

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

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

January 28, 2005

**Linens 'N Things
Investigation #P2005-IR-001**

I. INTRODUCTION

[1] 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 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. 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-002, and P2005-IR-003, address issues relating to these other organizations.

[2] Subsequent to the start of this investigation, the OIPC received a formal written complaint from an individual who alleged that Linens 'N Things had allowed the complainant’s credit card information to “get into the hands of identity thieves.” This individual’s October credit card statement showed a purchase made at a bus reservations centre in Calgary. The complainant followed up with the bus company and was told that a bus ticket had been purchased using the complainant’s credit card number.¹ The complainant also reported having made returns to the Linens 'N Things store at the Terra Losa location. EPS confirmed that the complainant’s credit card number was obtained from the LNT return receipts.

¹ Through media coverage of the EPS investigation described above, the complainant became aware that an individual had been charged by the police. Recognizing that the individual charged in the case had the same name as the individual who fraudulently purchased the bus ticket with her credit card number, the complainant contacted EPS and also submitted a complaint to the Commissioner.

II. JURISDICTION

[3] As of January 1, 2004, the PIPA applies to all 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 against such risks as unauthorized access, collection, use, disclosure or destruction (section 34 of the PIPA).

[4] In response to the documents provided by EPS, the Commissioner initiated an investigation pursuant to section 36 of the *Personal Information Protection Act* (“PIPA” or “the Act”). Under section 36(1)(a) the Commissioner may conduct investigations to ensure compliance with any provision of the PIPA. Section 36(2)(e) allows the Commissioner to investigate complaints that personal information has been collected, used or disclosed in contravention of the Act and section 36(2)(f) that an organization is not in compliance with the Act.

[5] The Commissioner has jurisdiction in this case because Linens 'N Things (“LNT” or “the store”) is an “organization” as defined in section 1(i) of the Act. On November 26, 2004, the Commissioner appointed me to investigate this matter. This report sets out my findings and recommendations.

III. FINDINGS OF FACT

[6] During the investigation, I met with EPS, talked to the complainant, reviewed the recovered documents and examined a police report on an earlier LNT incident. I also interviewed representatives of Linens 'N Things, including the company’s Privacy Officer for Canadian operations, the Store Manager for the Terra Losa Shopping Centre (Store 716), the District Regional Manager, the Regional Executive Director, and the organization’s external legal counsel. LNT provided me with their report of the incident, as well as their customer returns and records disposal procedures and employee training protocols.

Documents recovered by Police

[7] 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 contained 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.

[8] Personal information from some of these receipts was consolidated by criminal suspects in a notebook found by EPS. One of the individuals charged confirmed that information had been transcribed from some LNT receipts to this notebook. The same individual subsequently retrieved two bags of additional LNT records and turned them in to EPS. These additional records consisted of:

- customer return receipts
- staff purchases
- voided sales receipts for incomplete transactions, and
- close out balances.

[9] The first bag of additional records contained approximately 96 individual documents that contained identifiable personal information with credit card numbers and approximately 100 individual documents that did not contain credit card numbers. The second bag contained over 200 items. Many of the records in the second bag were illegible, possibly from contact with water and other soiled materials.

[10] All of the records were dated between March and April of 2004 and originated from the LNT store at the Edmonton Terra Losa Shopping Centre location.

[11] Some unrelated documents were present in the second group of records, including a vehicle registration, moving violation tickets and a petty cash receipt from another retail store. The suspect claimed to have obtained the records from a third party, who found them in a waste dumpster. The condition of the second group of documents, as well as the presence of unrelated documents, support this theory.

Earlier Incident – Calgary Trail (South) Store

[12] During this investigation, EPS provided me with a copy of a Police Report dated September 14, 2004. The Report stated that on August 3, 2004, an anonymous individual turned over LNT documents to EPS. These documents dated from May 2004 and consisted of 23 customer return receipts from the company's Calgary Trail South store. Eighteen of these receipts contained credit card numbers and personal information of the cardholder. The others contained debit or cash transactions and personal information. The finder stated that the receipts were found in a dumpster. Several days later, the finder turned in additional receipts, most contained credit card information.

[13] At the time of the incident, the manager of the Calgary Trail store confirmed that all return receipts for the month of May 2004 were missing from the accounting office at the store. He was unsure if the receipts were stolen, or if staff had mistakenly thrown them out. LNT subsequently informed me that the rest of the May records were recovered and returned to the store.

[14] ***Fraudulent use of credit card information:***

- With respect to the incident at the Calgary Trail store, EPS received a complaint from an individual whose credit card number had been repeatedly used to purchase items. The police report indicates that the EPS traced the source of the fraudulently used credit card to the return receipts originating at LNT. EPS provided all credit card numbers from the recovered LNT receipts to the bank to forward to the issuing agencies. The police informed me that these issuing agencies followed standard procedures to notify customers of the possibility of compromise to their credit card information.
- With respect to the Terra Losa store, the individual who complained to our office claimed that her credit card number was used to make a fraudulent purchase in the sum of \$170.99. She confirmed that she had used her credit card to make a return to the Terra Losa store on April 7 and April 26, 2004. Follow up investigations done by EPS and reported to this office on January 3, 2005 show the following:
 - A credit card was used to place an order for tires from a tire store. The tire store became suspicious and did not ship the tires.
 - Another credit card number was used to place an order from a retail store for a baby carriage, and two others were used to place orders with another retail store for gift certificates, all of these orders were caught before they were shipped and charges were reversed.

