



Office of the Information
and Privacy Commissioner

NEWS RELEASE

Edmonton, February 8, 2005

Investigations find Alberta businesses failed to protect personal information from identity thieves

Recent investigations by the Office of the Information and Privacy Commissioner (OIPC) found that three Alberta businesses failed to protect personal information in their custody.

On November 24, 2004, Edmonton Police Service (EPS) notified the OIPC that documents containing personal information from a number of Alberta businesses were found during a police investigation. Some of the records were found in a motel room; others were subsequently turned over to police by two individuals charged with credit card fraud. The records included return of goods slips, debtor account files from a collection agency, and cell phone contracts. Personal information in the records included Social Insurance Numbers, bank account information, credit card numbers, and customer signatures.

In response to the information from EPS, Information and Privacy Commissioner Frank Work initiated investigations of Linens 'N Things, Nor-Don Collection Network Inc., and Digital Communications Group Inc., under the *Personal Information Protection Act* (PIPA).

PIPA applies to private sector organizations in Alberta, and requires them to protect personal information against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

The investigators found that these businesses failed to protect personal information in their custody. Recommendations from the investigations required all three organizations to contact the individuals whose information was, or may have been, exposed to identity theft. In at least one case this meant contacting hundreds of customers.

Additional recommendations required the organizations to:

- ensure all records containing personal information are stored securely,
- limit access to personal information to staff on a “need-to-know” basis,
- develop procedures for storage, retention and destruction of personal information, and
- provide privacy and security training/awareness for employees.

One organization was also required to obtain computer equipment to obscure credit card numbers printed on receipts and return slips.

Along with the affected individuals, these three businesses were victimized in these incidents, but each is responsible under PIPA for securing personal information. The OIPC is advising other businesses not to put themselves in the same situation.

-30-

*****Note: Commissioner Frank Work, Elizabeth Denham, Private Sector Lead, and Jill Clayton, Portfolio Officer are available for media interviews at our Edmonton office.**

To obtain a copy of an Investigation Report, click the following links:

Investigation #P2005-IR-001

http://www.oipc.ab.ca/ims/client/upload/P2005_IR_001.pdf (Linens 'N Things)

Investigation #P2005-IR-002

http://www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf (Nor-Don Collection Network Inc.)

Investigation #P2005-IR-003

http://www.oipc.ab.ca/ims/client/upload/P2005_IR_003.pdf (Digital Communications Group Inc.)

Backgrounders with a summary of each investigation are attached.

For further information contact:

Tim Chander
Research and Issues Manager
(780) 422-6860

Backgrounder -- Linens 'N Things

On November 24, 2004, Edmonton Police Service (EPS) notified the Office of the Information and Privacy Commissioner (OIPC) that documents containing personal information of customers of a Linens 'N Things (LNT) store had been found during a police investigation. Some of these records were found in a motel room; other records were subsequently turned over to EPS by two individuals charged with credit card fraud. The records recovered by EPS consisted of return receipts from credit card, debit card and cash purchases detailing customer names, addresses, phone numbers, and details of purchases made. The receipts detailed the value of the return, the customer's credit card number and expiry date, or the customer's debit card number. All return receipts also contained the customer's signature.

At the same time, EPS found customer information of a number of other Alberta businesses, as well as records relating to a credit screening program conducted by the Government of Alberta.

As of January 1, 2004, the *Personal Information Protection Act* (PIPA) applies to private sector organizations in Alberta. The Act sets out the provisions under which organizations may collect, use or disclose personal information, and also places a duty on organizations to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction. In response to the documents provided by EPS, the Commissioner initiated an investigation.

The investigator recommended that LNT take the following actions with respect to the issues raised in this investigation:

- Take action to notify individuals whose information was exposed to identity theft;
- Confirm the details of a new contract with a third-party shredding company to ensure that proper privacy and security protections are in place;
- Review all filing cabinets and storage areas to ensure effective locking mechanisms are in place;
- Obtain computer equipment that will obscure/truncate credit card numbers, preventing these numbers from printing out in full on the receipts and return slips;
- Conduct an internal audit of information handling practices, including disposal of records. Provide a copy of this audit to the OIPC within 90 days;
- Strengthen LNT's corporate-wide privacy and security policies and develop an implementation plan, including training for all employees.

LNT's security and disposal practices failed to fully comply with the organization's obligations under PIPA. This failure exposed customers to actual and potential risks of identity theft. The organization has taken, or has committed to take, appropriate action by developing new procedures, training staff, and contacting individuals whose information was exposed or compromised by identity thieves as outlined above.

