms

self-replicating like a virus but doesn't require human assistance; can spread exponentially faster than a virus because it can clone and transmit itself

Spyware

malware that monitors computer activity and collects personal information like e-mail messages, usernames, passwords, credit card information

Trojans

malicious code or software that can take control of a computer and steal or cause damage or disruption

AND NOW... Artificial Intelligence

"Cyber criminals spend money on R&D just like legitimate businesses," says lawyer Swanson of Miller Thomson. *"They're now using AI, for example, to rapidly scan systems for vulnerabilities. It automates what they do so they can do it faster."*

The fallout from cyber attacks on your business

Cyber breaches are increasingly costly -- and sometimes deadly -- for businesses.

The average per capita cost of a data breach in Canada – **$202** – was among the highest in the world in 2017 [6]

There are costs related to business disruption, remediation, and notification. According to the Ponemon Cost of a Data Breach study, organizations in **Canada had the highest direct costs related to compromised records in 2017:**

$81 per record.

These costs included engaging forensic experts and legal counsel, identity protection services for victims and more.

Canada also had the highest average detection and escalation costs for a data breach – **$1.78** million. These costs include forensic and investigative activities, assessment and audit services, crisis team management and communications.

But there are more than just financial consequences to cyber theft and fraud and these deeper consequences can impact a company's ability to survive a cyber attack.

[6] Ponemon Cost of Data Breach Study

Damage to company value and customer base

For example, a 2017 global survey, The Impact of Data Breaches on Reputation and Share Value, found that companies experienced an average stock price decline of **5%** following a breach.

Even more damaging, **30%** of impacted consumers discontinued their relationship with the business following a breach.

And, if a breach involves sensitive customer data and a company does not handle the repercussions competently, customer acquisition and loyalty can erode further. Most people will choose not to do business with a company they don't trust.

Damage to company value and customer base

Litigation is another increasingly costly outcome of cyber breaches. Class action lawsuits are on the rise.

An Alberta court, for example, is currently assessing class-action certification of a lawsuit launched against Uber on behalf of Albertans whose personal information was compromised in a 2016 data breach in which the personal information of **57 million customers** was stolen.

As part of a settlement reached with US state law enforcement officials over allegations it attempted to conceal a 2016 data breach, In September 2018 Uber was required to pay a fine of

$148 million

Although still in the early stages in Alberta and Canada, mandatory notification legislation is expected to fuel litigation because many victims who are notified will seek monetary compensation. Businesses that fail to meet the legislated requirements related to breaches put themselves at risk of significant damages.

“Ignorance of the law is no excuse.

If the Office of the Privacy Commissioner investigates a breach at your company, you’ll need to be able to show that you took all reasonable steps to avoid a breach.

If the subsequent investigation shows that you didn’t, it won’t go well for you.”

James Swanson
Partner, Miller Thomson LLP

Mandatory transparency and compliance: Alberta businesses have obligations under government breach reporting legislation.

The majority of Alberta private sector businesses have been subject, since 2010, to mandatory rules under the provincial Personal Information Protection Act (PIPA) requiring them to report data breaches when personal information was compromised. With the arrival of federal breach notification requirements on November 1, 2018, all Canadian organization must follow the new Breach of Security Safeguards Regulations.

It's expected that enforcement of privacy breaches will become more proactive across the country, and companies that fail to meet mandatory reporting obligations may face significant fines.

The new federal requirements, under the Personal Information Protection and Electronic Documents Act (PIPEDA), apply to any business operating in a province that is not subject to substantially similar provincial legislation, such as Alberta.

Like PIPEDA, the Personal Information Protection Act (PIPA) in Alberta governs the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

The reporting provisions of PIPA and PIPEDA and very similar. Under PIPA if a company experiences any incident involving the loss of or unauthorized access to or disclosure of personal information, it will be required to notify the provincial Information and Privacy Commissioner "without unreasonable delay." In turn, the Commissioner may require the organization to notify individuals of the loss of their personal data.

A company must provide notification "where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, or unauthorized access or disclosure."

