OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

INVESTIGATION REPORT F07-01

MINISTRY OF SMALL BUSINESS & REVENUE & EDS ADVANCED SOLUTIONS INC.

June 20, 2007

Quicklaw Cite: [2007] B.C.I.P.C.D. No. 13
Document URL:http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF07-01.pdf

Summary: An employee of EDS, a Ministry service provider, was caught improperly browsing through a Ministry computer system for personal information of friends and acquaintances. This had gone undetected because of insufficient technical security measures. The inadequate security measures constituted a breach of s. 30 of FIPPA. Further, by taking more than nine months to notify affected individuals, the Ministry and EDS breached their s. 30 obligations. The Ministry and EDS have since taken significant steps to improve security and to develop employee awareness of, and compliance with, privacy law.

TABLE OF CONTENTS

1.0 INTRODUCTION

[1] In the fall of 2005, an employee of EDS Advanced Solutions ("EDS"), an affiliate of EDS Canada and a service provider to the Ministry of Small Business and Revenue ("Ministry"), was caught improperly browsing through a Ministry computer system for personal information of friends and acquaintances. This had gone undetected because of insufficient technical security measures. As discussed below, the inadequate security measures constituted a breach of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), which requires public bodies to implement reasonable measures to protect personal information from risks such as unauthorized access, disclosure and use. The Ministry and EDA also breached their FIPPA obligations by taking more than nine months to notify affected individuals. The Ministry and EDS have since taken significant steps to improve security and to develop employee awareness of, and compliance with, privacy law, but this report underscores that public bodies and their contractors need to ensure that they have proper systems and technologies in place to protect privacy.

[2] Under s. 30 of FIPPA, public bodies are responsible for ensuring that all personal information in their custody or under their control is secure. This includes ensuring that employees treat that personal information in accordance with FIPPA. Where a breach of privacy occurs, the public body must take prompt action to ensure that the breach is contained and where appropriate to prevent similar occurrences. A recent study of the causes of privacy breaches[1] concluded that 54% of breaches are caused by human error or wrongdoing.[2] The challenge for public bodies—and their service providers—is to develop prevention strategies that take into account human fallibility and wrongdoing. Public bodies and service providers therefore must also develop breach response plans to deal promptly and effectively with privacy breaches.

[3] This report is the product of the investigation by this office ("OIPC"), under s. 42 of FIPPA, of unauthorized access by an EDS employee to personal information of third parties. This report examines the adequacy of protective measures taken by EDS, as contractor, and the Ministry, as public body, under s. 30 of FIPPA. It concludes with findings and three recommendations but makes no order under s.58.

---

[1] A "privacy breach" is any unauthorized access to or collection, use, disclosure or disposal of personal information. See OIPC Guideline, "Key Steps in Responding to Privacy Breaches" at http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf

[2] A recent Alberta Information and Privacy Commissioner Investigation Report P2006-IR-005 states:

> [26] The likelihood of employees failing to adhere to organizational policy and procedure was examined by Palisade Systems Inc., a network and data security company. In its survey of 127 companies who reported data breaches in the United States in the past year, 54% indicated that the breach was a result of "employee error". Thus, an important consideration in designing reasonable security arrangements is that humans are naturally fallible and any personal information safeguards must account for this….

2.0 BACKGROUND

[4] The Ministry is responsible for processing Medical Services Plan ("MSP") premium payments on behalf of the provincial government. The Ministry contracted out the processing of premium payments to EDS effective November 26, 2004. In order to process MSP premium payments, the Ministry requires access to the Registration and Premium Billing Database ("RPBD") of the Ministry of Health ("MOH"). The RPBD contains the personal information of approximately four million users of the public health system in British Columbia. The personal information contained in the RPBD includes name, address, date of birth, personal health number, social insurance number, names and addresses of relatives of listed individuals and information relating to the payment of MSP premiums.

[5] The RPBD is housed on a Ministry of Health ("MOH") server. The Ministry has access to the RPBD through an information sharing agreement with MOH. MSP is administered through Health Insurance British Columbia ("HIBC"), which MOH has outsourced to MAXIMUS BC, a service provider. Under the outsourcing agreement, MAXIMUS BC provides RPBD technical support for HIBC.

[6] On October 18, 2005, the Ministry received a complaint from a woman alleging that a Ministry employee had improperly accessed her personal information. The complainant explained that her ex-husband had told their daughter that he could get her home address through a friend of his at the Ministry, whose identity the complainant knew. This was a serious allegation, as the complainant feared for her safety. The Ministry's initial examination of the database revealed that the named Ministry employee had not accessed the complainant's information on the RPBD, but that an EDS employee had accessed the complainant's records for unknown reasons on October 4, 2005. On October 25, 2005, EDS was notified of the potential breach by the Ministry.

