

**ALBERTA  
INFORMATION AND PRIVACY COMMISSIONER**

**Report on an Investigation Into the Security of Customer  
Information**

**January 31, 2005**

**Nor-Don Collection Network Inc.  
Investigation #P2005-IR-002**

**I. INTRODUCTION**

[1] On November 24, 2004, the Edmonton Police Service (“EPS”) notified the Office of the Information and Privacy Commissioner (“OIPC”) that documents related to debtor accounts, assigned by a credit union to Nor-Don Collection Network Inc. (“NCN”), had been found during a police investigation of another matter. The 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. Investigation Reports F2004-IR-003, P2005-IR-001, and P2005-IR-003, address issues relating to these other organizations.

**II. JURISDICTION**

[2] As of January 1, 2004, the *Personal Information Protection Act* (“PIPA” or “the Act”) applies to provincially-regulated 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 (section 34 of the PIPA).

[3] In response to the information provided by EPS, the Information and Privacy Commissioner initiated an investigation pursuant to section 36 of the PIPA. Under section 36(1)(a) the Commissioner may conduct investigations to ensure compliance with any provision of the PIPA.

[4] The Commissioner has jurisdiction in this matter as NCN is an “organization” as defined in section 1(i) of the Act.

[5] On November 26, 2004, the Information and Privacy Commissioner appointed me to investigate this matter. This report sets out my findings and recommendations.

### **III. FINDINGS OF FACT**

[6] During this investigation I met with EPS and reviewed documents recovered in their investigation. I also met with and interviewed representatives of NCN, including the Privacy Officer, President and CEO, the Edmonton Branch Manager, and the organization's external legal counsel. NCN provided a copy of their internal investigation report, as well as their Employee Handbook and document shredding policy. I also spoke with the credit union's Privacy Officer, and representatives from the furniture and moving companies referred to later in this report.

[7] The records recovered by EPS consist of 29 sheets listing debtor accounts assigned to NCN, and 86 associated collection files.

[8] Personal information on the assignment sheets consists of debtors' names and the amount of the debt. These records date from mid-2000 to spring 2001.

[9] Each collection file includes a cover page as well as documentation supporting the debt. Personal information on the cover pages includes:

- name of debtor, address, home phone number, date of birth
- Social Insurance Number
- financial status (i.e. "bankrupt")
- occupation
- amount of principal owed, annual interest rate on debt, interest accrued, and total debt owed.

[10] In some cases, the cover pages also include basic contact information (name, address, telephone number) for the debtor's family members.

[11] Documentation supporting the debts includes Court Judgments, personal loan agreements, promissory notes, personal loan security agreements, an Alberta Registries Personal Property Registry Verification Statement, personal cheques, and credit card application forms. Personal information contained in these documents includes:

- name of debtor, date of birth, Social Insurance Number, home and business telephone numbers, marital status

- address, length of time at current address, own/rent status, amount of monthly rent/mortgage payment
- occupation, name and address of employer, employer's phone number, length of time employed, monthly income, information about previous employers
- bank name, branch, account number, account balances, value of assets and liabilities, net worth
- information about previous and outstanding loans including name of lending institute, address, branch, account number, reference number, member number, interest rate, amount of loan and payments, number of payments and due dates, term of loan, directions for disbursement of loan proceeds
- vehicle make, model, year and serial number
- credit card numbers, balance, limit
- signature of debtor
- name and contact information of the debtors' relatives, and nature of relationship.

[12] The supporting documents date from approximately 1985 to 2001. When recovered, the records were in folders labeled by year.

[13] EPS first heard of the records on October 25, 2004, when a source reported they had been found in a dumpster at 107<sup>th</sup> Street and Jasper Avenue, Edmonton (NCN's former premises). The source claimed the records were found on or about October 24.

[14] The individual who eventually turned the records in to police confirmed this report, stating that the records were obtained from a third party, who found them in a dumpster at that location. EPS believes it unlikely the records were in criminal hands for very long before being reported to police.

[15] NCN believes the information breach occurred sometime during the organization's move to new premises, which took place between early June and the end of October, 2004.