If a company experiences any "breach of security safeguards", it will be required to:

1. Perform a risk assessment to determine "real risk of significant harm"
2. Report the incident "as soon as feasible" after the breach occurs to:
   a. The federal Privacy Commissioner,
   b. Individuals affected by the breach, and
   c. Any organization (like a bank) that might be able to reduce the risk of harm to the affected individuals.
3. Maintain a record of the breach for a minimum of two years– even if the data breach has no risk of significant harm.

A breach of security safeguards refers to any loss, unauthorized access or disclosure of personal information, if the breach creates a real risk of significant harm to an individual. This encompasses bodily harm, humiliation, damage to reputation or relationships, loss of professional or employment opportunities, financial loss, identity theft, negative effects on credit record or damage to or loss of property.

With potential fines of up to $100,000 under both PIPA and PIPEDA, organizations should prepare to comply with the requirements.

Timely solutions to reduce risk for your business

Effectively managing risk is essential for any business to optimize performance and achieve goals.Fong suggests that by focusing on the following three areas, businesses will be able to survive, and thrive, after an attack.

Security – establish risk-prioritized controls and processes to protect the company's most valuable assets

Vigilance – develop threat monitoring awareness and capabilities focused on critical business processes

Resilience – establish the ability to rapidly contain damage, and to mobilize the resources when needed to minimize the impact of an attack

> ***"Cyber security is just one part of managing risk across the entire enterprise,"*** **says Fong. This mindset has to begin at the top of an organization, with the executive team and members of the board if there is one.** ***"Security can be counter-intuitive to productivity so a cultural shift is sometimes necessary to make proper risk-based decisions."*** **Everyone in an organization needs to be made aware that security is an essential component to the success of the business.**

> "Every business will be attacked by cyber criminals.
>
> The difference you can make is the frequency and impact of it."

Justin Fong

Cybersecurity Leader for Western Canada, Deloitte

Fong suggests Alberta businesses should develop a strategic risk-based approach to security. This begins with establishing a vision of where you want your business to be regarding risk tolerance, conducting a security gap analysis, prioritizing issues and then creating a plan for the next one to five years to address gaps. *"Cyber risks evolve quickly and have to stay on top of them to protect the health of your company."*

"The size of a business is irrelevant.

Cyber crime is about vulnerability.

Criminals look for the weakest link and that's what they exploit."

James Swanson
Partner, Miller Thomson LLP

Four quick cybersecurity wins

Executing these four strategies can immediately and dramatically reduce the potential for cyber theft and fraud and also limit the damage caused by a breach.

Access controls are strong

Check that permission and access controls are strong. This means vital areas of the business – such as certain applications and devices connected to the network, cheques, cards, electronic payments – are segmented with strong security controls that restrict access only to authorized individuals.

Technology is up to date

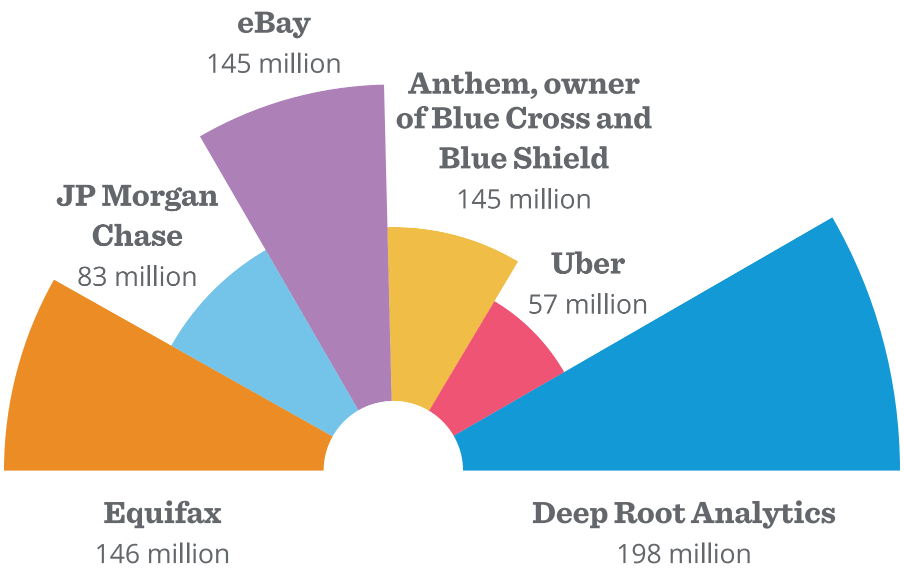
The massive 2017 data breach at Equifax that compromised the personal information of some **150 million people** was the result of a simple failure to patch software – updating a program to fix vulnerabilities. This is a common cause of cyber breaches.