[7] EDS immediately revoked the RPBD access rights of the employee in question (an accounts receivable analyst) and re-assigned the employee to new work. In cooperation with the Ministry's Alliance Management Office,[3] EDS conducted an investigation into the alleged unauthorized access. The investigation team obtained and analysed the database audit logs provided by HIBC and EDS removed the employee's computer and hard-drive for analysis. The team also acquired system access logs, email logs and phone records for further analysis. Further examination of the EDS employee's activities in a 10-working-day window surrounding October 4, 2005 revealed that the employee had inappropriately accessed the personal information of three other individuals. EDS investigators interviewed the employee, who acknowledged accessing the information of three of the four individuals identified in the 10-day window but denied accessing the complainant's personal information.

[3] The Alliance Management Office is the Ministry office responsible for managing the Ministry's relationship with EDS.

[8] A report prepared by EDS dated November 14, 2005 concluded the following:

> Based on the findings of our investigation thus far we have concluded that although most of the employee's access to the database were [*sic*] legitimate, there were unfortunately some unexplained accesses. Following interviews with the employee and in conducting the investigation we have determined that no disclosure of personally identifiable information occurred but it is necessary to modify the employee's behaviour so that this type of activity is not repeated. We have already imposed disciplinary action with the employee.

[9] EDS investigators initially concluded that, although the employee had accessed the personal information, a privacy breach had not occurred, as there was no evidence that the employee had disclosed it to anyone else.[4]

[10] The EDS report nonetheless recommended that EDS:

1. Deliver revised privacy and security education material to EDS employees
2. Reinforce disciplinary processes to achieve the desired behaviour of employees conducting work with personally identifiable information.
3. Reinforce accountability using privacy and security awareness training and internal audits.
4. Implement proactive auditing practices.
5. Review current database usages to assess current activities and address any issues that might exist.
6. Create new education and awareness materials.

[11] On November 18, 2005, the Ministry reported the matter to the OIPC and advised that it would be conducting its own investigation because the Ministry was not satisfied with EDS's report. The Ministry reported to the OIPC on March 10, 2006 that it had completed its investigation but required more time to discuss the results with EDS. The Ministry provided the OIPC with a copy of its investigation report on May 12, 2006.

[12] The Ministry's investigation report consists of two parts: a report prepared by Hooper Access and Privacy Consulting Ltd. ("Hooper Consulting") and a report prepared by Colin Abel, a licensed private investigator. With the assistance of MOH and HIBC, Abel was provided with full access to the computerized access logs of the EDS employee for the months of August, September and October 2005. Abel determined that, during those months, the EDS employee had improperly accessed 64 separate individuals' personal information, in some cases repeatedly. Within those files, the EDS employee had access to the information of a total of 94 individuals.

[4] As reported by Hooper Access and Privacy Consulting Ltd. in a report prepared for the Ministry and dated March, 2006, p. 4.

[13] Hooper Consulting reviewed the results of Colin Abel's investigation and reached the following conclusions:

> Personal information has…been accessed and in accessing the personal information, it has been "used"…. Clearly, the access and use of the personal information is not in accordance with the *Freedom of Information and Protection of Privacy Act*…it has been determined that a substantial breach of privacy has occurred. The breach has potentially affected the privacy of 64 individuals and is clearly in contravention of the privacy provisions of the *Freedom of Information and Protection of Privacy Act* and the privacy obligations under the Master Services Agreement [between EAS and the Ministry].

[14] Hooper Consulting made a number of recommendations, including that the Ministry further review the EDS employee's RPBD access using a further scan of the system. The scan would focus on key names identified in the three-month search and would give the Ministry the ability to assess the extent of any inappropriate accesses by the EDS employee beyond the initial three-month search period. Hooper Consulting also recommended that the Ministry follow up with EDS regarding the recommendations EDS presented in its November 2005 report and recommended that notification of the breach be provided to those individuals whose information was inappropriately accessed by the EDS employee.

[15] The Ministry did not conduct any further scans of the system, but on May 10, 2006 the Ministry advised the OIPC that it planned to notify the affected individuals. However, it was not until July 31, 2006 that notification actually occurred. Between May and July the Ministry developed its notification strategy and prepared its information package and notification letters. The Ministry notified all individuals who appeared to have been targeted by the searches or whose social insurance numbers had been viewed. The Ministry also provided MOH with a list of all individuals whose personal health numbers had been accessed. A total of 27 individuals were notified. The remaining 67 individual names appeared only as part of search results and did not have a social insurance number accessed.

