Data Privacy and Identity Theft Unit

- Investigates and enforces data breaches involving Indiana residents
- Investigates and prosecutes Identity Theft
- Helps Identity Theft victims obtain refunds, cancel accounts, and correct their records
- Manages abandoned medical or professional records
- Manages the Do Not Call list and investigates and prosecutes violations of Indiana's telephone privacy laws – Do Not Call, robocalls, and others

Types of Identity Theft

Low Tech

High Tech

What to Do if You Suspect ID Theft

- **Request a free credit report at: www.annualcreditreport.com**
- **If you find fraudulent activity, contact the Attorney General's Office**
- **Visit www.IndianaConsumer.com/IDTheft**
- **Or call 1-800-382-5516**
- **Consider placing a Security Freeze**

How to Protect Your Township?

More than half of organizations attribute a security incident or data breach to a malicious or negligent employee

- Policies for employees using business computers
- Policies for employees handling personal information
- Policies for employee use of data, only as needed

Source: Ponemon Institute, www.ponemon.org

How to Protect Your Township?

Don't Forget Old Fashion Physical Security

Lock your doors

Lock your cabinets

How to Protect Yourself?

Shred old documents

How to Protect Yourself?

Check your bank accounts frequently

FIRST BANK OF WIKI
1425 JAMES ST. PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

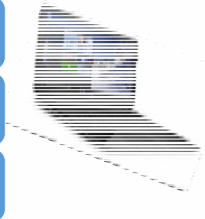
JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-09	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
	*** Totals ***		1,515.63	1,442.61	

How to Protect Your Township?

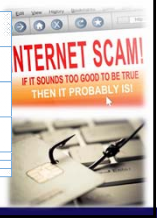
- Physically secure desktop computers, laptops, and servers
- Require strong password logons & change them often
- Use password protected files
- Encrypt files where possible



How to Protect Your Township?

The majority of breached organizations needed someone else to tell them they've been hacked.

- Use antivirus software
- Keep software updated
- Watch out for scams
- Watch out for phishing



How to Protect Yourself?

Use Strong Passwords

When considering an online password make sure it is a strong password by using:

- CAPITAL LETTERS
- lowercase letters
- Numbers
- Special characters

Example: !Sha08Emy!

Don't re-use the same password in more than one place

How to Protect Yourself?

Educate Employees about Phishing Scams

Phishing is a fake message that looks real. It's designed to get you to…

- Share personal information, like your account number, PIN, Social Security number;
- Give away your user name and password; or
- Click on a link containing malware to infect your device

Phishing attacks are on the rise and they are a leading cause of data breaches.

www.ftc.gov/tips-advice/business-center/small-businesses

Tips to Avoid Phishing Scams

- Be suspicious of any request for login or personal information
- Think before you click on any link or attachment you receive in a message
- Be alert for grammar errors and other signs that the message is fake

So, You've Had a Data Breach…

What now?

What to Do After a Data Breach

- Secure your operations to stop additional data loss
- Fix vulnerabilities
- Notify all appropriate parties:
  - Law enforcement
  - Affected businesses and individuals
  - Attorney General
  - Consumer reporting agencies

Source: https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf

After a Data Breach

Until recently, there was some confusion about whether local governments were required to follow:

- Disclosure of Security Breach Act, Ind. Code 24-4.9, or
- Notice of Security Breach Act, Ind. Code 4-1-11

According to A.G. Official Opinion 2018-5:

Municipal, County, and Township governments must follow the Disclosure of Security Breach Act, Ind. Code 24-4.9, also known as the DSBA.

Disclosure of Security Breach Act - Definitions

Definitions to know:

"Data base owner" means a person that owns or licenses computerized data that includes personal information.

Ind. Code 24-4.9-2-3

Disclosure of Security Breach Act - Definitions

"Breach of the security of data" (also known as a data breach) means the unauthorized acquisition (or theft) of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. This term includes:

- Theft of a laptop, flash drive, or portable device if personal information is on it and it is NOT encrypted
- Theft of a laptop, flash drive, or portable device if personal information is on it, and it is encrypted, BUT the thief has the encryption key.

Ind. Code 24-4.9-2-2

Disclosure of Security Breach Act - Definitions

"Personal information" means

- a Social Security number that is not encrypted or redacted; **OR**
- A person's first and last names, or first initial and last name, **and** one or more of the following that are not encrypted or redacted:
  - A driver's license number.
  - A state identification card number.
  - A credit card number.
  - A financial account number or debit card number with a security code, password, or PIN.

Ind. Code 24-4.9-2-10

Disclosure of Security Breach Act - Notice

After discovering or being notified of a data breach, the data base owner **SHALL** notify the following about the data breach:

- Indiana residents whose information was or may have been acquired by an unauthorized person;
- Indiana Attorney General's Office; and
- If more than 1,000 Indiana residents were affected, notify the 3 consumer reporting agencies Experian, Transunion, and Equifax

Notice shall be made without unreasonable delay.

Ind. Code 24-4.9-3-1 & 24-4.9-3-3

Disclosure of Security Breach Act - Notice

Notice to the affected Indiana residents can be given by:

(1) Mail
(2) Telephone
(3) Fax
(4) Email, or
(5) If more than 500,000 Indiana residents were affected, or if the cost of notice will be greater than $250,000, you can give substitute notice by a post on your website or notice to news media in the area where those affected by the breach live.

Ind. Code 24-4.9-3-4

Disclosure of Security Breach Act - Notice

Notice to the Indiana Attorney General can be given by:

(1) Mail (see address on last slide)

(2) Fax 317-232-7979

(3) Email idtheft@atg.in.gov

We request that all data breach notifications be submitted on our form, however, notice without the form still counts.

More information about security breaches including a link to the form can be found at:
https://www.in.gov/attorneygeneral/3037.htm

Ind. Code 24-4.9-3-1(c)

Disclosure of Security Breach Act - Notice

If notice is required for the 3 consumer reporting agencies (because more than 1,000 Indiana residents were affected) then –

the notice shall include information necessary to assist the agencies in "preventing fraud."

This may include providing the personal information of the people affected by the breach to the consumer reporting agencies.

Ind. Code 24-4.9-3-1(b)

Disclosure of Security Breach Act - Notice

Notice shall be made without unreasonable delay.

A delay is reasonable if the delay is:

- Necessary to restore the integrity of your computer system
- Necessary to determine the scope of the breach; or
- Due to a request from law enforcement or the attorney general to delay notice because it will affect an investigation

Ind. Code 24-4.9-3-3

Disclosure of Security Breach Act – Protect

A data base owner shall implement and maintain reasonable procedures,

including taking any appropriate corrective action,

to protect & safeguard from unlawful use or

disclosure

any personal information of Indiana residents collected or maintained by the data base owner.

Ind. Code 24-4.9-3-3.5(c)

Summary – To Do List

(1) Create policies for data security – both electronic and paper files
(2) Conduct regular employee training on all policies (passwords, phishing scams, general security)
(3) Make an Incident Response Plan – secure the system, who to contact, what to do if your system is down
(4) Back-up your data and prepare an emergency access plan for data that might be inaccessible
(5) Conduct regular system security audits
(6) Remember it's not IF, but **WHEN**

Any Questions?

Contact Info

Eliza K. Bradley
Deputy Attorney General
Data Privacy & Identity Theft Unit
Office of Indiana Attorney General
302 West Washington Street
IGCS – 5th Floor
Indianapolis, IN 46204
p: (317) 232-6224 | f: (317) 232-7979
Eliza.Bradley@atg.in.gov