# Identity Theft and Business Responsibility

February 5, 2009

Peter Rowley
Director, Information Systems

Computing & Network Services,
York University
prowley@yorku.ca

# What Is Identity Theft?

- Someone you do not trust acquires enough information about you to masquerade as you in the eyes of one or more organizations.
- This **identity thief** uses this capability to impersonate you for personal gain and/or to cause you harm.

# Two Steps

- The identity thief acquires some personally identifiable information (PII) for a particular person, e.g. a social insurance number, name, and birth date.
- The identity thief presents the information to an organization that accepts that set of information as proof of someone's identity, thereby impersonating that person and then proceeds to acquire more PII and/or harms the victim, e.g. by incurring debt.

# Acquiring PII

- How is personally identifiable information acquired?
- (Discussion and examples)
- Examples: "Identity Theft Revisited: Security is Not Enough", available from the Information and Privacy Commissioner for Ontario, **www.ipc.on.ca**

# Many Breaches are Inside Jobs

- Employees who have access to PII may make unauthorized use of it
- It is the responsibility of businesses to prevent this where and as possible
- How? (Discussion)

# Identity Management Systems

- Systems that handle authentication and authorization of users
- Authentication: you are who you say you are
- Authorization: given who you are, you have specific access to specific information systems (and not others)

# How Can IMS's Help To Prevent Identity Theft?

- (Discussion)

# Removing Identity Theft Opportunities

- Robust authentication
- Careful role-based authorization with frequent review and immediate updates

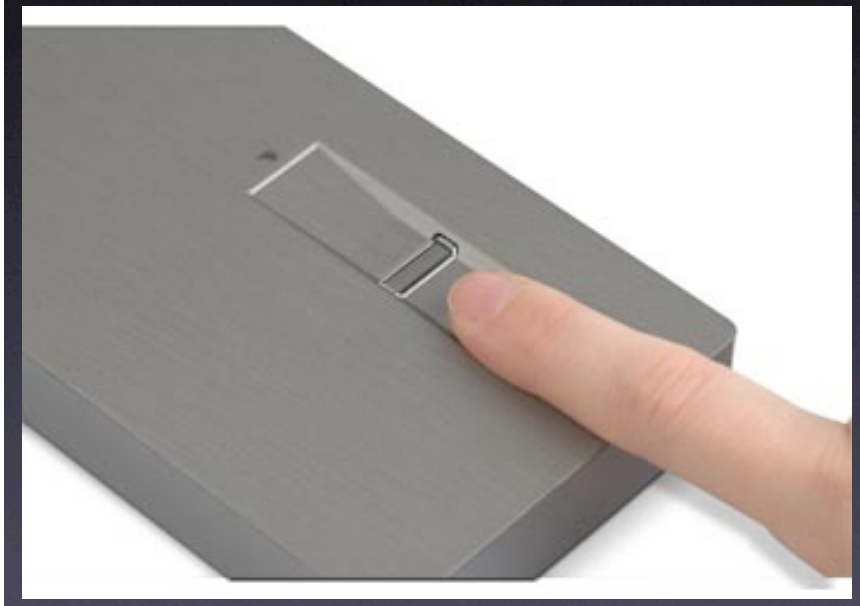
# Other Measures Businesses Can Take to Protect PII?

- (Discussion)

# Recommended Measures

- Collect PII only when necessary
- Encrypt, sever, or mask personal data
- Use techniques that render PII inaccessible if stolen
- Take inventory of all PII collection points, uses, assets, and disclosures
- Securely delete or destroy unnecessary PII

# Protecting Mobile Data



# Recommended Measures

- Avoid centralizing all personal data in one database; avoid giving one person access to all data
- Review who has access to which data, including all temporary and part-time employees and outside contractors
- Install a system to detect and respond to breaches, e.g. monitor database & transaction logs

# Recommended Measures

- Do not print complete credit card numbers on receipts
- Secure data with in-depth defenses so that if one is compromised, others remain
- Create a culture of privacy protection in your organization by training all staff and by clearly communication privacy policies

# Recommended Measures

- Obtain and record the informed consent of individuals before collecting PII
- Keep your purposes for collecting PII narrow and specific -- and stick to them
- Allow individuals to review and correct your PII about them

# If There's A Breach

- Contain the breach as quickly as possible
- Notify the individuals affected
  - New guidelines as of August 1, 2007
- Inform appropriate staff within the organization
- Investigate the details and causes of the breach
- Improve practices to reduce the chances of a similar breach occurring again

# Protecting Your Own PII

- Handout: How to Protect Your Privacy on Facebook

# More Information

- www.yorku.ca/secretariat/infoprivacy/index.htm
- www.ipc.on.ca/
- www.privacybydesign.ca