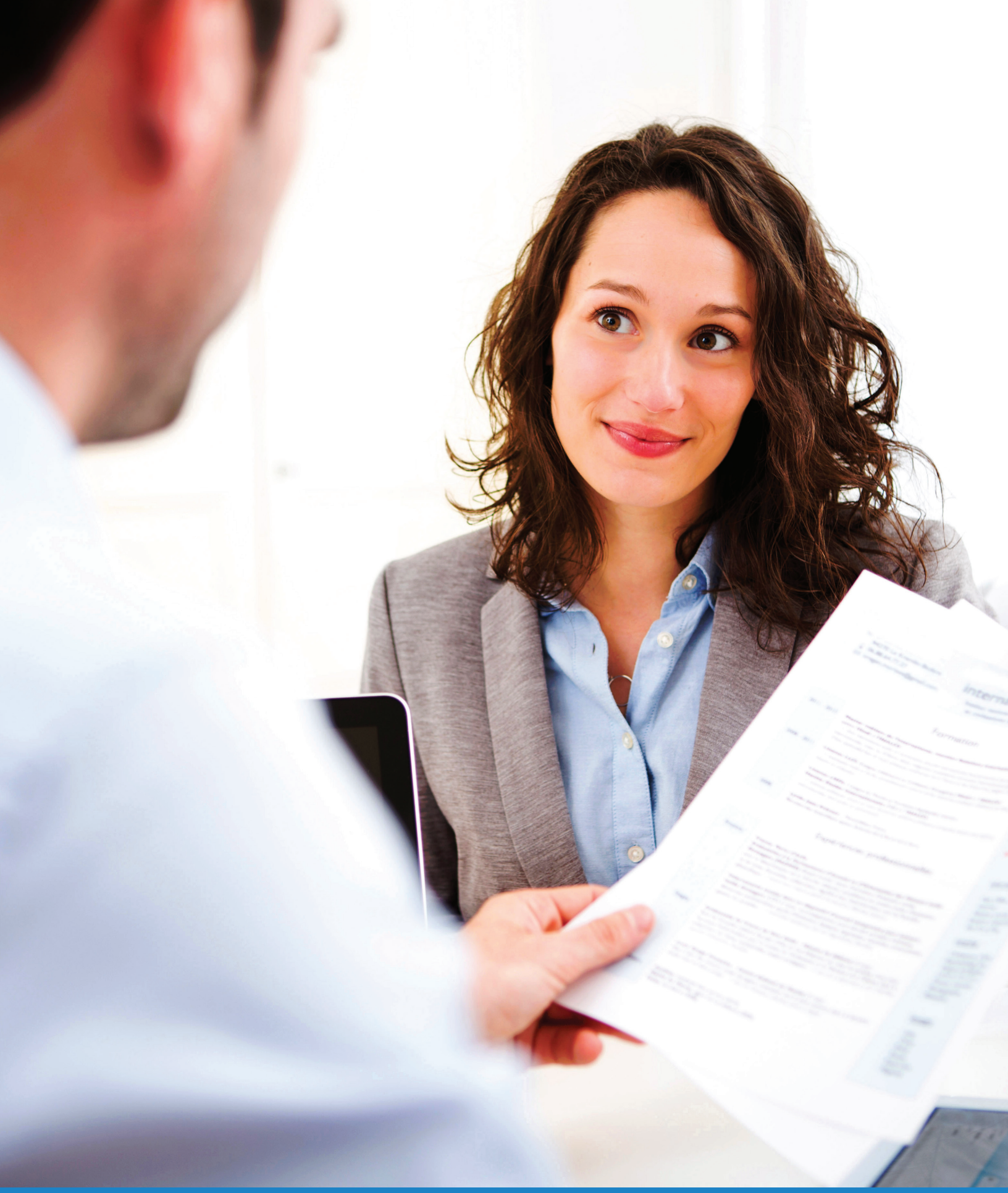
# Privacy Protection:

## Knowing what it takes to stay compliant

**We protect what matters.**

Shred-it®

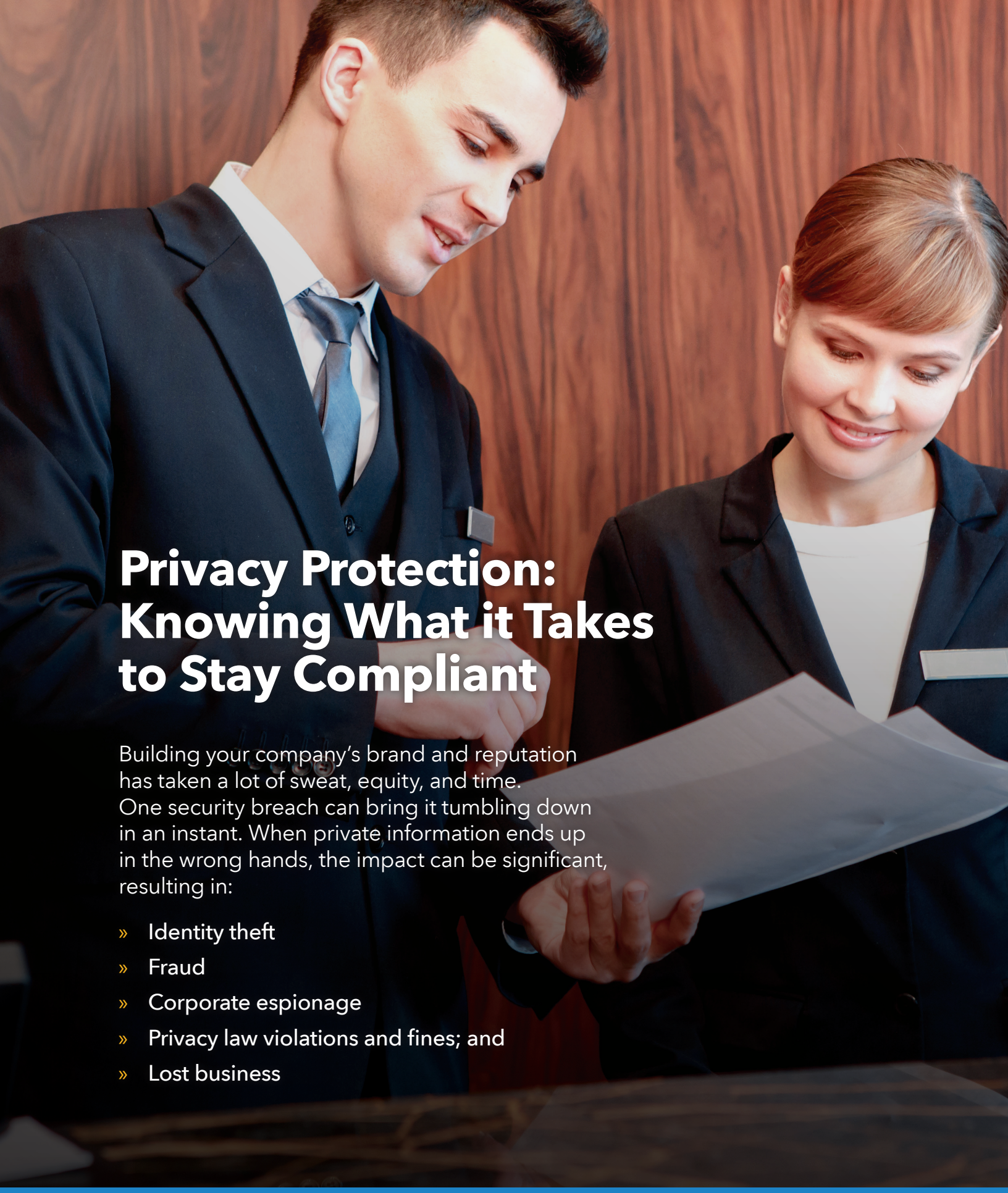


# Contents





Shred-it®



# Privacy Protection: Knowing What it Takes to Stay Compliant

Building your company's brand and reputation has taken a lot of sweat, equity, and time. One security breach can bring it tumbling down in an instant. When private information ends up in the wrong hands, the impact can be significant, resulting in:

- Identity theft
- Fraud
- Corporate espionage
- Privacy law violations and fines; and
- Lost business

## Who Needs to Protect Privacy?

The short answer is everyone. Almost every business in every industry sector accesses, uses or handles confidential information every day. This information can come into a business through a myriad of different formats including electronic and paper documents.

**For any business, ensuring private information stays private is everyone's responsibility, including:**

- All employees – whether full time, part time or casual employees
- Contractors and freelancers
- Business partners
- Suppliers including cleaners, recyclers, garbage collectors and IT support

And, for some industry sectors such as healthcare and financial services, the privacy protection requirements are even more stringent.

**MORE THAN**

# 23%

**IN OCCUPATIONAL FRAUD CASES RESULTED IN A LOSS OF AT LEAST**

# $1 MILLION[1]



Shred-it®

# What Needs Special Handling?

Almost every department has information that should be protected, both for privacy protection purposes as well corporate competitiveness. The table below contains a quick summary of typical departments and some of the document types that need special attention.

### Human Resources

- Job applications
- Health and safety documents
- Medical records
- Payroll information
- Performance appraisals
- Training information and manuals

### Sales and Marketing

- Customer lists and contracts
- Financial information
- Application forms
- Strategic plans
- Product samples
- Launch calendars
- Budgets and forecasts

### IT

- Hard drives
- Memory sticks
- CDs
- Zip disks
- Access codes
- Network configuration details

### Procurement

- Corporate records
- Supplier purchase orders
- Supplier records
- Supplier specification documents
- Credit card information
- Financial applications

### Accounting

- Contracts
- Invoices
- Customer lists
- Internal reports
- Payroll statements
- Supplier information
- Credit card information
- Financial applications

### Research & Development

- Appraisals
- Product test results
- Formulas
- Product plans
- New product information
- Reports
- Specification drawings
- Prototypes

### Management

- Budgets
- Correspondence
- Customer lists
- Legal contracts
- Forecasts
- Strategic plans

