

**ALBERTA
OFFICE OF THE INFORMATION AND PRIVACY
COMMISSIONER**

**Report of an Investigation into the
Collection & Protection of Personal Information**

March 5, 2008

**DeVry Canada LLC
(Trade Name: DeVry Institute of Technology)**

Investigation Report P2008-IR-002

I. INTRODUCTION

[1] An individual (“the Complainant”) who had been a student at DeVry Institute of Technology’s Calgary Campus (“DeVry” or “the Organization”) submitted a complaint to the Information and Privacy Commissioner alleging that DeVry failed to adequately protect his personal information. The Complainant’s concerns stemmed from his discovery that someone had submitted a fraudulent credit application to a furniture rental company using his name, some false information, and a photocopy of the Complainant’s actual driver’s license, social insurance card and DeVry student card. The Complainant believed that an employee of DeVry was responsible for this misuse of his personal information.

[2] In response to this complaint, the Information and Privacy Commissioner (“the Commissioner”) elected to conduct an investigation to determine whether the Organization’s activities represented a contravention of the *Personal Information Protection Act* (“PIPA” or “the Act”).

II. JURISDICTION

[3] PIPA applies to provincially-regulated private sector organizations operating in Alberta, including DeVry. PIPA sets out the provisions under which organizations may *collect, use or disclose* personal information, and also places a duty on organizations to protect personal information in their custody or control against such risks as unauthorized access, collection, use, disclosure or destruction.

[4] Section 36 of the Act empowers the Commissioner to conduct investigations to ensure compliance with any provision of PIPA and make recommendations to organizations regarding their obligations.

[5] The Commissioner has jurisdiction in this case because DeVry Canada LLC is an “organization”, as defined in section 1(i) of PIPA, and operates in Alberta.

[6] Pursuant to section 49 of PIPA, the Commissioner authorized me to investigate this matter. This report outlines my findings and recommendations, which may be made public according to section 38(6) of the Act.

III. BACKGROUND AND INVESTIGATION

[7] For clarity in this report, DeVry Canada LLC also operates under the trade name of DeVry Institute of Technology. The Organization is a subsidiary of the American DeVry Inc. Where “DeVry” or “the Organization” is cited, the Calgary Campus of DeVry Canada LLC is being referred to. Throughout this report, the American parent company will be referred to as “DeVry Inc.”

[8] For the purpose of this investigation, I spoke with the Complainant and reviewed his complaint and supporting documents. I also met with DeVry’s campus Privacy Officer, President, and Director of Student Finance. I toured the DeVry Student Finance department and reviewed the Organization’s privacy policy, as well as the parent company’s security and conduct standards. I also communicated with the parent company’s Chief Security Officer. I gathered further information from the Regional Manager of Insta-Rent Corporation (“Insta-Rent”), the recipient of the fraudulent application, and from Alberta Advanced Education and Technology (the department that funds the provincial portion of the student loan program). Finally, I met with the Calgary Police Service Constable conducting a related criminal investigation.

The Complaint

[9] The Complainant in this matter had been a student at the Calgary Campus of DeVry Institute of Technology. On October 17, 2007 he was contacted by a friend employed at Insta-Rent who had, by chance, happened upon a credit application in the Complainant’s name. The friend became suspicious since the information on the application appeared out-dated and provided the name of a sister as a reference, though the Complainant does not have a sister. Attached to the rental application was a photocopy of the Complainant’s DeVry student loan document and a single photocopy of his social insurance card, driver’s license and DeVry student card on one page. After the Complainant was contacted by his friend, he attended the Insta-Rent location and made photocopies of these forms.

[10] The Complainant stated he had not completed a credit application to rent furniture from Insta-Rent or provided a photocopy of his identification and

student loan document to anyone for that purpose. He believed that the photocopy of his identification had been made by DeVry when he was a student there (characteristics of the photocopy were the same) after applying for a student loan. When the Complainant telephoned the number that corresponded to his supposed sister, the number connected to the employee at DeVry who had assisted the Complainant in completing student loan documents. The Complainant suspected that his personal information was improperly obtained from DeVry by the employee and was fraudulently used to rent furniture. The Complainant reported this matter to the Calgary Police Service, the Commissioner, DeVry, and a media outlet.