[16] Although EDS initially did not recognize that unauthorized access to personal information is a violation of FIPPA, it is, at the time of this report, common ground that unauthorized access to personal information by an employee is a violation of FIPPA.[5]

3.0 DISCUSSION

[17] Public bodies in British Columbia are under a statutory duty to take reasonable measures to protect the personal information in their custody or under their control.

[5] In addition to the access being an unauthorized use as determined by Hooper Consulting, it was an unauthorized disclosure. In particular, s. 33.1(c) of FIPPA permits public bodies to disclose personal information to employees, including contracted employees where the information is necessary for the performance of the duties of the employee. Allowing an employee access to a system is, in effect, a disclosure of personal information for the purposes of FIPPA. Further, as noted below, s. 30 of FIPPA provides that public bodies must protect personal information from such risks as unauthorized access.

Private companies performing services under contract to a public body take on the legal obligations as prescribed by FIPPA.[6]

[18] Section 30 of FIPPA sets out the legal requirement:

> **Protection of personal information**
>
> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[19] Section 31.1 of FIPPA provides that the requirements and restrictions established in Part 3 of FIPPA, including s. 30, also apply to employees and associates of a "service provider". The term "service provider" is defined in Schedule 2 of FIPPA to mean "a person retained under a contract to perform services for a public body." Because of transitional provisions relating to the application of s. 31.1 of FIPPA,[7] only contracts between a Ministry and a service provider entered into after October 12, 2004, are subject to s. 31.1.[8] Because the EDS-Ministry agreement was entered into after this date, EDS has a direct legal duty, separate from the Ministry's FIPPA duty, to ensure that any information that is in its custody or under its control and subject to FIPPA is reasonably secure as required by s. 30.

[20] There are two issues in this investigation:

1. At the time of the unauthorized access was the Ministry in compliance with s. 30 of FIPPA?

2. Did the Ministry comply with s. 30 of FIPPA in responding to the unauthorized access?

[21] The next section discusses the reasonableness standard imposed by s. 30.

[22] **3.1 The Reasonableness Standard**—Section 30 of FIPPA requires a public body to take all reasonable measures to protect information under its custody or control. In Investigation Report F06-01,[9] dealing with the provincial government's sale of computer backup tapes containing personal information, I said this about the meaning of "reasonable":

---

[6] In this light, any contract with a service provider—particularly those for storage or management services involving personal information—should incorporate FIPPA compliance requirements to ensure that the service provider's actions do not place the public body in breach of its FIPPA obligations. See *Guidelines for Data Service Contracts* (OIPC Guideline 01-02), at: http://www.oipc.bc.ca/advice/Guidelines-Data_services.pdf. Service providers also have an independent obligation to comply with Part 3 of FIPPA by virtue of s. 31.1 of FIPPA, discussed below.

[7] These provisions are found in the *Freedom of Information and Protection of Privacy Amendment Act, 2004*

[8] See s. 23(2) of the *Freedom of Information and Protection of Privacy Amendment Act, 2004*.

[9] [2006] B.C.I.P.C.D. No. 7.

> [49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.
>
> [50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

[23] The need for security will depend on the sensitivity of the information. As also noted in Investigation Report F06-01:

> [52] The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.

[24] The Information and Privacy Commissioner of Ontario last year investigated a privacy breach resulting from unauthorized access to a health information database by a hospital employee.[10] Commissioner Cavoukian found that the hospital employee's unauthorized access to personal information in a database was a "use". She also determined that the use was not permissible under s. 29 of Ontario's *Personal Health Information Protection Act, 2004* ("PHIPA"). She found that the hospital's response to the complainant's concerns expressed at the time of her admission to, and during her stay in, the hospital was in breach of s.12(1) of PHIPA.

[25] Section 12(1) of PHIPA, which sets out the security standard in Ontario for health information, is similar to s. 30 of FIPPA:

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

[26] The Ontario Commissioner found that the hospital had failed to take reasonable steps to protect the personal information in three ways: first, it failed to follow its own

[10] See Order HO-002, available at: http://www.ipc.on.ca/images/Findings/up-HO_002.pdf.

privacy procedure in that it did not immediately protect the electronic record of the complainant using a privacy flag; second, it failed to prevent continued access to the complainant's electronic health record even after the privacy flag was placed on the file; and, third, the hospital failed to take sufficient steps to prevent further dissemination of information obtained by its employee following the breach. Commissioner Cavoukian was satisfied with the audit capacity of the health database in question, noting that clinical information systems do not incorporate stricter access controls because of the need for readily available information in emergency situations.