# When it Comes to Protecting Privacy, it is Not Only Good for Business, it's the Law.

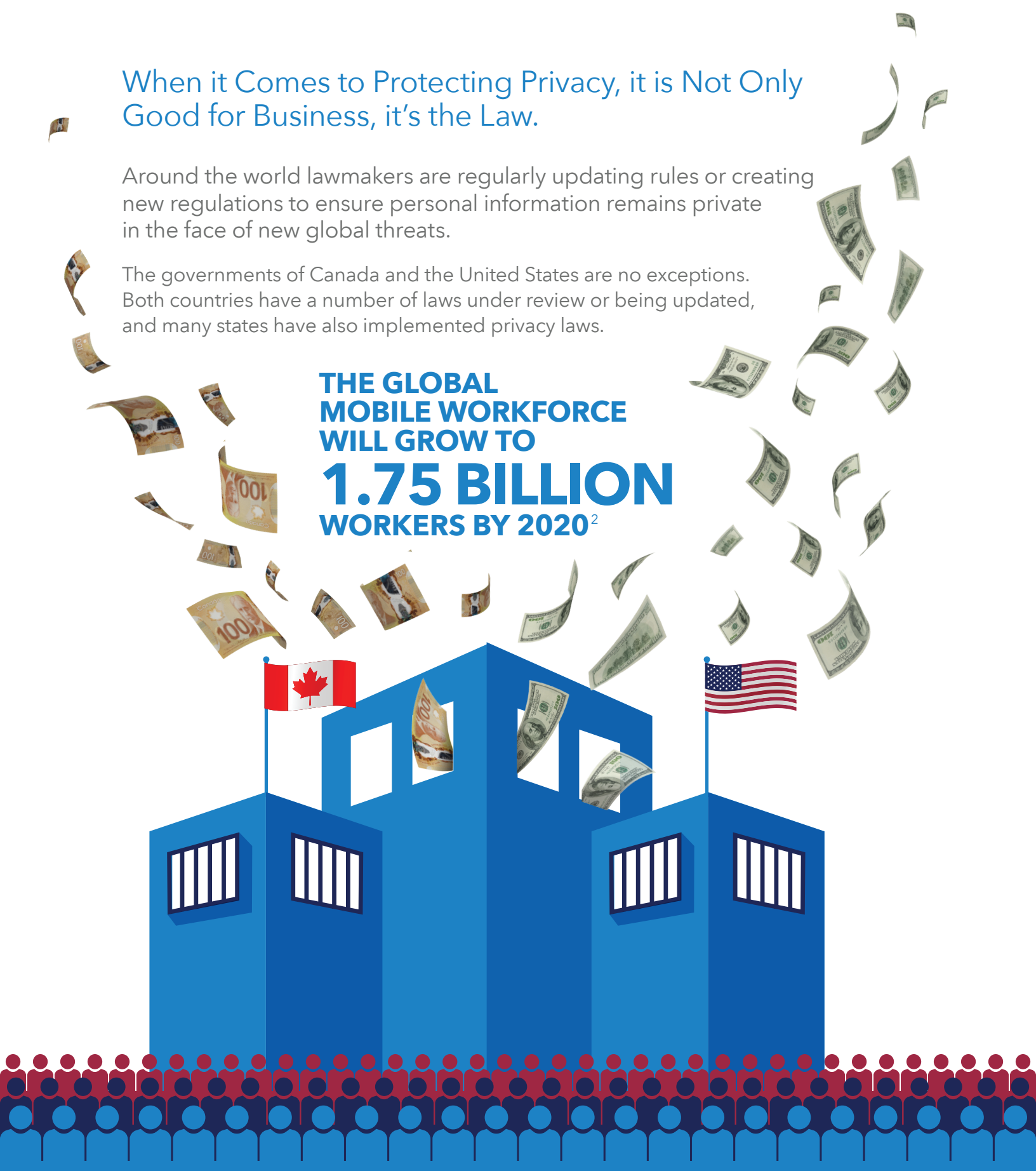
Around the world lawmakers are regularly updating rules or creating new regulations to ensure personal information remains private in the face of new global threats.

The governments of Canada and the United States are no exceptions. Both countries have a number of laws under review or being updated, and many states have also implemented privacy laws.