Verify that processes and policies are in place to ensure timely patching. Consider using automated tools that identify and apply patches within network devices, operating systems and applications. For systems that cannot be upgraded or patched, controls such as firewalls should be in place to protect the rest of the network.

Employees are aware of and trained to recognize cyber threats

It's estimated that **close to 90 per cent of data breaches are caused by human error**. In fact, in 2017 nearly one-third of Canadian businesses unknowingly leaked sensitive information – including customer data – to cyber thieves. Why? Lack of cyber security awareness.

Creating a cyber-savvy workforce is essential. Provide ongoing training for employees to understand how hackers work and what typical attacks are. Keep employees informed about the latest security threats and techniques, how they can protect themselves, and what your company is doing to mitigate these risks.



> *"Phishing trades on people's trust and lack of knowledge,"* says Swanson of Miller Thomson. *"If you train people to be suspicious, they will recognize a phishing email when they see it. You can even make training fun."* [think phake phishing expeditions]!

4

Partners and suppliers have adequate security measures in place

Cyber criminals often search out weak links in supply chains – such as vendors, service providers, partners – to infiltrate target networks. **Verify that the organizations your business works with closely have strong security protocols in place and these are regularly monitored.**

1,2,3,4,5 ways to reduce payments fraud

Payments fraud is at a record high according to the Association for Financial Professionals, and cheque fraud is the most frequent technique.

> “The more involved you are in the day-to-day financial transactions of your business, the lower the chance it will suffer a large loss.”

Brian Ford
Vice-President,
ATB Business Solutions

Here are five tips from ATB's Treasury and Payments Solutions team that can substantially reduce the potential for payment fraud in your business.

1. Eliminate paper cheques

Physical cheques are a problem, not a solution, to fraud and theft. Cheques are easy to steal, copy, intercept and change. Instead, use a digital payments system to make transactions more secure, effective and cost-efficient.

2. Organize payment approval work-flow

This ensures that designated people approve payments at numerous stages and provides a clear payment audit trail. Establish a policy that two signatures are mandatory for payments above a specified threshold.

3. Install controls around electronic payments

Important controls include: segregating duties of people involved in the payment process; establishing accountability, authorization and approval processes for all invoice payments.

4. Reconcile business banking transactions daily

Criminals sometimes start with small transactions to test whether a particular approach works. Don't wait to receive a monthly bank statement. Conducting monthly ledger reconciliations to validate transactions as well as login daily and review the bank balance to ensure transactions have processed as expected and to look for any abnormalities.

5. Establish specific procedures for authorization of money transfers and never compromise

Since email, phone and internet banking requests all carry different levels of risk, limit methods of acceptable wire transfers. As well, limit who can initiate and approve wire transfers and when transfers exceed a certain threshold, require call back or other verification procedures.

“Policies and procedures are only effective to the extent that people follow them. The value is lost when an employee compromises them because of a rush request or to please a boss.

This is why **ongoing education should be a top priority** – training that is relevant to employees’ work, the security issues they face, the changing techniques used by cyber criminals and the best practices employees should follow.”

Brian Ford
Vice-President,
ATB Business Solutions

First steps when you discover a thief has infiltrated your systems

- Contain the damage
- Identify what has been taken or affected
- Consult with legal counsel to determine obligations
- Notify law enforcement
- Assess the consequences to the business, employees, customers, partners
- Determine internal and external notification requirements
- Hire appropriate security experts to assist with remediation
- Reinforce your security

Justin Fong

Cybersecurity Leader for Western Canada, Deloitte

ATB's commitment to rigorous security processes to protect our customers

Safeguarding our customers' sensitive personal data is a top priority at ATB Financial. We continually review and update our security systems and protocols to stay ahead of potential threats.