Police Investigation

[11] The Calgary Police Service advised this Office that the suspect for this incident is the DeVry employee (“the Employee”) who assisted the Complainant with processing his student loan. Police determined that many details provided on the Insta-Rent application were loosely connected to the Employee. Also, the method of payment used to place a deposit against rental of the furniture was traced back to the Employee. At the time this report was completed, the police had concluded their investigation.

Alberta Advanced Education and Technology

[12] According to Alberta Advanced Education and Technology, once students have applied to the provincial and federal government for financial aid, they are responsible for submitting various loan documents during the loan year to the Provincial Student Finance Office and the National Student Loans Service Centre (the “Loan Centres”) throughout the year. If students choose to submit their loan documents through a service provided by Canada Post, they must display valid identification to the appropriate Canada Post representative each time. However, students are also given the choice of mailing these loan documents directly to the Loan Centres instead¹. If they choose to mail the documents to the Loan Centres, students must attach a photocopy of their identification with each set of documents in order to authenticate their identity. Whichever submission method students choose, a portion of the loan documents confirming registration must first be completed by the educational institution in which they are enrolled. Institutions must retain a copy of students’ loan documents.

DeVry

[13] Information provided by DeVry indicated that the Employee was an Online Student Financial Advisor in the Student Finance department. He began work at DeVry in February 2007 and was responsible for assisting online students with development of financial plans to support their studies. This included completing the enrolment portion of loan documents and processing payments. While the

¹ Students at some educational institutions also have the option of displaying identification for examination to an authorized agent of the Provincial Student Finance Office located on-campus who can receive the documents. As DeVry does not have an authorized campus agent, students must either use the Canada Post service or mail their documents to the Loan Centres.

Employee dealt mainly with active online students and former students with outstanding debts to DeVry, he occasionally assisted his colleagues by processing payments on other types of student accounts as well.

[14] To perform his duties, the Employee required access to the paper account files of active online students and inactive students with a balance owing. At the time of this investigation, there were approximately 85 online student files and 10-15 inactive student files with an outstanding balance. These files were housed in a locking filing cabinet next to the Employee's desk. The Employee also had electronic access to all student accounts. The personal information to which the Employee had legitimate access included students' names, addresses, phone numbers, email addresses, personal financial history, account payments, social insurance numbers (SIN), and credit card information.

[15] After completing the enrolment confirmation section of loan documents, DeVry offers to mail them to the Loan Centres on students' behalf so that students need not attend Canada Post, though this option is still available to them. To this end, DeVry's Financial Advisors usually photocopy students' drivers' licenses, social insurance cards, and student cards to attach to loan documents mailed to the Loan Centres. This was done to spare students from the inconvenience of attending Canada Post or making their own photocopies and mailing the documents themselves.

[16] DeVry officials reported that students are often ill prepared and unable to present requisite identification, thus delaying loan processing. As a courtesy to students anxious to receive their loans, DeVry began making extra photocopies of students' identification to keep on file. This was done so that for any subsequent loan documents submitted thereafter (up to four per year), the file copy of identification - provided it was still valid - could be attached. This was intended to be a customer service measure for students that would expedite the loan process. The Employee not only performed this service, but also had access to the paper files containing the identification photocopies.

[17] When the Calgary Campus of DeVry became aware of this incident, the Organization notified the Chief Security Officer of DeVry Inc. in the United States. The Chief Security Officer acts as the single point of contact for corporate security incidents across North America. In response, he assembled an incident response team representing the legal department, internal audit, regulatory compliance, human resources, financial aid, communications, and operations management. The services of an external investigator, financial advisory firm, and law firm were also engaged.

[18] The Employee was terminated from DeVry and the files in the cabinet to which he had access were moved to locked cabinets in a locked file room to which only authorized parties have keys. The door to the file room was also being outfitted with a push-button programmable lock during the course of this investigation.