**THE GLOBAL MOBILE WORKFORCE WILL GROW TO**

**1.75 BILLION**

**WORKERS BY 2020**[2]





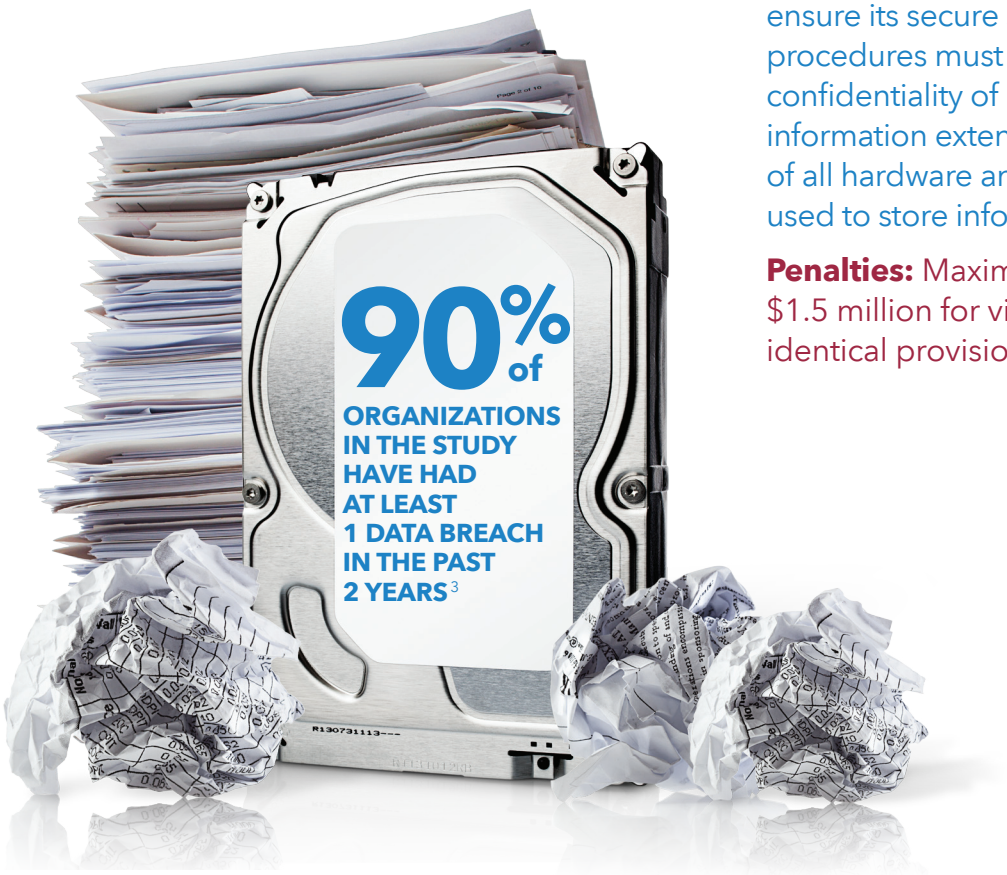
Shred-it®

# A Look at Federal Privacy Rules in the US

## Health Insurance Portability and Accountability Act (HIPAA)

Designed to protect the privacy and security of protected health information (commonly called Privacy Rule and Security Rule), HIPAA covers all health information (in both paper and electronic format) including patient records, medical logs, insurance and billing information.

**Who must comply:** Anyone who collects, has access to, or uses private health information including healthcare providers, health plans, clearing houses and their business associates.




## Health Information Technology for Economic and Clinical Health (HITECH)

This law expands the requirements and application of the Privacy Rule and Security Rule while increasing penalties for HIPAA violations.

**Who must comply:** Similar to HIPAA, this law applies to anyone who collects, has access to or uses private health information (and everyone who does business with these companies).

**What's required:** Companies must have administrative, technical and physical measures in place to protect the privacy of protected health information and ensure its secure storage. Policies and procedures must also ensure that the confidentiality of electronic patient information extends to the final disposal of all hardware and electronic media used to store information.

**Penalties:** Maximum penalty of $1.5 million for violations of an identical provision.

## Fair and Accurate Credit Transactions Act (FACTA)

FACTA provides consumers, companies and credit reporting agencies with new tools to expand consumer access to their credit information, boost credit information accuracy, enhance the security of financial information and help combat the growing problem of identity theft.

**Who must comply:** Any person or business that possesses consumer information, including financial institutions and creditors (such as lenders, insurers, landlords, employers, government agencies, financial institutions, automobile dealers and waste disposal companies).

**What's required:** All companies must develop and use written identity theft prevention measures and ensure steps are taken to protect it from unauthorized access.

**Penalties:** Any person failing to comply is liable to the consumer for actual damages or a sum of money up to $1,000 per person affected.

## Gramm-Leach-Bliley Act (GLB)

Also known as the Financial Modernization Act of 1999, GLB protects the privacy of consumer information held by financial institutions. The law also requires financial institutions to disclose information sharing practices to consumers.

**Who must comply:** Any business providing financial products and services including banks, check cashing businesses, insurance companies, real estate appraisers, tax preparation companies, ATM operators and accountants.

**What's required:** Companies must have written security plans that detail the steps they are taking to protect consumer information, have appropriate document storage protocols that limit unauthorized access, and have procedures in place for secure document destruction.