[16] On June 4, 2004, a moving company contracted by NCN transported documents, computers, two shredding bins and small items of equipment from the old premises to the new location. The following were left behind:

- workstations, desks and chairs
- a number of filing cabinets
- broken equipment (i.e. keyboard, monitors)
- "archived files" left in a secure storage area
- a box used to collect records to be shredded.

[17] After-hours access to the old premises required a key and an individualized code to deactivate an alarm that was set off when the door was opened. Records provided by the alarm company indicate there was no access to the premises from approximately June 10 onwards. However, NCN reported that the premises were accessed on at least the following occasions after June 4:

- the NCN Branch Manager completed a weekly walk-through.
- the Branch Supervisor – Retail entered the premises to retrieve an archived file (date unknown).
- on or about October 15, the Branch Manager was on-site to meet with an office furnishings company regarding their purchase of furniture items that had been left behind. Arrangements were made to have the items picked up on October 22.
- on October 22, three NCN employees entered the premises to empty the remaining filing cabinets and prepare them for pick-up by a moving company contracted by the office furnishings company. Both NCN and the moving company reported that documents in hanging file folders from the filing cabinets were stacked along the floor. An NCN employee reported that these records included some of the credit union's account files, although it is not known whether any of these records were those later recovered by EPS.
- the three NCN employees left the premises early that afternoon leaving the moving company on-site. NCN's Branch Manager reported that he returned later that day to lock the deadbolt and set the alarm (the door self-locked and did not require a key).
- in the latter part of October (likely between October 22 and 29) a cleaning service company was on-site to complete a "final" clean-up.
- on October 29, the three NCN employees again entered the premises to box the records that had been removed from the filing cabinets on October 22. A shredding company was on-site to collect material for off-site destruction, and a number of empty boxes that had been left behind were collapsed and placed in the dumpster. By this date, EPS had already received reports that the records were in criminal hands.
- on October 30, three NCN employees were on-site arranging transport to the new location of three loads of document boxes containing archived administrative records as well as client account files.
- on the same day, 20-30 boxes of old and broken equipment and garbage were emptied into the dumpster on-site. NCN employees reported there were no documents containing personal information in these boxes.

[18] NCN believes the alarm monitoring system was disabled early in June when the phone lines were switched from the old premises to the new location. For a time, the audible alarm was still triggered by on-site motion

detectors, although no signal was sent to the alarm company. Reports by NCN employees suggest that the alarm was not always activated when individuals left the premises.

[19] Further investigations by EPS revealed that the building manager was called to the premises on August 18 by a leasing agent who could not turn off the audible alarm. They reported they were unable to contact anyone from NCN, and so disabled the alarm themselves. There is no evidence NCN was aware this was done, or that the audible alarm was ever reconnected.

[20] NCN believes the records may have ended up in the hands of unauthorized individuals as follows:

- NCN's typical process upon being assigned a new account by the credit union was to enter information about the account into a collection tracking database. Once entered, all documentation was filed in a filing cabinet. NCN believes the records in this case may not have been filed, but instead were kept in a separate file or drawer after being entered in the database.
- NCN believes that, at some point, this separate file may have been placed in a shredding bin, or box used to collect material for shredding.
- some shredding bins had locking mechanisms; others did not. NCN employees report that those that had locking mechanisms were sometimes left unlocked. The box used to collect material for shredding was accessible to all staff.
- the shredding bins were moved to the new premises on June 4, and the box of records remained at the old premises until the end of October. NCN believes that at some time, an unauthorized individual(s) may have removed the records at issue from the shredding bin or box. This could have been an NCN employee(s), or any third party who had access to the premises.

[21] NCN does not believe that the records at issue were found in a dumpster because:

- the organization's internal investigation did not find any evidence that documents containing personal information were placed in the dumpster at any time during the move.
- the records recovered by police were found in a file folder and in good condition, which does not support claims they were recovered from a dumpster.
- NCN believes it is in the interests of the individuals charged as a result of the police investigation to report that the records were found in a dumpster as doing so would protect anyone that may have assisted them in obtaining the documents.

[22] EPS responded that the good condition of the recovered files is consistent with the type of building that they came from and, as the dumpster was in a sheltered location, its contents were not affected by the elements. Further, EPS received two independent reports confirming where and when the documents were found, and the suspect in this case admitted her full involvement to police to her own detriment, lending credibility to her story.