[27] The Office of the Alberta Information and Privacy Commissioner also recently determined that unauthorized viewing of personal information on a database is inappropriate access within the meaning of s. 38 of the Alberta *Freedom of Information and Protection of Privacy Act.*[11] That provision is equivalent to s. 30 of FIPPA.[12]

[28] **3.2 Reasonable Steps After Breach**—In order to help public bodies and private sector organizations evaluate their compliance with the FIPPA security standard, the OIPC has published four key steps for managing a privacy breach.[13] When a privacy breach occurs, public bodies and service providers need to make every reasonable effort to recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring. The OIPC has applied this standard in our review and evaluation of the Ministry's actions in response to the privacy breach under investigation.

[29] The four key steps public bodies must undertake in managing a privacy breach are:

1. Contain the breach;
2. Evaluate the risks;
3. Determine whether notification is required; and
4. Develop prevention strategies.

[30] The first three steps should occur as soon as possible following the breach, simultaneously or in quick succession.

3.2.1 Contain the Breach

[31] On October 18, 2005, the Ministry received a report of a possible privacy breach. With the assistance of HIBC, the Ministry knew by October 25 that the source of the

---

[11] Investigation Report F2007-IR-003, Office of the Alberta Information and Privacy Commissioner available at http://www.oipc.ab.ca/ims/client/upload/F2007_IR_003.pdf

[12] Section 38 of the Alberta Freedom of Information and Protection of Privacy Act provides: "The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction."

[13] The OIPC has produced a document entitled, "Key Steps in Responding to Privacy Breaches" available at: http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf.

breach was an employee of EDS and not a Ministry employee, as originally suspected. EDS immediately revoked the access privileges of the employee in question and seized her computer for analysis. These were appropriate steps to take in the circumstances and effectively contained the breach once discovered.

3.2.2 Evaluate the Risks

[32] In order to determine what additional steps are immediately necessary, public bodies are expected to evaluate the risks associated with the breach.

[33] Some of the factors a public body should take into consideration when evaluating the risks associated with a breach are set out in Order P06-04:

> [80] In discussing what "reasonable security arrangements" entail in Investigation Report F06-01, I considered the relevance of the sensitivity of the personal information at stake, the foreseeability of a privacy breach and resulting harm, the relevance of generally accepted or common practices in a particular sector of kind of activity, the medium and format of the record containing the personal information, the prospect of criminal activity or other intentional wrongdoing and the cost of security measures.[14]

[34] In this case, EDS and the Ministry undertook two separate investigations. Once the source of the breach was known, by October 25, 2005, the investigations attempted to determine the duration of the breach, the number of individuals affected and the types of information accessed by the EDS employee. The risks identified by the Ministry were enumerated in Colin Abel's report:

- There were 16 suspicious accesses to information during the three-month period examined. Activities considered "suspicious accesses" were those not supported as business related because there was no account activity posted on or around the date that the accesses were made.
- 160 lines of queries were done by the employee during these incidents.
- The incidents involved 64 separate individuals' files which were accessed in different ways, some repeatedly. The employee accessed the personal information of 94 individuals.
- The EDS employee accessed personal information including addresses, postal codes, dates of birth, names of spouses and children, account information, Social Insurance Numbers and other personal data.
- The EDS employee used personal health numbers of third parties to conduct searches, indicating that the employee had likely done previous unauthorized searches in order to obtain the personal health number of the third parties.

[14] [2006] B.C.I.P.C.D. No. 35.

- The unauthorized access included searches of records belonging to coworkers, former coworkers, neighbours, the EDS employee's family, the complainant and the complainant's family.
- The EDS employee accessed the complainant's records including her address, premium payments and new spouse's name, personal health number ("PHN") and date of birth.
- The browsing occurred over a minimum of three months covered by the audit data (August, September and October 2005). However, given that some of the searches were begun using PHNs, it was likely that the browsing had been occurring for some time prior to August 2005.

[35] Also relevant to the risk assessment was the fact that the employee responsible for the privacy breach was no longer employed at EDS by the spring of 2006. The public body correctly concluded that notification was required in these circumstances and undertook certain preventive measures in an attempt to ensure that future unauthorized browsing could not occur.

3.2.3 Determine Whether Notification Is Required

[36] A number of groups may require notification following a privacy breach. The most important of these are the affected individuals. An important purpose of notification of affected individuals was described in Investigation Report F06-01:

> [106] …In my view, the key (but not sole) consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been disclosed.

