

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

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

February 3, 2005

**Digital Communications Group Inc.
Investigation #P2005-IR-003**

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 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. Investigation Reports F2004-IR-003, P2005-IR-001 and P2005-IR-002 address issues relating to these other organizations.

II. JURISDICTION

[2] As of January 1, 2004, the *Personal Information Protection Act* (“PIPA”) 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 under their control against such risks as unauthorized access, collection, use, disclosure or destruction (section 34 of the PIPA).

[3] In response to the EPS findings, 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 over DCG because it is an “organization” as defined in section 1(i) of the Act. DCG is a cell phone service dealer for Roger’s Wireless and operates 16 stores in the province. The Commissioner does not have jurisdiction over Rogers Wireless because it is a federally-regulated organization. The Office of the Federal Privacy Commissioner of Canada (“OPCC”) regulates telecommunications

companies. The results of this investigation (although restricted to the activities of DCG as a separate and distinct legal entity) will be shared with the OPCC.

[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 the investigation, I met with EPS detectives, reviewed the recovered documents, interviewed the President of DCG, and visited DCG central office and one of the DCG stores.

Documents recovered by police

[7] The documents recovered by EPS consist of 53 Wireless Service Agreements (cell phone contracts). Most documents are the sales copies of a multi-part-form contract. All but three are personal contracts for cell phones; the other contracts were taken out in the name of a business. These “business to business” records do not contain personal information; therefore, they are not subject to the PIPA.

[8] Each cell phone contract contains personal information which may include:

- name, address, cell phone number, home phone number
- e-mail address
- customer’s signature
- two of the following:
 - social insurance number
 - drivers license number
 - credit card type and number
 - bank account numbers
 - Other identification (such as student ID, Passport number, Canadian Citizenship number)
- In addition, the payment option part of the form contained either bank account information *or* the individual’s credit card type and number.

[9] All of the records were dated between October 1 and October 31, 2004 and originated from a variety of DCG stores in the Edmonton area.

[10] One of the individuals charged in connection with the recovered information told EPS that the records were obtained from a third party who found them in a waste dumpster. However, the condition of the records (not torn or soiled) does not support this theory. The police believe these records were found by this third party in early November 2004.

[11] To date, EPS has found no evidence that any of the personal information contained in the cell phone contracts has been fraudulently used.

Previous incidents/thefts

[12] The owner of DCG reported that he had experienced several incidents of employee theft, including three he claimed were reported to EPS in 2004. Two employees were terminated in the summer of 2004 as a result of DCG's internal investigation into these thefts. DCG asserts that they independently obtained security advice from contacts in EPS. On the basis of this advice and as a result of the employee thefts, DCG implemented mandatory criminal records checks for all new employees.

[13] EPS reports that cell phone contracts from DCG in the hands of unauthorized persons had been brought to the attention of EPS several times since February 2003. EPS reports that they informed DCG of these security issues. DCG disputes the number of times that the police brought this to the attention of company officials.

IV. ISSUES

[14] 1. Did DCG make reasonable security arrangements to protect personal information in its custody?

[15] 2. What action should be taken with respect to the individuals whose information was involved in this breach?

V. ANALYSIS

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

[16] 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.”

[17] DCG reported that (before these 2004 incidents occurred) its document management practice was as follows:

- Sales copies (“pinks”) of cell phone contracts were retained in the individual stores for customer contact purposes.
- Other contract copies were forwarded to the central office where accounting staff attach an invoice and enter the transaction into the computer.
- Hard copy documents were filed in the accounting room at the central office (in an unlocked file cabinet). Seven employees work in this area.
- After three months, the paperwork was boxed according to the month, and transferred to an unlocked (but monitored) storeroom above the main floor of the building.
- Once the records were three years old, they were shredded on site by DCG staff.

[18] Prior to the incidents that occurred in the summer of 2004, DCG had few safeguards in place to protect sensitive customer information. The following privacy and security gaps were identified during the investigation:

- Extensive customer credit and personal information (contract documentation) was not adequately controlled between head office and the stores.
- Employee access to sensitive customer information was not restricted. The administrative areas of the office were supervised but open to all employees working at that location.
- The accounting office and inventory storage areas were not secured.
- Although a Roger’s Wireless policy required contract documentation to be retained three years, and then disposed of, there was no documentation of when disposal was carried out, and by whom.
- DCG could not confirm that contract documentation was retained beyond the three year retention period.
- Although the owner acknowledged that there is fraud and theft in the cell phone industry, DCG did not implement background and security checks until the summer of 2004.
- DCG did not have specific privacy policies and procedures.

[19] Subsequent to the incidents in the summer of 2004, and in response to the November 2004 recovery of cell phone contracts by EPS, DCG implemented or committed to implement the following controls:

- Centralized control of all customer contract documentation.
- Development of Human Resources Policies, including confidentiality requirements.
- Required that all employees sign a sales agreement, which includes confidentiality provisions.
- Securing the store room, including construction of a wall to better secure the inactive records storage.
- Plan to implement an electronic system to reduce or eliminate the hard copy documents.
- Implemented a mandatory criminal records check for all new employees.

[20] Despite the new measures implemented in 2004 customer information that had been in the custody of DCG was found in the hands of criminal suspects. This investigation, along with information provided by EPS and DCG, suggests that the records recovered by EPS were either improperly disposed of or (as is suggested by the condition of the records) taken by an employee.

[21] I find that the organization contravened Section 34 of the PIPA by failing to make reasonable arrangements to protect personal information in its custody.

2. What action should be taken in response to the individuals whose information was involved in this breach?

[22] There have been no confirmed incidents of actual credit fraud or identity theft that can be attributed to DCG's cell phone contracts. However, these contracts were in the hands of individuals who have been charged with fraud. At this time, neither EPS nor DCG is able to confirm if there are other DCG records still exposed to risk.

[23] DCG believes that the remainder of the contract documentation from the October 2004 time period has been properly shredded. However, the destruction of these records was not documented and cannot be verified. Should any other documents be brought to their attention, DCG has committed to contact all (estimated 1500) individuals representing the theoretical maximum of all contracts issued during that period.

[24] DCG worked with this office to develop a customer notification procedure for the 50 affected individuals. DCG contacted these customers to advise them of the steps they could take to ensure that their credit information is not fraudulently used.

[25] DCG advised the affected customers of the following:

- informed of the details of the incident;
- informed of what DCG has done to protect customers' information from further unauthorized access;
- offered assistance in notifying the credit reporting agencies and placing a fraud alert in the customers' consumer reports;
- provided with the direct line of a senior official to answer any further questions the customers may have.

VI. RECOMMENDATIONS

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

- Initiated the action outlined above to notify individuals whose information was compromised or potentially compromised. Provide assurance to this office that all 50 customers have been successfully contacted by February 14, 2005.
- Reviewed 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.
- Implemented a policy that at each year-end, a review is undertaken to ensure all records older than 3 years are shredded.

[27] In addition to the above, I recommend that DCG:

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

[28] OIPC visited the DCG offices on February 3, 2005 and is assured that the organization has implemented effective security measures.

VII. CONCLUSION

[29] Neither the EPS nor DCG can absolutely confirm how the individuals charged in connection with the recovered cell phone contracts acquired these documents. However, this Office suspects that the breach occurred because the sales copies were either improperly disposed or were removed from the custody of DCG by an employee of the company.

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

[31] DCG cooperated with our Office during the investigation.

[32] This file is now closed.

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