IV. ISSUES

[19] The issues that will be examined in this report are as follows:

- (a) Did the Organization collect personal information for purposes that are reasonable, in accordance with section 11(1) of PIPA?
- (b) Did the Organization make reasonable security arrangements to protect personal information, in compliance with section 34 of PIPA?

V. ANALYSIS

(a) Did the Organization collect personal information for purposes that are reasonable, in accordance with section 11(1) of PIPA?

[20] The personal information at issue is the data contained on the Complainant's driver's licence and social insurance card which had been photocopied by DeVry. Section 11(1) of the Act states:

An organization may collect personal information only for purposes that are reasonable.

[21] Before sending their loan documents to the Loan Centres, students must have a portion of the forms completed by DeVry for enrolment verification. At that time, DeVry is required by the Loan Centres to collect one copy of these documents for its files. Once this is complete, students may attend a participating Canada Post outlet, display their identification, and remit their loan documents there. Otherwise, DeVry students can simply mail their loan documents to the Loan Centres. If students choose to mail their documents, they must include a photocopy of their driver's licence, social insurance card and student card. This is necessary, according to the Loan Centres, in the absence of an authorized Canada Post representative authenticating student identity (since the Loan Centres are not the subject of this complaint and are not governed by PIPA, I have not examined the reasonableness of this requirement). Throughout any given loan year, a student is required to go through this process of submitting loan documents as many as four times. Also, students must apply for loans on an annual basis in order to receive annual funding.

[22] DeVry's official role in the process, as described above, is limited to completing the enrolment confirmation portion and retaining a copy of loan documents. However, as a service to students, DeVry normally mails them to the Loan Centres on the students' behalf. This service includes photocopying students' identification that must, according to Loan Centre rules, accompany the loan documents. It was one of these photocopies that was used for the fraudulent Insta-Rent credit application.

[23] It is clear that DeVry makes identification photocopies on the students' behalf, for the Loan Centres' purposes, not its own. In fact, it is the students' responsibility to photocopy their identification if they choose to mail their documents to the Loan Centres. By making the photocopies and mailing loan

documents, DeVry is simply assisting students to secure funding for tuition. DeVry's photocopying of identification constitutes a collection of personal information. Provided that collection is limited to the time between making the photocopy and mailing it to the Loan Centres a short time later, I find that assisting students in this regard (at the students' behest) is a reasonable purpose in compliance with section 11(1) of PIPA.

[24] As stated, students must submit more than one set of follow-up loan documents during the year. Students opting to have DeVry mail the material to the Loan Centres would therefore require identification to be photocopied each time. To facilitate this process, DeVry developed the practice of making extra photocopies to keep on student account files. The DeVry Student Finance department's sole purpose for making extra copies is to assist students with possible future loan documents the student might ask to have mailed. This practice was adopted to ensure that students receive their funding expeditiously since delays were being caused by students' failure to come prepared with necessary identification. It was intended to be a convenient and practical customer service initiative; however, in my view, it comes at the expense of the Organization's compliance with PIPA.

[25] Collecting extra photocopies of identification for future loan documents is not required for the immediate purpose of assisting students to submit their loan documents. Nor is it necessary for providing the same assistance in the future, should students once again avail themselves of it. Obviously, some students may not apply for a loan the following year or may not be enrolled at DeVry the next year. Though it may be the Organization's experience that students reapply for subsequent loans, this does not itself authorize DeVry to collect spare copies of identification.

[26] When a student chooses to have DeVry mail his or her loan documents, the Organization's authority to collect the information is restricted to the single transaction of making the photocopy and forwarding it to the Loan Centres with the current documents. DeVry must have distinct authority under PIPA to collect or use personal information for a new purpose beyond this temporary collection. To collect its own photocopies to keep on file, DeVry's purposes must be reasonable, in accordance with section 11(1) of the Act.

[27] I acknowledge that DeVry has concurrent authority to collect some of this personal information for other purposes. For example, the loan documents which DeVry must fill out and retain a copy of already contain the student's SIN, effectively giving DeVry custody of the same personal information (this is not the case for driver's licenses). However, authority to collect personal information for one purpose under section 11(1) of the Act does not extend to any other purposes. An organization must be authorized under PIPA to collect or use personal information for each of its intended purposes.