[37] In this light, notification to be effective must be given in a timely enough fashion to allow those affected to effectively mitigate the breach's risks. The reasonableness of the timing is measured by whether it is objectively diligent and prudent in all the circumstances.

[38] In this case, it is relevant that the original breach report came from an individual who was concerned that her ex-husband had accessed her home address and who was worried about her safety. By October 25, 2005, the Ministry was in a position to know that the EDS employee had accessed the billing record of the complainant on October 4, 2005. Although it knew this, the Ministry failed to notify the complainant or any other individual affected by the breach until August 1, 2006—over nine months later.[15] This is unacceptable given the complainant's safety concerns, which none of

[15] The OIPC gave the Ministry an advance opportunity to comment on a draft of this report and the Ministry of Small Business & Revenue did so in a June 14, 2007 letter from Michael Carpenter, Chief Information Officer & Executive Director for the Ministry. He stated that the complainant reported the breach and was aware of the name of the EDS employee who accessed the information. He also stated that the complainant participated in an investigation on October 20, 2005, at which time it was determined that her MSP account had been accessed. The Ministry's first report of this breach to the OIPC on November 18, 2005, was verbal and did not include this information. The Ministry subsequently provided

those involved have disputed. There is no doubt that the complainant should have been notified at once: if not on October 25, 2005, then immediately—immediately—after that.

[39] It is also clear beyond argument that the other affected individuals should have been notified within the days following discovery of the unauthorized access. Instead, the nine-month delay meant that any reasonable opportunity for risk mitigation was lost. Accordingly, by delaying notification for over nine months the Ministry and EDS failed to meet their obligations under s. 30 of FIPPA.

[40] It should also be noted that, as pointed out in the OIPC's resources on privacy breaches,[16] the OIPC ought to be notified where appropriate following a privacy breach, taking into considerations such factors as:

- The sensitivity of the personal information;
- Whether the personal information could be used to commit identity theft;
- Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;
- The number of people affected by the breach; and
- Whether the information was fully recovered without further disclosure.

[41] In this case, the Ministry received the report of the breach on October 18, 2005, and by October 25, 2005 had confirmed that the breach had occurred. Yet it failed to report the breach to the OIPC until November 18, 2005, a month after the breach occurred. While FIPPA does not require that the OIPC receive notification of privacy breaches, the OIPC does have authority under s. 42 to conduct investigations to ensure compliance with any provision of FIPPA. Prompt notification to the OIPC aids the OIPC in assisting public bodies and affected individuals, in the case of public bodies by helping them develop effective strategies to mitigate the harms arising from a breach. The best practice is to notify the OIPC promptly of any privacy breach after consideration of the factors listed above.

---

one written update report on March 10, 2006 and two investigation reports. None of these reports to the OIPC indicated that the applicant was aware that it was an EDS employee and not a Ministry employee who had accessed the information and none of the reports indicated that the complainant had any participation whatsoever in the investigations. Finally, in response to a request from this Office for confirmation that the complainant was first notified of the unauthorized access to her personal information (including her home address) in July of 2006, Ministry staff confirmed in a January 30, 2007 email that the complainant was notified verbally on August 1, 2006 and in writing on August 8, 2006. Although Ministry staff also indicated that there might have been earlier communication with the complainant, no further information on this was provided until Michael Carpenter's June 14, 2007 letter commenting on the draft of this report. It remains unclear what the complainant knew and in any case the Ministry's obligation to provide written notification sufficient to ensure that the complaint could adequately mitigate the risks was not satisfied until August of 2006. Certainly there is and can be no argument that the remaining individuals were properly notified in a timely manner—they were not.

[16] See http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf.

3.2.4 Develop Prevention Strategies

[42] To comply with FIPPA's security requirements, a public body should develop and implement prevention strategies. In this case, the breach was caused by unauthorized browsing of a Ministry database by a service provider's employee. The Ministry identified these three prevention strategies in moving forward:

- System Auditing;
- Supervision of Contractor; and
- Policies, Procedures and Training.

[43] Each of these will now be discussed.

System Auditing

[44] The RPBD is known as a "legacy system". It is an older mainframe computer database developed 25 years ago and it has a very rudimentary audit capacity. It does not have any real-time auditing capacity; it is only capable of retrospective audits. In other words, the system itself does not identify inappropriate access or disclosure; instead, someone would have to raise a concern to initiate the audit process. In order to determine if an individual has inappropriately accessed personal information in the database, a software script has to be written by a database expert and historical event logs for a specified time period must then be pulled and reviewed using the script. That process is both time-consuming and labour-intensive. In comparison, a real time audit automatically notifies a public body when certain pre-determined events occur, such as unauthorized attempts to access data, actual unauthorized access to data of identified individuals or repeated access to the same files.

