

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

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

April 19, 2006

**Monarch Beauty Supply
[a division of Beauty Systems Group (Canada) Inc.]**

Investigation P2006-IR-003

I. INTRODUCTION

[1] On June 2, 2005, the Edmonton Police Service (“EPS”) received documents from a confidential informant. These documents consisted of financial records and customer credit and debit card sales receipts from a Monarch Beauty Supply store located in west Edmonton. “Monarch Beauty Supply”, is an operating division of Beauty Systems Group (Canada) Inc. (“BSG”). In early September, 2005, the Economic Crime Unit of the EPS brought this matter to the attention of the Office of the Information and Privacy Commissioner (“OIPC”).

[2] In response to this information, the Commissioner commenced an investigation under section 36(2)(f) of the *Personal Information Protection Act* (“PIPA” or “the Act”).

[3] During the investigation, the OIPC also received a written complaint from an individual (“Complainant”) who claimed that BSG had allowed her credit card information to end up in the hands of a suspected criminal who used this information for fraudulent purposes. The Complainant's credit card statement showed one instance of a fraudulent purchase, namely, the purchase of a laptop computer.

II. JURISDICTION

[4] As of January 1, 2004, the PIPA applies to all provincially-regulated private sector organizations in Alberta. The Commissioner has jurisdiction in this case because BSG is an “organization” as defined under subsection 1(i) of the Act.

[5] On September 20, 2005, the Commissioner authorized me to conduct an investigation. This report sets out my findings and recommendations.

III. INVESTIGATION

[6] In conducting this investigation, I met with EPS, spoke with the Complainant, reviewed the recovered documents and examined the police reports. I also spoke with the Human Resources Manager/Privacy Officer and the Western Division Human Resources Manager for BSG. BSG completed an extensive internal investigation and submitted their report of the incident, as well as their privacy policy and procedures, sections of the BSG store operations manual, record retention policy, and internal documents pertaining to privacy and document handling/retention practices.

[7] I note that virtually all of the BSG personnel directly involved with or connected to the incident, including the Store Manager, District Manager and Territory Manager, were no longer employed by BSG at the time the Commissioner notified BSG's Privacy Officer of our investigation. The current Store Manager, District Manager and Territory Manager of BSG were not involved with this incident.

IV. FINDINGS OF FACTS

[8] The Monarch Beauty Supply store in question is located in west Edmonton and was previously owned and operated by Monarch Beauty Supply Company Ltd. ("Old Monarch") which was acquired by BSG on August 27, 2002. Old Monarch was either amalgamated with BSG or dissolved into BSG subsequent to acquisition.

[9] BSG distributes hair care products, nail polishes, make up, and other personal care products. It has a sales force of nearly 1300 consultants across the USA and Canada. There are approximately 800 shops open to customers in the beauty trade industry.

[10] BSG customers must be licensed barbers, beauticians, hairstylist or estheticians, who hold an account with the organization. Although BSG's transactions are only with licensed individuals/entities, many of BSG's customers purchase products as individuals and in a commercial capacity. As such, the investigation involved records of many transactions involving personal information.

[11] The EPS received two bundles of credit and debit card receipts bearing the name, “Monarch Beauty Supply”, with a west Edmonton address. These bundles came from a confidential informant, who is described by EPS as “well placed” within the criminal community.

[12] The first bundle was received by the EPS in late April, 2005, and was destroyed in accordance with EPS policy (unclaimed materials which are not considered exhibits for EPS are destroyed within a specified period of time). EPS contacted the Store Manager of the Monarch Beauty Supply store in question and the organization’s Territory Manager to advise them of the found documents and alert them to the dangers of identity fraud.

[13] The Territory Manager issued a memorandum dated June 2, 2005 to the BSG District Managers to address this matter. As the Territory Manager had been advised that the EPS had recovered most of the documents, he believed that no further action was required.

[14] The second bundle was received by the EPS in early June 2005. It was the second bundle that was brought to the attention of the OIPC.

[15] Once OIPC notified BSG’s Privacy Officer, the organization immediately commenced an extensive internal investigation and fully cooperated with our Office.

[16] During OIPC’s investigation, EPS advised us that further credit card receipts from Monarch Beauty Supply had been recovered in the hands of criminal suspects during an unrelated search in August 2005. Also in October 2005 (in another unrelated search), the EPS recovered additional Monarch Beauty Supply credit card receipts.

[17] EPS explained that the credit and debit card receipts turned over by the informant and found in the hands of criminals were more than likely initially stolen from BSG by an individual who was “binning” (which is the practice of going through garbage bins for records/documents).