EPS confirmed that all of these card numbers were traced to customer return records that originated at LNT.

IV. ISSUES

- [15] 1. Did LNT properly safeguard customer information?
2. What is the appropriate action with respect to individuals whose information was involved in this breach?

V. ANALYSIS

1. Did LNT properly safeguard customer information?

[16] Section 34 of the Act 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.”

[17] LNT reported its customer-returns process was as follows:

- One cash register was dedicated to processing returns.
- Only designated staff (the Lead Cashier) were authorized to process returns.
- Refunds were issued in the payment method of the original transaction (VISA, MasterCard, American Express, Debit or cash).
- When a customer returned goods, the Lead Cashier generated two copies of a return receipt.
- The customer completed the return by filling in his/her name and address on one copy.
- The store’s “Manager-on-Duty” (“MOD”) verified each return transaction and signed the return receipt with the customer present. Note: The Terra Losa store had one General Manager and four Merchandise Managers. At any given time, one of these individuals was designated as the MOD. The Lead Cashier processing the return also signed the return receipt.
- The Lead Cashier produced two copies of a thermal receipt using “point of sale” equipment provided by a bank. The thermal receipt printed the customer’s credit card number in its entirety, as well as the card expiry date; numbers were not obscured. The

customer signed the thermal receipt and received one copy of all documentation.

- The second copy of the return receipt was stapled to the second copy of the thermal receipt and was immediately placed in a white business envelope marked “refunds” and was locked in the cash drawer of the return cash register.
- At the end of the day, the cash drawer was collected by the Manager or the Lead Cashier and was taken to a locked office at the back of the store. Only the 5 store Managers had a key to this office.
- Purchases and returns were entered onto the computer and a summary sheet listing the number of cash transactions, credit card transactions, etc. were generated.
- Return receipts were checked off against the summary listing and the list was used to bundle the receipts. One bundle of return receipts represented one day’s activity
- Refund receipts, and mid-transaction cancellations were retained in the cash office for one month.
- At the end of each month, the refund receipts were deposited in a blue bin, also stored in the cash office. One month’s worth of documentation was kept in each blue bin, awaiting shredding which was done once documentation was three months old.
- Shredding was done on the premises once per month by one of the four Merchandise Managers or the Lead Cashier. No one individual was designated to do this shredding. There were no records of the destruction process, or of which staff member carried it out.

[18] *Controls in place at time of incident:*

- Designated staff and a dedicated cash register for store returns;
- Limited key access to returns documentation in the return till cash drawer during store operating hours. Only the lead Cashier and the MOD had keys to cash drawer;

- Controlled access to Manager's Office where cash drawer contents were reconciled at the end of day (only 5 employees had a key);
- Return receipts were reconciled against the daily transaction listing (provided an opportunity to identify any documentation that may have been missing) and summary sheet listing number of cash transactions, credit card transactions, etc.;
- A Manager was required to enter a code (PIN) in order to complete the return transaction.

[19] The retail industry reports that returns of goods transactions are vulnerable to fraud by customers and employees. To this end, the LNT stores have implemented good controls to reduce the risk of fraud **at the return till.**

[20] The store however, did not properly secure the records as they moved through their life cycle (from active, to inactive, through to disposal). The Managers' Office was open to employees, the blue bins were not locked, and the store had inadequate controls in their records disposal practices.

[21] Therefore, I conclude that the organization failed to properly dispose of sensitive customer information by permitting them to be placed in a garbage bin without being securely shredded. I come to this conclusion for the following reasons:

- This investigation, along with circumstantial evidence collected by LNT's internal review and EPS reports, suggest that records were thrown into the regular trash (an industrial garbage bin at the rear of the store);
- Some of the recovered documents had suffered water damage and showed signs of having been in the garbage bin;
- When Police questioned the suspects, they stated that they had received the documents from a "dumpster diver".²

[22] Despite the organization's intention to shred customer information, the absence of proper control procedures for staff to follow permitted the incident to occur.

² According to experts in commercial crime, "dumpster diving" (a term used by criminals to describe rooting through garbage for items of value to them, such as credit card numbers) for business records is a very common source of information for identity thieves.

[23] I find that Linens ‘N Things failed to adequately safeguard personal information of its customers; therefore, the organization contravened Section 34 of the PIPA.

[24] Since this incident, LNT acknowledged the gaps in its records security and disposal procedures and is in the process of implementing the following for all LNT Canadian operations:

1. All return receipts are placed in locked cabinets at each day’s end and logged.
2. At each month end, that month’s logged return receipts are segregated and placed in a locked cabinet.
3. At each month end, the records that are 90 days old are placed in a sub-contractor’s secured box for shredding by a secure, bonded shredding company and destroyed. The destruction is also to be logged.
4. Store manager level authorization is required to access any records which are locked in secure storage.
5. At any point in time, the records for a particular day can be accounted for as being either in specific storage or as having been destroyed.
6. LNT formally appointed a Privacy Officer accountable for the personal information handling practices for LNT.
7. LNT has initiated an internal audit of all of its personal information handling practices and will revise its policies and procedures as required.

