



What business can do to reduce the risk of identity theft

- Keep valuable customer data, such as credit-card or bank account numbers, in a secure location in your business so that it is not readily visible to others who may have access to the premises.
- Handle personal information as you would actual cash.
- Shred or destroy paperwork you no longer need, such as bank machine receipts, receipts from electronic and credit card purchases, utility bills, and any other document from customer transactions that contains personal and/or financial information.
- Do not collect personal information indiscriminately. Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Destroy, erase or render anonymous information that is no

longer required for an identified purpose or a legal requirement.

- Paper files and computers need to be protected with physical security measures such as locks, restricted-access areas and alarm systems.
- Encrypt all computerized records, including on networks, lap tops and remote access devices such as Blackberries, which contain personal information. Use technological tools such as passwords and fire walls.
- Use organizational controls to prevent "inside jobs." These include employee and contractor security clearances, limiting access on a "need-to-know" basis, and staff training.
- Educate employees about

the importance of maintaining the security and confidentiality of personal information.

Safety at the check-out counter

- Ensure customers can enter their debit card PINs in a secure way. Add shields to key pads. Regularly check point-of-sale equipment to verify it has not been tampered with. Ensure security cameras cannot record customers entering their PINs.
- Pin Pads should be secured to the counter with some identifying sticker so you can tell if it has been swapped out.
- Ensure cashiers verify signatures on credit cards and ask for photo ID when signatures do not

match or when the signature on the back of a credit card is smudged.

- Use equipment that does not print the entire debit or credit card number on a receipt.
- When selling online, protect against fraud with encryption software and other security technologies. Regularly update.

Avoid collecting and using Social Insurance Numbers

The Social Insurance Number should not be used as a general identifier.

What to do when there is a breach

Individuals should be told immediately that their personal information has been compromised, particularly when there is a risk of identity theft or some other harm. Contact police and credit bureaus and notify the Officer of the Privacy Commissioner of Canada.

For more information check the web site of the Officer of the Privacy Commissioner of Canada <http://www.privcom.gc.ca>.