[45] The RPBD system has two further significant technical limitations. First, it does not allow administrators to limit user access to a subset of all persons on the RPBD database. Therefore, once an EDS user is granted access to the RPBD system that user can view personal information of all persons on the RPBD system whether or not viewing of those records is necessary for the performance of the user's duties[17]. However, it is possible to limit, to a certain extent, the information available about each individual.

[46] The second limitation relates to the manner in which data is organized and accessed in the RPBD. Data in the RPBD system is organized by transactions. Each available transaction has a set of data associated with it. If an employee requires the ability to view some (but not all) of the data elements within a transaction, they are permitted to view all of the data elements. Administrators cannot limit access to data in combinations that do not already exist among the available transactions.

[17] This is important because s. 33.2(c) of FIPPA permits a public body to disclose personal information to an employee only where such disclosure is necessary for the performance of the duties of the employee.

[47] As noted above, s. 30 of FIPPA requires a public body to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. FIPPA permits access to personal information by employees and service providers where that information is necessary for the performance of the duties of the individual. In the context of electronic information systems, assigning permissions to access personal information based on the role of the user is a key strategy in ensuring compliance with this legal standard. It is not at all clear how assignment of user access to transactions that include access to personal information that is not necessary for the performance of the duties of the employee complies with FIPPA. The implications of this are clear for public bodies in acquiring information systems that contain personal information.

[48] As the RPBD system is currently configured, it lacks both real-time auditing capacity and the assignment of access to personal information data elements by job duty. As a result, the employee in this case was able to engage in undetected improper access to personal information for a minimum of three months and in all likelihood for a longer period. The technical security of the RPBD system fails to satisfy the requirements of s. 30 of FIPPA. However, as noted below, since this breach occurred, EDS has taken interim steps to monitor the RPBD system that mitigate these s. 30 shortcomings.

[49] EDS plans to discontinue direct access to the RPBD by transferring the data from the RPBD to a new system known as the Revenue Management System ("RMS").[18] The RMS will include an audit system capable of proactive identification of unauthorized accesses to personal information. The RMS also has a more sophisticated means of controlling access to subsets of data. The migration process is targeted for completion in the third quarter of 2008.

[50] EDS has already appointed a full-time systems auditor and implemented a regular audit schedule for EDS employees' use of all systems including the RPBD. The new, regular audit schedule, which began in July 2006, involves searching for patterns of inappropriate access on a regular basis. Even with the implementation of the new RMS, EDS will continue to require a systems auditor to conduct periodic audits to determine inappropriate accesses by authorized users. The implementation of the new RMS is an opportunity for the Ministry to improve the technical security of the system so that it satisfies the requirements s. 30 of FIPPA. We recommend that the Ministry explore the use of real time auditing of inappropriate access for RMS as opposed to the use of a full-time systems auditor to accomplish the same purpose and expect a report to the OIPC from the Ministry on or before September 30, 2007 discussing the relative merits of the two auditing processes and the Ministry's intentions in this regard.

[18] The Ministry reports that indirect access will be required as the RPB is an 'upstream system' in that it feeds data to RMS.

[51] The combination of the appointment of a full-time systems auditor and the implementation of a regular audit schedule are, in the circumstances, sufficient to mitigate the limitations of the RPBD system described above and so brought EDS and the Ministry into compliance with s. 30 of FIPPA upon implementation of these steps.

Supervision of the Contractor

[52] Although EDS has been contracted to carry out various services on behalf of the Ministry, the Ministry remains ultimately responsible for ensuring that all Ministry records are properly protected as required under s. 30 of FIPPA.[19] In order to ensure that Ministry records made accessible to EDS through the contractual agreement are subject to adequate security measures, the Ministry must have in place some mechanism to supervise compliance.

[53] The Ministry provided copies of two schedules to the contract with EDS: Schedule 25 (Privacy Obligations) and Schedule 27 (Privacy Management Plan). Schedule 25 requires EDS to comply with FIPPA. It also includes provisions relating to privacy training requirements, the need for a privacy management plan, the ability for the province to conduct privacy impact assessments and security audits, and setting security standards in accordance with s. 30 of FIPPA. EDS is also required to monitor personnel to prevent and detect security breaches such as unauthorized access. Where non-compliance occurs, EDS must report the steps it proposes in order to address or prevent recurrence of the non-compliance. These schedules satisfy the reasonable security standard set out in s. 30 as they relate to the incident at hand.