While, for obvious reasons, we can't disclose details of our multi-layered defences, some of the security measures we have in place to protect customers include the following:

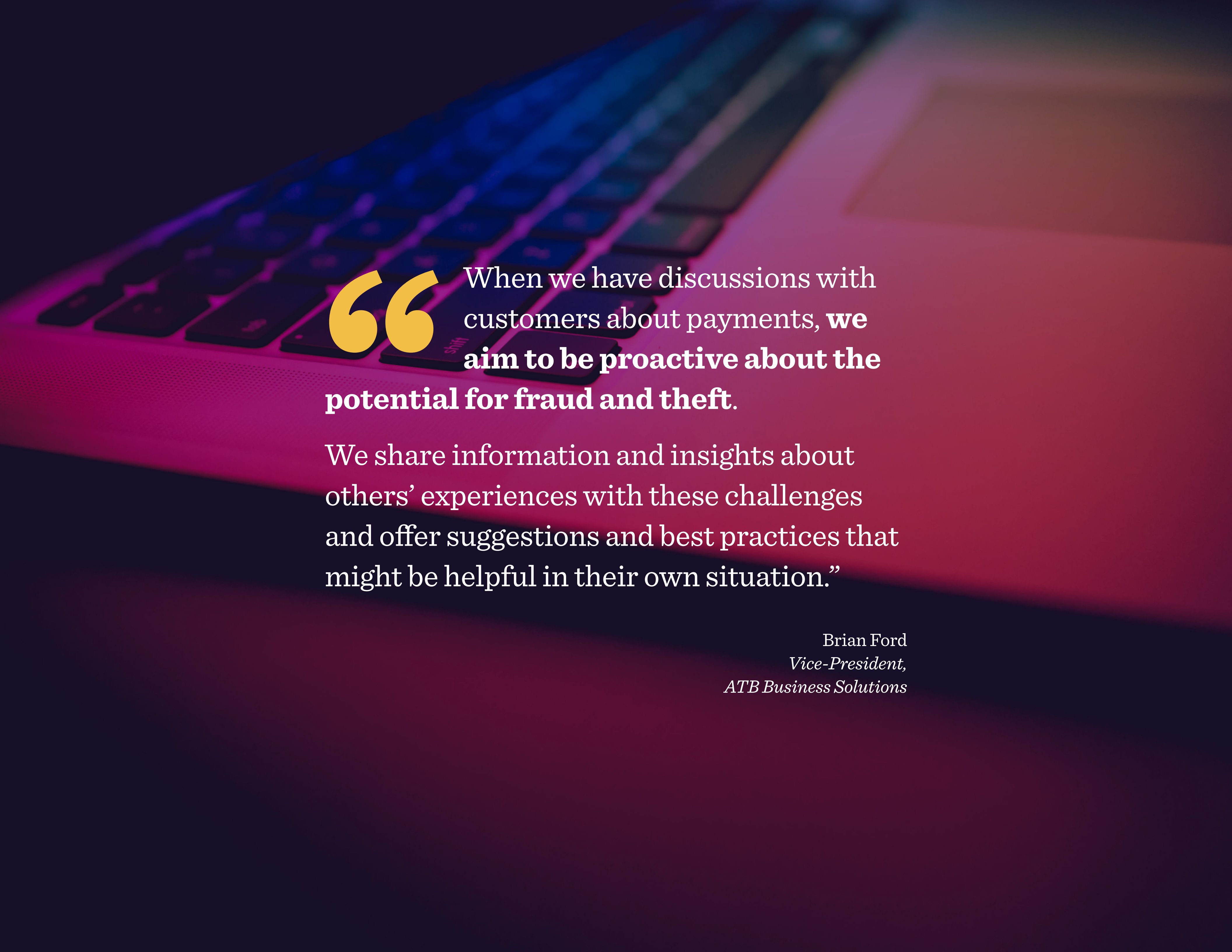
Two-factor authentication for online banking

Encryption technology to help ensure that data passing between your device and our web server is secure