**Penalties:** Financial institutions can be fined up to $100,000 and corporate officers and directors can be fined up to $10,000 for civil penalties. Officers and directors can also face imprisonment for breaching the law. Under the Federal Deposit Insurance Act, additional penalties can be levied up to $1 million in fines against corporate directors or officers.

## Sarbanes-Oxley Act (SOX)

Enacted in response to the high-profile corporate investor swindling cases, SOX aims to improve the corporate responsibility of publicly-traded companies, while curbing corporate and accounting fraud.

**Who must comply:** Publicly-traded companies and relevant suppliers.

**What's required:** Strict financial reporting is required, and the law obligates companies and their auditors to maintain stringent information and records management policies.

**Penalties:** Fines and imprisonment of up to 20 years (depending on the severity of the infraction).

## Safe Harbor Program

A self-regulatory, voluntary framework designed to protect personal information transmitted between the European Union and the United States, the Safe Harbor Program ensures that companies take adequate precautions to protect sensitive information used for international transactions.

## Economic Espionage Act (EEA)

The EEA classifies the format and type of trade secret information to protect its actual (or potential) economic value from theft and spying.

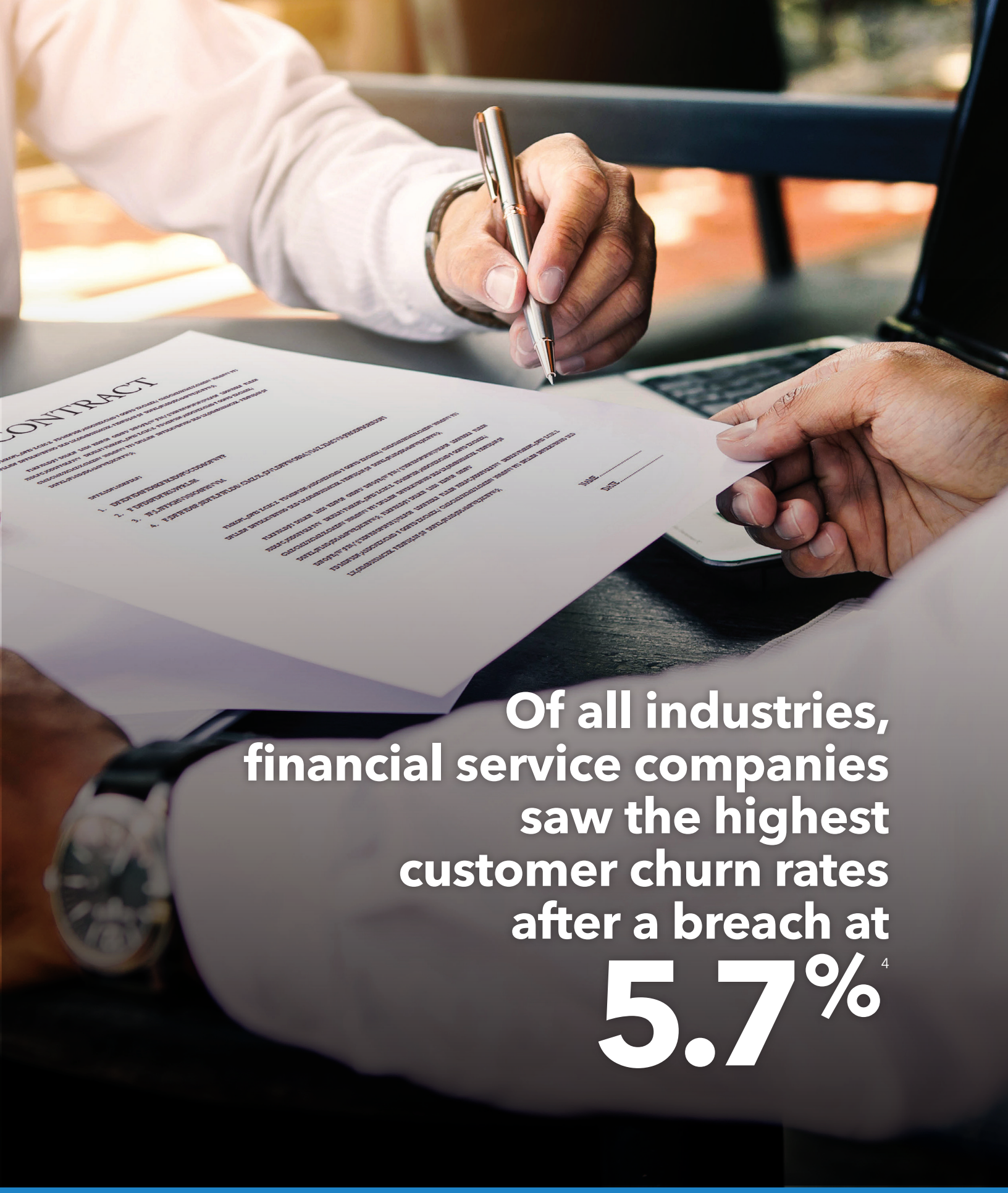
**What's required:** Owners must show they have taken adequate measures to protect information defined as a trade secret.