Policies, Procedures and Training

[54] The Ministry provided copies of three EDS documents: the confidentiality covenant signed by all EDS employees, the Code of Business Conduct and the EDS Security Policy. All three documents make it clear that EDS employees must protect the confidentiality of personal information, in part by only accessing information for a job-related function and on a need-to-know basis. This standard is consistent with the requirements of FIPPA. Despite this, it is a matter of concern that, following its own internal investigation, EDS concluded that a privacy breach had not occurred because there was no evidence that the EDS employee had disclosed the improperly accessed information. It is the Ministry's obligation to ensure that service providers understand that unauthorized access to personal information is a violation of s. 30 of FIPPA. (As noted above, EDS now understands that unauthorized access of personal information is indeed a violation of FIPPA.)

[19] The OIPC has consistently taken this position, in the context of ASD, since the Commissioner's January 21, 2002 letter to all ministers, reminding them that their ministries' FIPPA obligations continue despite an outsourcing arrangement and asking them to ensure that robust contractual and other privacy measures are built into outsourcing arrangements from the outset. See Appendix 1 for a full copy of this letter.

[55] Following the breach, EDS developed an 11-point Privacy Protection Action Plan. The action items included a combination of revised policies, updated privacy and security training including a reinforcement of disciplinary consequences for privacy breaches, the creation of a hotline to allow staff to report suspected privacy breaches, the hiring of additional privacy and security staff, the development and implementation of a privacy compliance audit plan, an update of the EDS investigation practices for privacy breaches, a review of the current data base usage and a review of potential system improvements to detect inappropriate access in real-time. The Ministry reported that all action items were completed by April 2007.

[56] EDS requires each employee to attend annual refresher privacy and security training, attendance at the training is tracked. Employees are told that unauthorized access to personal information will result in immediate disciplinary action up to and including dismissal. Employees are also required to sign the confidentiality covenant annually as a further reminder of privacy obligations. New employees are not permitted access to any systems until after they have completed the privacy and security awareness training. EDS has also implemented the practice of "privacy walkabouts". This involves senior staff walking around the floor of the organization to identify any practices not in compliance with the confidentiality agreement, the EDS Code of Business Conduct and the privacy and security obligations set out in the contract with the Ministry.

[57] As part of its action plan, EDS developed an Incident Handling Guide. The document is intended to guide EDS staff when a privacy or security incident occurs. The plan describes responsibilities of individual positions and the steps that these individuals must take when a privacy breach occurs. This new guide is a definite improvement for EDS in that it clearly identifies unauthorized access to personal information as a privacy breach[20] and further clearly describes responsibilities by position. This will hopefully result in less delay in containing and mitigating a privacy breach should one occur. Unfortunately, the policy does not adequately address the issue of notifying affected individuals. In fact, the section on notification of individuals is difficult to find and provides that notification of affected individuals may be delayed while the breach is "properly investigated", although the policy does go on to say that notification should be "timely, conspicuous and delivered." EDS and the Ministry should revisit this policy with a view to ensuring that it takes into account the factors set out in the Notification Assessment Tool[21] and with a view to ensuring that EDS staff understand that notification must occur as soon as possible.

[58] In conclusion, the EDS policies, procedures and training changes described above, properly implemented at all times, satisfy the reasonable security standard set out in s. 30. This is subject to the observation that the Incident Handling Guide needs to

[20] The Guide also recognizes that inappropriate collection, use, disclosure or disposal of personal information are also privacy breaches.

[21] The Breach Notification Assessment Tool was created by this office in cooperation with the Office of the Information and Privacy Commissioner for Ontario and is available at: http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf.

be revised to take into account the factors set out in the Breach Notification Assessment Tool, described earlier, particularly with respect to the timing of the notices.

4.0 CONCLUSION

[59] In summary, the OIPC's findings are that:

1. The unauthorized access to the personal information of 94 individuals was a violation of s. 30 and s. 31.1 of FIPPA.

2. The initial breach containment steps were appropriate in the circumstances and effectively contained the breach once discovered, thus complying with s. 30 of FIPPA.

3. The decision to notify affected individuals was appropriate in this case.

4. By delaying notification of individuals for over nine months the Ministry and EDS failed to meet their obligations under s. 30 of FIPPA.