Summary of Recovered Documents

[18] Records recovered by EPS consisted of the following:

1046 Customer credit card sales transaction receipts. These documents consisted of sales receipts detailing the customer name, credit card account number, expiry date, type of credit card, purchase price, and signature of the customer.

1560 Customer debit card sales transaction receipts. These documents consisted of sales receipts detailing the account number, expiry date, and purchase price but did not include customer name or PIN.

93 BSG financial transaction records - Daily Transmittals - (daily summaries of the sales transactions for the store). The vast majority of financial records were whole and complete, with some ripped in half. The documents contained customer names.

[19] All of the documents dated from August 2002 to July 2003 and originated from the Monarch Beauty Supply store in west Edmonton.

[20] There were several Daily Transmittals and credit and debit card receipts missing within each month of the specified date range.

Fraudulent Use of Credit Card Information

[21] The Complainant noticed an unfamiliar purchase on her monthly credit statement (\$500 for a laptop computer). The Complainant's credit card company suspected fraudulent activity and immediately cancelled the credit card and issued her a new one. A few weeks later, the EPS notified the Complainant that a criminal had uncovered one of her credit card sales receipts from Monarch Beauty Supply, and used it to purchase the laptop. Subsequently, the Complainant lodged a complaint with OIPC.

V. ISSUES

- [22]
1. Did BSG make reasonable security arrangements to protect customer personal information in its custody?
 2. What action should be taken with regard to the customers of BSG whose information was involved in this security breach?

VI. ANALYSIS

1. Did BSG make reasonable security arrangements to protect customer personal information in its custody?

[23] Section 34 of 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.

[24] Shortly after receiving the Commissioner's letter and speaking with me, BSG initiated an internal investigation and worked with OIPC to determine how the recovered documents came into the possession of criminal suspects.

[25] The Human Resources Manager/Privacy Officer and the Western Division Human Resources Manager, who have primary responsibility for privacy matters within BSG, explained that they first became aware of the recovered documents following the Commissioner's September 20, 2005, notice of investigation.

[26] EPS indicated that they notified the Monarch Beauty Supply Store Manager in late April 2005 regarding the recovered credit and debit card receipts. The Store Manager did not recall the specific date that EPS spoke with her but explained that upon notification she contacted the District Manager, who reported the incident to the organization's Territory Manager for Canada. This manager spoke with EPS and, as a result, believed that EPS had recovered most of the documents. Therefore, he did not notify the BSG Privacy Officer of the incident.

[27] In response, the Territory Manager issued a memorandum dated June 2, 2005 to the BSG District Managers, stating that customer sales receipts had been improperly disposed. The Territory Manager required all Store Managers to purchase shredding devices to ensure that all documents containing customer personal information would be shredded before disposal.

[28] Subsequent to OIPC notifying BSG's Privacy Officer, BSG undertook an extensive internal investigation involving interviews with EPS detectives and BSG personnel, performing site visits and evaluation of existing privacy and record handling policies and procedures.

[29] As a result of its internal investigation, BSG has determined that the Monarch Beauty Supply store in question had been preparing for inventory in late April 2005. The Store Manager and District Manager were present during the preparations for inventory, as well as two employees from another BSG store. The two employees were instructed to dispose of the old sales journals from boxes located in the Store Manager's office. The Store Manager and District Manager believed that the two employees would shred the documents using the existing store shredder, as per operational practice.

[30] BSG believes that instead of carrying out the usual operational practice, the two employees tore the sales journals in half and then placed them in garbage bags which were disposed in the dumpster behind the store contrary to the intended directions regarding disposal of these documents. Although she could not recall with certainty, the Store Manager believes that the locks on the dumpster were broken at that time.

[31] During this investigation, BSG examined the recovered documents, and has come to the conclusion that the documents originated from the disposal during inventory in April 2005 at the Monarch Beauty Supply store. Because of their concern about the impact of the breach on their customers, BSG officials conducted an analysis of the recovered documents to identify the customers who were potentially at risk. It was determined that all the customers at risk were located in Edmonton.

BSG Summary of the Sales Documentation Process

[32] When a customer purchases a product from a BSG store, a transaction record is created by BSG's point of sale (the "POS") system which is installed on each cash register in each store. The specific type of information gathered and record produced varies by the type of payment:

- for cash sales, the POS receipt contains the date and details regarding the product sold (i.e. type, price and quantity);
- for sales on BSG account, the POS receipt contains the above information plus a (BSG) account (i.e. customer) number and invoice number;
- for credit card sales, the POS receipt contains the information contained in a cash sale plus the credit card authorization number. In addition, a separate receipt is generated by the card payment hardware, which is provided by a financial institution. The receipt contains the full credit card number, expiry date, name, authorization number and a space for signature;
- similar to credit card sales, debit card sales result in a POS receipt containing the information contained in a cash sale plus the debit card authorization number and a separate receipt is generated by the card payment software, which is provided by a third party financial institution. This receipt contains the full debit card number.