[23] EPS believes it is of note that the NCN records were found along with documents from a credit reporting agency wholly owned by NCN and sharing the same office space. The credit reporting agency's records were maintained separately from NCN records. An employee of the credit reporting agency provided a statement to EPS that these other documents were placed in one of two on-site shredding bins that were later moved to the new premises. However, as EPS sources reported these records were retrieved from a dumpster at the old location, police believe it unlikely the records made it to the new office space. Instead, both the credit reporting agency records, as well as the NCN records, may have remained at the old premises after June 4 and ended up in the dumpster towards the end of October.

#### **IV. ISSUES**

- [24] 1. Did NCN make reasonable security arrangements to protect personal information in its custody?
2. What action should be taken with regard to the individuals whose information was involved in this breach?

#### **V. ANALYSIS**

##### **1. Did NCN make reasonable security arrangements to protect personal information in its custody?**

[25] Section 34 of the PIPA states:

*An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.*

[26] The debtor accounts at issue in this matter were assigned to NCN in 2000 and 2001; personal information supporting the debts was provided at that time. The records were in NCN's custody at the time of the breach.

[27] Prior to the move to new premises, NCN had a number of security safeguards in place, including the following:

- after-hours access to the old premises required a key and an individualized alarm code. A limited number of employees had entry cards to the building, and even fewer had keys and key pad access.
- motion detectors were on-site and a security company monitored access to the premises.
- there were two shredding bins on site, and regular monthly pickups by a shredding company. Only three employees had access to keys to the shredding bins.
- the storage area at the old premises was locked and access was limited.
- employees were required to sign a form acknowledging “receipt of the Privacy Act” and agreeing to adhere to guidelines. They were also required to sign another document agreeing to protect and limit their use of confidential information.
- all employees received a copy of the Employee Handbook containing NCN’s policies for Proprietary and Confidential Information, Personnel Records and Employee Privacy, and Security and Loss Prevention.
- an email was sent to all staff in December 2003 providing information about new privacy legislation.

[28] The following additional security measures were implemented during the organization’s move to new premises:

- employees were required to pack their desk contents in plastic bins that were secured with plastic ties. Each bin was numbered to help ensure it was delivered to the appropriate space in the new location.
- NCN staff followed the movers on June 4 when they transported materials from the old premises to the new location and were therefore able to confirm the movers did not make any unscheduled stops along the way.
- between June 4 and the end of October, the NCN Branch Manager completed a weekly walk-through of the old premises.
- an NCN employee supervised the shredding company on October 29 when they collected materials for shredding. The shredding company provided NCN with a certificate of destruction.

[29] Despite these measures, personal information that had been in NCN’s custody was found in the hands of unauthorized individuals. A number of factors contributed to put these records at risk.

[30] Before the move to new premises, access to the credit union’s debtor account files was restricted to collectors and tracers in NCN’s Retail Department (approximately 12 individuals at any given time). However,

these records were filed in an unlocked cabinet located in a central filing area, potentially accessible to staff working in other departments.

[31] Although it was intended that staff would use the two shredding bins on site to destroy all records, the procedures in place did not ensure security in the shredding process. Boxes at employee workstations used to collect materials for shredding were not secure; shredding bins were left unlocked at times. There was no written records destruction policy or procedure.

[32] Between early June and the end of October, records containing personal information were left behind at the old premises in an unlocked filing cabinet, and then on the floor, and in an open box. Although an NCN staff member completed weekly walkthroughs of the old premises, nothing was done to secure these records, which were accessible to anyone entering the premises.

[33] As alarm monitoring was disabled early in June it is not possible to state conclusively who had access to the premises during the time of the move. However, it is known that during the move the premises were accessed by NCN employees, as well as a number of third parties

[34] Most of these third parties were unsupervised at some point. Only the NCN employees had signed documents committing to maintain confidentiality of personal or business proprietary information to which they might have access.

[35] Finally, NCN employee reports suggest the premises alarm was not always activated during the period from June to the end of October. EPS obtained statements that the audible alarm was disconnected by the property manager in August, although NCN was not notified.