2. What is the appropriate action with respect to individuals whose information was involved in this breach?

[25] The organization’s officials agreed that timely notification of customers affected by the breach was important to the company’s reputation. This notification was critical to enable customers to take steps to protect themselves against the serious consequences of identity theft.

[26] Two hundred nine (209) customer return records were recovered by the EPS investigation. This represents approximately twenty two (22) percent of a total of 967 credit card returns for the Terra Losa store

between March 3 and April 28, 2004. This number (967) represents the theoretical maximum number of credit card records that could have been exposed to fraud.

[27] It is not known whether the balance of the 967 customer return slips from the Terra Losa store during this time period were ever in the hands of unauthorized individuals, or if they had been shredded according to store policy. LNT believe that there is minimal chance that the balance of the return records is at risk; however EPS believes some of these outstanding records may still be exposed.

[28] On being informed of the EPS findings, LNT contacted its card-payment-processing service provider of the dates and transaction elements potentially involved; this permitted a quick identification of all card transactions which could be exposed to risk. The service provider engaged the antifraud security practices of the credit and debit card issuer and payment systems, thereby providing added scrutiny over those cards potentially at risk for fraudulent uses. Although fraud involving the balance of the customer return slips cannot be absolutely ruled out, I find that LNT took all actions available to them to mitigate this risk.

[29] With regard to the records found or provided to EPS by the criminal suspects, the individual customers were exposed to different levels of risk of fraud. These levels can be categorized as follows:

Category A: includes customers whose records had been compromised to the degree of actually being used by identity thieves or being compiled in a useful form for identity theft including:

- Several confirmed criminal uses of credit card information
- Several unconfirmed but suspicious criminal uses of credit card information
- A significant number of cases (32) where names and credit card numbers were collected and transcribed by identity thieves into a notebook turned over to the police.

Category B: includes customers whose exposed records included sufficient information to be useful to identity thieves (for example, records which included name, credit card number and expiry dates), including

- 77 credit card returns with legible credit card numbers that could be used for fraud. These records were recovered by EPS.

Category C: includes customers whose records were potentially but not proven to be exposed in sufficient detail for fraudulent use, including:

- 59 debit card returns (debit card numbers but no PIN)
- 24 credit card and debit card returns rendered illegible by water damage.

[30] The individuals whose credit information was fraudulently used or suspected of being used have been contacted by their financial institutions through the EPS investigation and the timely notification of the card-processing system by LNT.

[31] For the remainder of customers, LNT worked with our Office to determine the appropriate response strategy for each category described above. The strategy was based on the following criteria:

- All Category “A” customers will be personally contacted by a LNT official. These individuals will be advised of this incident, offered assistance in notifying the credit reporting agencies and placing a fraud alert in the customers’ consumer reports. These customers will also be provided with a one-year credit watch service, at no cost to them. This offer was extended to the sole complainant in this incident.
- All Category “B” customers will be personally contacted by a LNT official and advised of the incident. These individuals will also be offered assistance in notifying the credit reporting agencies and placing a fraud alert in the customers’ consumer reports. Both category “A” and category “B” customers will be provided with a notice regarding what LNT has done to protect the customers’ information from similar risks.
- Category “C” customers’ information consisted of debit card numbers without PINs or with illegible credit card information. Because their information could not be fraudulently used, LNT found it unnecessary to contact these individuals. LNT did communicate this incident to a card-payment-processor which has notified the respective financial institutions of the customers in Category “C”. It is the position of the financial institutions that they could not directly release the contact information of the customers in Category “C” to LNT. However, these financial institutions committed to take remedial measures deemed necessary to protect their customers’ interests.

[32] In the event that LNT is informed that any of the customers in Category “B” or “C” did have their personal information compromised to the extent of those customers in Category “A” due to this incident, LNT has committed to extend (to these individuals) the full offer provided to Category “A” customers.

[33] LNT also agreed to develop an identity theft notice and post it in all stores and on the company’s web-site. This notice will provide details of this incident and information on what the organization has done to protect customers’ information from further unauthorized access.

VI. RECOMMENDATIONS

[34] I recommend that LNT take the following actions with respect to the issues raised in this investigation:

- Notify individuals whose information was exposed to identity theft, as outlined above;
- Confirm the details of the contract with the shredding company to ensure that proper privacy and security protections are in place;
- Make sure filing cabinets and storage areas can be locked;
- Obtain point of sale 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 this Office within 90 days;
- Strengthen LNT’s corporate-wide privacy and security policies and develop an implementation plan, including training for all employees.

VII. CONCLUSION

[35] 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.

[36] The organization took immediate corrective action during this investigation.

[37] LNT cooperated fully with our Office throughout the investigation.

[38] This file is now closed.

Elizabeth Denham, Private Sector Lead
Office of the Information and Privacy Commissioner