Backgrounder -- Nor-Don Collection Network Inc.

On November 24, 2004, Edmonton Police Service (EPS) reported to the Office of the Information and Privacy Commissioner (OIPC) that records related to debtor accounts assigned by a credit union to Nor-Don Collection Network Inc. (NCN) were recovered during a police investigation of another matter. Along with these documents, police recovered customer information from a number of other Alberta businesses, as well as records related to a credit screening program conducted by the Government of Alberta. Two individuals were charged with credit card fraud as a result of the police investigation.

As of January 1, 2004, the *Personal Information Protection Act* (PIPA) applies to private sector organizations in Alberta. The Act sets out the provisions under which organizations may collect, use or disclose personal information, and also places a duty on organizations to protect personal information in their custody or control against such risks as unauthorized access, collection, use, disclosure or destruction. In response to the information provided by EPS, the Information and Privacy Commissioner initiated an investigation.

At this time, neither EPS nor NCN is able to confirm with certainty how the individuals charged as a result of the police investigation acquired the documents at issue. However, it is clear that during a move to new premises, NCN's security and disposal practices failed to comply with the requirements set out in PIPA, and an unauthorized individual(s) was able to exploit weaknesses and obtain sensitive personal information.

NCN has taken the following steps to help reduce the risk of future breaches in its Edmonton branch office:

- Initiated action to notify individuals whose information was compromised, or potentially compromised;
- Reviewed all filing cabinets and storage areas at the new location to ensure effective locking mechanisms are in place;
- Ensured that all records containing personal information are stored securely, and access is limited to staff on a "need-to-know" basis;
- Reviewed access controls for the premises to ensure appropriate mechanisms are in place;
- Developed the following policies:
 - Canadian Privacy Policy
 - Document Storage and Retention Policy
 - Document Shredding Policy
- Contracted with a shredding company to supply on-site shredding services.

In addition, the investigator recommended that NCN:

- Deliver an information session for employees of the Edmonton office as part of communicating new privacy and records retention and destruction policies;
- Conduct regular and ongoing monitoring to ensure security controls are implemented and effective;
- Ensure that reasonable controls are in place to protect personal information in the event of any future premises moves;
- Report back to the OIPC on or before February 28, 2005 regarding implementation of these recommendations.

NCN has taken, or has committed to take, appropriate action by contacting individuals whose information was exposed to risk as a result of this breach, developing new policies and procedures, implementing more rigorous safeguards, and regularly monitoring the effectiveness of those safeguards.

Backgrounder -- Digital Communications Group Inc.

On November 24, 2004, Edmonton Police Service (EPS) notified the Office of the Information and Privacy Commissioner (OIPC) that documents containing personal information of customers of Digital Communications Group Inc. (DCG) had been found during a police investigation. These records were turned over to EPS by two individuals charged with credit card fraud. At the same time, EPS found customer information of a number of other Alberta businesses, as well as records relating to a credit screening program conducted by the Government of Alberta.

As of January 1, 2004, the *Personal Information Protection Act* (PIPA) applies to private sector organizations in Alberta. The Act sets out the provisions under which organizations may collect, use or disclose personal information, and also places a duty on organizations to protect personal information in their custody or under their control against such risks as unauthorized access, collection, use, disclosure or destruction. In response to the EPS findings, the Information and Privacy Commissioner initiated an investigation.

Neither the EPS nor DCG can confirm how the individuals charged in connection with the recovered cell phone contracts acquired these documents. However, based on the other documents recovered by the police, this Office suspects that the records may have been removed from the custody of DCG by an employee of the company.

DCG has taken the following steps to help reduce the risk of further breaches:

- Notified individuals whose information was compromised or potentially compromised.
- Reviewed and adapted all filing cabinets and storage areas to ensure effective locking mechanisms are in place;
- Ensured that all records containing personal information are stored in locked cabinets and access is limited to staff with a "need to know" (e.g. accounting and data entry staff);
- Entered into a contract with a shredding company to provide on-site shredding of contract documentation; and
- Implemented a policy that at each year-end, a review is undertaken to ensure all records older than 3 years are shredded.

In addition, the investigator recommended that DCG:

- Document the destruction of customer records;

- Conduct regular and ongoing monitoring to ensure security controls are effective; and
- Deliver an information session for employees of the Edmonton stores as part of communicating new privacy and records security procedures.

DCG's security and disposal practices failed to comply with the organization's obligations under the PIPA. This failure exposed DCG's customers to potential risks of identity theft.