[33] At the end of each business day, the Store Manager compiles a package of materials (the “Daily Transmittal”) including the sale summaries and credit and debit card, POS and return receipts. The Daily Transmittals are sent to BSG’s head office in Ontario and copies of a portion of the Daily Transmittals (not including copies of individual credit and debit card receipts) are retained in the local office (the “Local Dailies”) and later destroyed according to a document retention policy.

BSG’s Summary of Document Handling in 2002 and 2003

[34] BSG determined the following in relation to the specific incident:

- Prior to acquisition by BSG, Old Monarch shipped the then equivalent of the Daily Transmittals to storage in Surrey, B.C. It is BSG’s practice that no changes to the operations of newly acquired businesses occur for a one year period. This practice was followed in this case and no changes to electronic or paper handling information systems were implemented until September 2003.
- The Daily Transmittals up to and including June 2002 are located in the Old Monarch storage facility in Surrey, B.C. The Daily Transmittals from (and including) September, 2003 are located at BSG’s headquarters in Ontario.
- The only documents unaccounted for and potentially exposed consist of customer credit, debit and return information for transactions taking place from July 2002 to August 2003.

[35] BSG has been unable to determine the reason why the Daily Transmittals were not forwarded to either the Old Monarch facility in Surrey, B.C. or to BSG headquarters in Ontario, but remained in the Monarch Beauty Supply store in question, however, BSG believes that it was due to the transition following the acquisition and integration of Old Monarch.

Previous Privacy Training for Employees

[36] In March 2004, BSG held a privacy training seminar for Human Resource Management and other senior management down to the District Manager level (which is the level immediately above the Store Manager). This training was held in Ontario. However, the District Manager involved in this case did not attend the privacy training seminar. The training was not provided to Store Managers.

[37] On November 3, 2004 a memorandum was circulated to all BSG employees reminding them of their privacy obligations in safeguarding customer information.

Findings

[38] Based on my findings and BSG's internal investigation, I find that BSG improperly disposed of sensitive customer information by discarding daily financial records, and credit and debit sales transaction receipts in an unlocked dumpster accessible to the public.

[39] Employees failed to properly destroy records because they did not have specific instructions provided by management personnel.

[40] My finding is based on the following factors:

1. Although BSG was in the process of integrating Monarch Beauty Supply, there was a specific retention and distribution system clearly set out. The Daily Transmittals and credit and debit receipts were to be forwarded to Surrey, B.C. or the BSG headquarters in Ontario. Due to the transition following the acquisition and integration of Old Monarch, the documents remained in the Monarch Beauty Supply Store and were consequently improperly disposed.
2. The Store Manager and District Manager were not diligent in safeguarding the documents which contained sensitive customer information. They believed that the two non-management employees (from another BSG store), would use the shredder to destroy the sales journals. In this instance, the former management personnel gave insufficient instruction on how to proceed with the care and disposal of the documents, despite the organization's memoranda, privacy policies and procedures.
3. Although BSG facilitated a privacy training seminar in March 2004, it was limited to senior managers, excluding Store Managers and front line staff.
4. BSG's file and retention policy, outlining the care and disposal of documents, was not current with respect to the operational practice of shredding. The written policy states, "All documents relating to your store business are strictly confidential. When you are ready to discard any store documents, you must shred them by hand and throw them away. Under no circumstances should any store documents be discarded without being hand-shredded first".

5. Although BSG believed that most if not all of the documents were recovered by EPS, the Territory Manager mistakenly believed that nothing further was required and did not notify the BSG's Privacy Officer. As a result, an internal investigation was not immediately commenced; therefore customers were further exposed to risk of fraud.
6. Subsequently, EPS recovered forty (40) additional Monarch Beauty Supply customer credit card receipts in the possession of two suspected criminals. These credit card receipts originated from the April 2005 incident. The Complainant's credit card receipt was one (1) of forty (40) credit card sales receipts recovered from the suspected criminals.
7. BSG did not take any steps, (other than the issuance of a memorandum reminding managers of the requirement to shred documents), or commence an internal investigation until notification of the Information and Privacy Commissioner's investigation.

[41] I find that BSG contravened Section 34 of the PIPA by failing to follow proper disposal procedures to protect customer personal information. As a result, the documents containing personal information were disclosed to unauthorized individuals, and in one known instance, this information was used fraudulently. Those customers' sales receipts which cannot be accounted for remain at risk of fraud.