**Penalties:** Maximum fines of $5-10 million (or twice the legal gain) if trade secrets were stolen to benefit a foreign entity or cause injury to the owner of that trade secret. Individuals found guilty can also face up to 15 years in jail.

## Patriot Act

The Patriot Act was created to deter terrorist acts in the United States and around the world, and punish offenders. It contains measures to enhance law enforcement investigation tools and contains obligations requiring financial institutions to verify customer account information and maintain records on customer identities.

**Penalties:** Financial penalty equal to and not less than two times the amount of the transaction, up to $1 million levied against any financial institution or agency found violating the law.



**Of all industries, financial service companies saw the highest customer churn rates after a breach at**

# 5.7%[4]



Shred-it®

# A Look at Federal Privacy Laws in Canada

## Privacy Act

The Federal Privacy Act imposes privacy obligations on the collection, use and disclosure of private information by government institutions and crown corporations.

**Who must comply:** All federal government departments and agencies, and crown corporations.

**What's required:** Overseen and enforced by the Federal Privacy Commission, the Act sets out rules for the collection, handling, disclosure and use of any information about an identifiable individual. In addition to the Privacy Act, there are separate provincial and territorial public sector legislations which are similar to the federal law but there are some important variations so it is important to verify the rules that apply to your jurisdiction.

## Personal Information Protection and Electronic Documents Act (PIPEDA)

This legislation governs how private sector organizations handle private and confidential information that is collected or used during the course of commercial activities. It applies even when there are overlapping provincial or sector-specific privacy laws.

**Who must comply:** Federally-regulated organizations including banks, airlines, telecommunications companies, as well as retail stores, publishing companies, the service industry, manufacturers and other provincially-regulated organizations.

**What's required:** Organizations must have procedures in place to protect personal information in their possession from unauthorized access, employ document retention policies to safeguard confidential data while it is being used or stored, and destruction procedures that ensure all personal information that is no longer needed for the purposes it was collected is securely and permanently destroyed.

# Privacy Act and PIPEDA: What's at Stake?

These Canadian Federal regulations apply to any and all information about an identifiable individual in any form including name, address, gender, race or ethnic origin, ID numbers, religious beliefs or political views, income, credit or loan information, blood type and health history.

When an organization is found to have violated the law, the Federal Privacy Commission is authorized to publicize its findings, identify businesses found to be non-compliant and refer complaints to the Federal Court for enforcement. Fines, as well as industry or regulatory sanctions, could be imposed and there is no ceiling on monetary damages that the court may award.

## Protecting privacy starts with identifying risks

Knowing where private information could be vulnerable to theft is an important first step towards improving your internal protection measures and legal compliance.

**Use this checklist:**
**shredit.com/information-security-best-practices-and-checklist**
to review all areas of your company to identify potential risk zones and take steps to plug the holes in corporate security before you find yourself in breach.