Firewalls to protect your information with us

Customer verification procedures

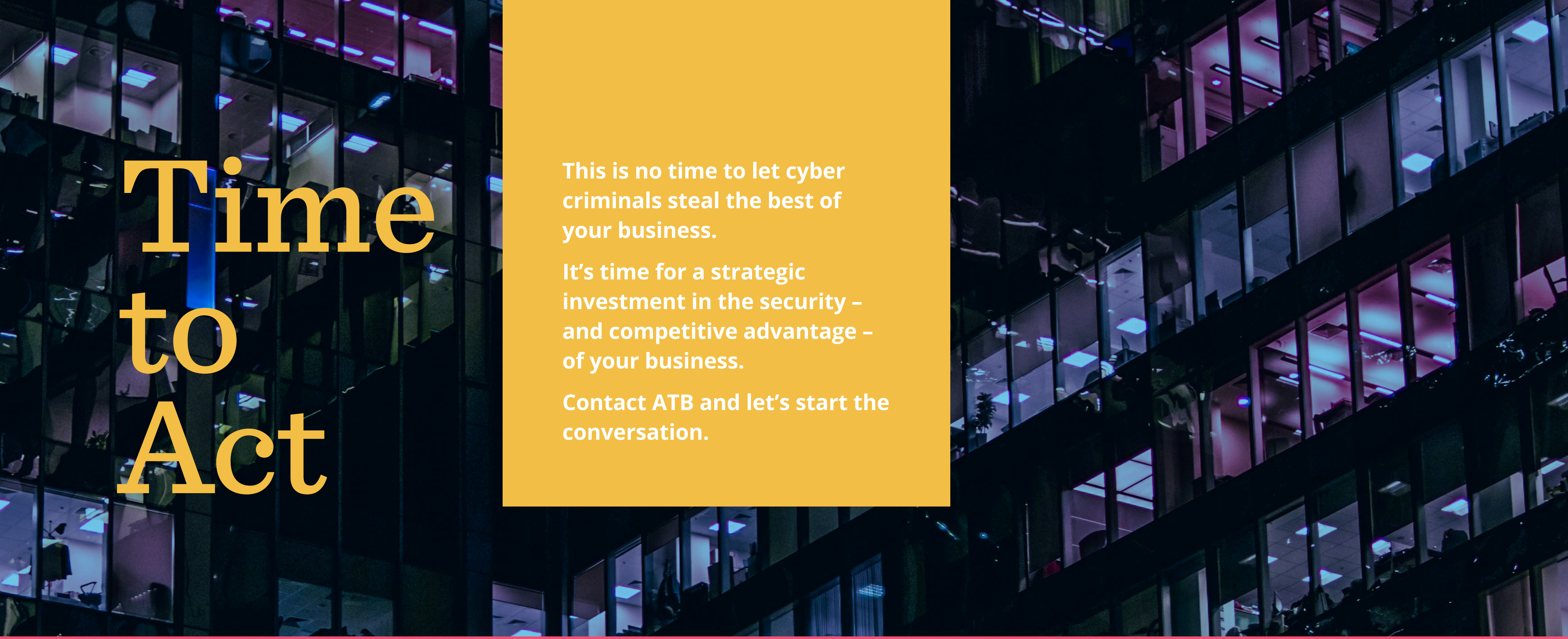
Analyzing banking transactions to identify suspicious patterns



“When we have discussions with customers about payments, **we aim to be proactive about the potential for fraud and theft**.

We share information and insights about others’ experiences with these challenges and offer suggestions and best practices that might be helpful in their own situation.”

Brian Ford
Vice-President,
ATB Business Solutions



Time to Act

This is no time to let cyber criminals steal the best of your business.

It's time for a strategic investment in the security – and competitive advantage – of your business.

Contact ATB and let's start the conversation.

About ATB Financial Treasury and Payments Solutions

By effectively managing incoming and outgoing payments, a business can strengthen cash flow and the financial health of the enterprise.

This is why the ATB Financial Treasury and Payments Solutions team carefully assesses our customers' needs and provides advice, services and tools to deliver optimal integrated payments solutions.

We enable our business customers to efficiently and securely process payroll, pay suppliers, receive customer payments, make deposits and manage cash balances. For the health of your business.

Special thanks for their contributions to this white paper

Justin Fong, *Partner, Cybersecurity Leader for Western Canada, Deloitte*

James Swanson, *Partner, Miller Thomson LLP*