

IDENTITY THEFT

PROTECT YOUR BUSINESS PROTECT your CUSTOMERS

Protecting customer data is both a legal and a customer relationship issue. How does your organization protect the information it collects? This checklist will help you develop secure information management practices.

Collection

- ✓ Only collect essential data
- ✓ Obtain consent when you collect

Security & Storage

- ✓ Don't store unneeded data
- ✓ Encrypt data on networks, laptops and remote access devices
- ✓ Update security software frequently
- ✓ Save to networks not hard drives
- ✓ Use locks, alarms and video cameras
- ✓ Conduct employee background checks
- ✓ Terminate network access when employees leave the organization
- ✓ Limit access to sensitive data

Disposal

- ✓ Use scrubbing software or destroy hard drives
- ✓ Shred all sensitive documents

Response Plan

- ✓ Prepare a strategy to manage a breach

For more advice and tools on ID theft, visit cmcweb.ca/idtheft

Produced by the Federal-Provincial-Territorial
Consumer Measures Committee

Canada

IDENTITY THEFT

WHAT TO DO WHEN INFORMATION GOES MISSING

To respond to a breach you need to investigate the problem internally and devise a plan for informing those affected.

Timing is critical.

Investigating the Breach

Assess the situation by asking:

- ✓ What information was stolen?
- ✓ When was it stolen?
- ✓ How did it happen?
- ✓ Which files were affected?
- ✓ Is other information at risk?
- ✓ Is advice from a lawyer/accountant needed?

Communicating the Breach

Be prepared to inform:

- ✓ Credit reporting agencies
 - Equifax (1-800-465-7166)
 - TransUnion (1-877-525-3823)
- ✓ Affected customers or businesses
- ✓ Law enforcement and PhoneBusters at 1-888-495-8501 or phonebusters.com
- ✓ Privacy Commissioner

IDENTITY THEFT:

Recognize it.

Report it.

Stop it.



The Canadian Anti-fraud Call Centre