**76% of**
**CANADIANS SAID THEY HAVE REFUSED TO PROVIDE A BUSINESS WITH THEIR PERSONAL INFORMATION, AND HALF HAVE CHOSEN NOT TO DO BUSINESS WITH A COMPANY DUE TO ITS PRIVACY PRACTICES**[5]




Shred-it®

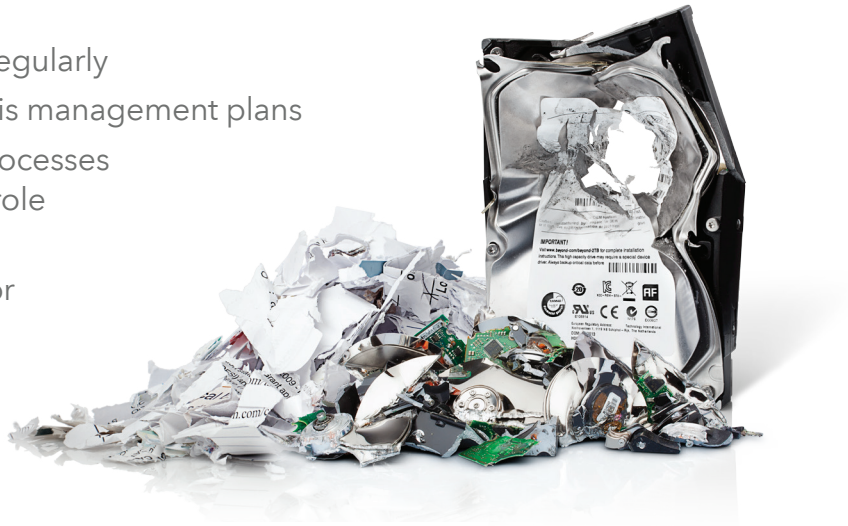
**90% of organizations globally consider malicious insiders a major threat to security**[14]

# Get on the Offensive

In any battle, a strong offence is sometimes the best defense. When it comes to privacy protection, being proactive is often the best approach. Bring together the best people, processes and technology to help reduce your risks and make sure you keep security top of mind within the corporation.

## Best practices

- Understand your legal obligations
- Conduct a comprehensive risk assessment
- Establish detailed policies and procedures for confidential information including:
  - *Collection*
  - *Use and access*
  - *Retention*
  - *Secure storage*
  - *Processing*
  - *Disclosure*
  - *Destruction*
- Designate employees to oversee security
- Monitor suppliers' document security protocols
- Have a clean desk policy requiring employees to clear their desks if they leave for extended periods of time.
- Implement a *Shred-it All* policy to take the guesswork out of what to shred and what not to shred
- Secure all electronics – when they are in use and once they've outlived their lifecycle
- Review and update procedures regularly
- Include document security in crisis management plans
- Train and re-train staff on risks, processes and help them understand their role in securing private information
- Conduct regular audits to monitor effectiveness and compliance



# How Shred-it® Can Help

Shred-it is the global leader in information security, providing information destruction services to more than 400,000 global, national and local businesses.

### Shred-it Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organization's needs

### Advice and Expertise

- Trained experts in information security
- Provide a Risk Assessment Survey at your organization
- Helpful resources available at **shredit.com/resource-center**

## Visit us at shredit.com/equalis


**Sources:**

1. 2016 Global Fraud Study https://www.acfe.com/rttn2016/costs.aspx
2. Global Mobile Workforce Forecast, 2015-2020
3. Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data by Ponemon Institute, May 2016
4. 2017 Cost of Data Breach Study, Ponemon and IBM
5. 2016 Survey of Canadians on Privacy by Phoenix Strategic Perspectives for Office of the Privacy Commissioner of Canada
6. Mimecast Study 2016 http://www.businesswire.com/news/home/20160817005095/en/Mimecast-Study-45-Percent-Organizations-Prepared-Malicious




Shred-it®