[42] Since this incident, BSG acknowledged the gaps in their security and disposal procedures. BSG has made the following commitments and changes to their policies and procedures:

- When made available at a commercially reasonable cost, obtain equipment or software to truncate debit and credit card information printed on customer sales receipts. Until this is implemented, BSG will no longer produce a store copy of individual credit and debit card receipts, rather the only receipt printed will be given to the customer.
- At each day's end, place the Daily Transmittals and Local Dailies in locked cabinets accessible only to the Store Manager and logged into a journal.

- Ensure that the Daily Transmittals (to be sent to BSG's head office in Ontario) be removed only once per week and, upon removal, immediately sent via courier and logged into a journal. The Local Dailies should remain in the locked cabinet; any removal will be logged.
- Records identified for disposal will be: shredded by the Store Manager and inserted into non-clear bags and placed in a locked trash bin or, the shredded documents will be picked up by a bonded third party provider.
- Ensure that at any point in time, the location of daily financial records is accounted for.
- Conduct an onsite security audit for each store and direct Store Managers to acquire locking filing cabinets for records storage.
- Progressively amend receipt handling policies. BSG has determined that they do not require a paper copy of each individual credit or debit payment receipt. This will be accomplished through the changing of the stand-alone payment machines to produce only one copy of the payment receipt given to the customer. Individual transaction credit/debit information will be kept in electronic form only.
- Document the retention and destruction (shredding) of documents, including identification of information held, date of destruction, means of destruction and identity of individual(s) carrying out the destruction. Records identified for destruction will require the signature of the Store Manager and District Manager.
- Require all actual or potential privacy or security breaches to be reported as soon as practicable to the BSG Privacy Officer.
- As a result of the BSG Privacy Officer's physical security review at the west Edmonton store, the organization will ensure that:
 - Locks are installed on the doors of the office and the meeting room; and
 - Locks will be placed on any storage space containing records and be accessible only by the Store Manager.
 - BSG will also review physical security measures at its other locations to ensure proper levels of physical security.

2. What action should be taken with regard to the customers of BSG whose information was potentially affected?

[43] BSG agrees that timely notification of customers affected by the security breach is important to enable their customers to take steps to protect themselves against the serious consequences of fraud and identity theft.

[44] Two thousand six hundred and six (2606) customer credit and debit card sales transaction receipts were recovered by EPS. This represents one thousand and forty six (1046) customer credit card receipts and one thousand five hundred and sixty (1560) customer debit card receipts. The found documents were in the hands of unauthorized individuals and the Complainant was subjected to one incident of fraudulent activity because of the organization's security breach. Some of the original sales receipts within the specified date range remain outstanding and may still be at risk.

[45] In reviewing BSG's customer personal information (customer name, credit card number, type of credit card, expiry date) contained in the found documents, I find that this is high risk personal information. Therefore, it is important that a notification letter be sent to the affected customers in order to provide notice of the security breach and recommend measures to allow BSG customers to protect themselves from harm.

VII. RECOMMENDATIONS

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

- Notify and provide assistance to customers whose personal information has been or could potentially be compromised. BSG offered to broaden the scope of their customer notification to include all Edmonton based customers. The letter of notification will be issued to approximately 1,580 customers.
- The notification letter will outline the incident, suggest steps customers may take to protect themselves and provide the name of the designated BSG representative to address customer concerns.
- Contact the relevant credit card agencies and financial institutions to determine processes to be followed and to ensure coordination and continuity of assistance to the affected customers.

- Conduct further privacy training in document handling procedures, physical security measures, destruction and disposal procedures and training on basic privacy awareness for store employees. In addition, continual privacy training and verbal and written reminders will be periodically provided to all staff.

[47] Provide written confirmation to this Office, on or before May 30, 2006 confirming the implementation of these recommendations.

VIII. CONCLUSION

[48] BSG's retention/disposal and security practices failed to fully comply with the requirements in PIPA. Consequently, unauthorized individuals were able to obtain access to and exploit customer personal information.

[49] Once this matter was brought to the attention of BSG's Privacy Officer, the organization immediately commenced an extensive internal investigation and fully co-operated with our office. Shortly after notification, BSG initiated certain changes and steps in its document handling policies and has implemented or committed to implementing further changes and procedures to security, policies and procedures.

[50] BSG has committed to take appropriate action by:

- Notifying all their customers of the security breach and providing assistance,
- Developing new security and disposal policy and procedures,
- Amending existing policies and procedures as specified in this report,
- Conducting privacy training for all management on the amendments to their existing policies and procedures and new security and disposal policy and procedures, and
- Implementing more rigorous safeguards, and regularly monitoring the effectiveness of these safeguards.

[51] This file is now closed.

Linda Sasaki, Portfolio Officer
Office of the Information and Privacy Commissioner

cc: Complainant