[36] Based on these factors, I find that NCN contravened section 34 of PIPA by failing to make reasonable arrangements to protect personal information in its custody. As a result, records containing personal information were at risk for access by unauthorized individuals.

## **2. What action should be taken with regard to the individuals whose information was involved in this breach?**

[37] After learning of this breach, NCN reviewed its collections database entries for accounts assigned by the credit union between 1993 and December 2004. Database entries were compared against the account files recovered by EPS, as well as NCN's files.

[38] NCN reported to our Office that the credit union did not specify a records retention or return period for accounts; an assignment continued until the debt was collected, or circumstances dictated that it could not be (i.e. bankruptcy, death, etc.).

[39] Of 1429 database entries, 649 were assigned in 1997 or earlier. Of these, NCN has very little documentation on file.

[40] NCN believes it is reasonable to assume that these records were destroyed, as debtor account records were generally kept for 6 years after an account closed, before being shredded. However, there was no written retention policy to this effect, and the destruction of records was not documented and can not be verified.

[41] Of the 780 accounts assigned from 1998 onwards, NCN has documentation for 420 of them. Eighty-six (86) were additionally confirmed recovered by EPS, leaving 274 accounts assigned between 1998 to 2004 for which there is no file documentation. Given the organization's stated 6 year retention policy, it cannot be assumed that these records were shredded. Instead, they may be at risk for unauthorized access.

[42] NCN proposes to contact individuals who were, or may have been, exposed to risk as a result of this breach as follows:

- NCN will send a letter to the last known address of those individuals whose personal information was known to be in the hands of unauthorized persons (the accounts recovered by EPS). The organization will advise the individuals that their personal information was compromised and as a result, they may be at risk for fraud. NCN will also provide information about actions that have been taken to prevent similar breaches from occurring in the future and will offer assistance about how the individuals can protect themselves from identity theft by notifying credit reporting agencies and placing a fraud alert in their consumer reports. A toll free number to contact NCN for more information will also be provided.

- The other 274 individuals whose account documentation is unaccounted for, and who may have been exposed to risk of fraud, will receive a similar letter and information, but will be advised that their personal information may have been exposed to risk.

[43] Due to the nature of the records at issue, NCN recognizes that it may be difficult to locate individuals who were, or may have been, affected by this breach. This is particularly likely to be the case where the outstanding debt has not been collected. However, NCN has agreed to take the same measures in contacting these individuals as they would in collecting the debt. In the event correspondence is returned to the organization, NCN will attempt to contact the individuals by telephone.

[44] At this time, EPS has not reported any instances of fraud that can be traced to personal information from any NCN files. In the event NCN is informed in the future of any actual instances of fraud relating to this incident, the organization will provide those individuals with a one-year credit watch service where available, at no cost to them.

## **VI. RECOMMENDATIONS**

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

- Initiated the action outlined above 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 (this was completed at the time of the move to new premises).
- 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 (all employees will be required to acknowledge this policy annually)
  - Document Storage and Retention Policy (requiring that the destruction of debtor account files be recorded)
  - Document Shredding Policy

- Contracted with a shredding company to supply on-site shredding services.

[46] NCN is also currently investigating ways to restrict the receipt of fax transmissions to during regular office hours only.

[47] In addition to the above, I recommend that NCN:

- Deliver an information session for employees of the Edmonton branch 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 (e.g. the premises alarm is activated, shredding bins are locked, confidential materials are stored securely, etc.).
- Ensure that reasonable controls are in place to protect personal information in the event of any future premises moves.<sup>1</sup>
- Report back to this Office on or before February 28, 2005 regarding implementation of the above.

## **VII. CONCLUSION**

[48] 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 the 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 these weaknesses and obtain sensitive personal information.

[49] 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.

---

<sup>1</sup> The Office of the Information and Privacy Commissioner/Ontario has published a useful guide entitled *Moving Information: Privacy & Security Guidelines*, July, 1997, which is available on their web-site.

[50] I thank NCN for cooperating fully with our Office during our investigation of this matter.

[51] This file is now closed.

Jill Clayton, Portfolio Officer  
Office of the Information and Privacy Commissioner