5. The technical security of the RPBD system itself fails to satisfy the requirements of s. 30 of FIPPA. However, the combination of the appointment of a full-time systems auditor and the implementation of a regular audit schedule are sufficient to mitigate the technical limitations of the RPBD system described above and so have brought EDS and the Ministry into compliance with s. 30.

6. The Ministry has in place appropriate contractual provisions that ensure that EDS was subject to an appropriate security standard in this case.

7. The EDS policies, procedures and training changes ensure an appropriate prevention strategy.

[60] A further comment about notification is in order. Where safety is an issue, the importance of prompt notification cannot be over-stated. In future, the Ministry and EDS should, where notification is determined to be appropriate in accordance with the discussion above, notify affected individuals within hours if not days of the privacy breach. Further, where it is appropriate to notify this office of a privacy breach, the notification should occur at the earliest practicable time and in any case within 10 days after discovery of the breach. With respect to the EDS Incident Handling Guide we recommend that it be reviewed with a view to ensuring that it takes into account the factors set out in the Breach Notification Assessment Tool created by the OIPC in cooperation with the Ontario Information and Privacy Commissioner's office.

[61] With respect to the implementation of the new RMS, we recommend that the Ministry explore the use of real-time auditing of inappropriate access for RMS as opposed to the use of a full-time systems auditor to accomplish the same purpose and expect a report to the OIPC from the Ministry on or before September 30, 2007

discussing the relative merits of the two auditing processes and the Ministry's intentions in this regard.

[62] This breach was caused by the unauthorized activities of a single employee. The Ministry and EDS, in the fullness of time, have met the challenge of developing prevention strategies that take into account human fallibility. The OIPC appreciates the cooperation of the staff of both the Ministry and EDS with this investigation.

[63] Catherine Tully, Manager, Investigations and Mediation, conducted this privacy breach investigation and prepared this report.

June 20, 2007

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File: F05-27140

The following is the text of the letter sent to ministers and deputy ministers of the provincial government on January 21, 2002

Alternative Service Delivery – Privacy Issues – OIPC File No. 14569

The government has made clear its intention to explore, and pursue, alternative service delivery models where appropriate, including through the contracting-out or privatization of service delivery. As Information and Privacy Commissioner for British Columbia, I am concerned that the privacy rights of citizens not be lost or compromised in this process.

Alternative service delivery models can improve service delivery and yield cost-savings. The privacy risks should not, however, be underestimated where personal information is being collected, used, disclosed or managed by an outside service provider who is not familiar with legal privacy requirements. Such risks include use or disclosure of personal information by unauthorized personnel, compromised integrity of personal information, accidental disclosure of personal information and improper retention or secondary use of personal information.

Ministries are, of course, subject to the privacy provisions of Part 3 of the [the Freedom of Information and Protection of Privacy] Act, including when they adopt alternative service delivery methods such as contracting-out. On November 14, 2001, my Office issued *Guidelines for Data Services Contracts*, OIPC Guideline 01-02 ("OIPC Guidelines"). These are intended to pro-actively support any initiatives that involve the contracting-out of services involving personal information. A copy of the OIPC Guidelines is enclosed for your information. The OIPC Guidelines acknowledge that a public body cannot, through a service delivery agreement, contract out of its privacy obligations under Part 3 of the Act. I urge you to ensure that your Ministry, in contracting out or otherwise securing private sector provision of services to or for the public, includes appropriate privacy compliance provisions in all contracts involving personal information.

As between any government-developed privacy compliance standard and the Act's requirements, the Act of course prevails. The OIPC will, in discharging its statutory role to enforce compliance with the privacy provisions of Part 3, refer to the OIPC Guidelines for general guidance. The OIPC's disposition of a particular matter will, of course, be determined in each case by the Act's requirements and by the relevant facts (including the nature of the personal information involved and the type of the services or relationship).

In addition, this Office has for years urged public bodies to carry out a privacy impact assessment ("PIA") for each proposed policy, program or legislative amendment. A PIA tool for this purpose may be found on our website, at www.oipcbc.org [now www.oipc.bc.ca]. This tool is designed to allow a ministry to identify, at the earliest stage of policy or program development, any privacy impacts that may be show-stoppers or that should influence design. It makes sense to perform a PIA as soon as possible in the process, as this is more cost-effective in identifying and addressing privacy impacts and ensuring compliance with Part 3 of the Act. I ask you to ensure that your Ministry carries out a PIA for each alternative service delivery proposal involving personal information.

In keeping with this Office's culture of co-operative, pro-active approaches to privacy-compliance, I would be happy to discuss general privacy-compliance issues with you at any time.