[28] DeVry is restricted to the authorized function of completing immediate loan documents. Neither students nor the Loan Centres require DeVry to retain identification photocopies for current loan document processing. For future loan documents, students may opt to photocopy their own identification and mail

their loan documents to the Loan Centres themselves, or, may decide to have Canada Post examine their identification, making photocopies unnecessary. In terms of the effectiveness of the practice, in the future, students may no longer be enrolled at DeVry, they may not apply for future loans, or may not be eligible. I also note that students' identification can expire by the time subsequent loan documents may be necessary. In my view, the less privacy invasive method of fulfilling DeVry's purposes is to make photocopies at the time a student agrees to or requests submission assistance. It must also be acknowledged that DeVry does not have use for or require regular access to copies of students' identification cards, or to some of the information contained therein, such as driver's license numbers.

[29] This analysis recognizes that *recording* data from identification cards differs from *photocopying* those documents. Otherwise, the Loan Centres would simply request license *numbers* and SIDs rather than copies of the identification cards. Having photocopies of actual identification cards allows for better authentication of identity, which the Loan Centres are not able to verify if loan documents are not submitted to authorized Canada Post officials. An employee could probably not have perpetrated "identity theft" in this particular case with the Complainant's driver's license *number* and social insurance *number* alone. The fact that someone was able to produce photocopies of real identification cards facilitated the offence by giving credibility to the false claim. Thus, identification in a highly reproducible form is more of a security risk than is collecting the information contained on those cards, as will be discussed in the second issue to be examined in this report.

[30] I am not satisfied that convenience for potential future document submissions satisfies the standard of 'reasonable purpose' for collection of personal information under the Act. Therefore, I find that the Organization was in contravention of section 11(1) of PIPA when it collected additional photocopies of identification documents. Although the activity was intended as a customer service initiative to assist students, it is inconsistent with the Organization's original authority to collect personal information and created an unnecessary security risk for the individuals served, relative to the benefit.

[31] I note that if the Organization sought to keep copies of students' identity cards intended for the Loan Centres in the future, consent from students pursuant to sections 7(1) or 8 of PIPA would be necessary. Students witnessing and not objecting to extra photocopies being made or being placed in their files does not amount to consent. Of course, these sections of PIPA must be read within the context of section 11 of the Act. As the Act prohibits collection for unreasonable purposes, it is not relevant whether the Complainant consented within the meaning of section 7(1) or 8 to the collection or not: the Organization is prohibited from collecting identification photocopies if its purpose for collection is unreasonable. The limit section 11(1) places on the collection of personal information would have no purpose if individuals could consent to the unreasonable collection of personal information.

[32] My determination is therefore restricted to the finding that DeVry did not have a reasonable purpose for photocopying identification for secondary

purposes that were beyond submitting current loan documents for students, and thereby acted contrary to section 11(1) of PIPA.

(b) Did the Organization make reasonable security arrangements to protect personal information, in compliance with section 34 of PIPA?

[33] Section 34 of PIPA requires the following:

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.

The Act does not detail what constitutes “reasonable security arrangements”; however, the Commissioner’s Office has consistently urged organizations to implement three layers of protection: *physical, administrative and technical/electronic* [e.g. “PIPA Advisory 8: Implementing Reasonable Safeguards”, Investigation Reports P2006-IR-005, H2006-IR-002, H2007-IR-002]. When considering safeguards, organizations should contemplate foreseeable risks; the likelihood of damage occurring; the potential harm caused by a security breach; the sensitivity of the personal information; costs, and established industry standards.

[34] DeVry Inc. maintains a set of security standards and a code of conduct and ethics that apply to all North American DeVry campuses. These standards are thorough and describe sensible security measures. The security standards address mainly technical issues, but also cite generalized prohibitions against unauthorized access, disclosure or duplication of information. The standards recommend a multi-tiered document classification system for records categorized by levels of sensitivity or confidentiality. Personally identifiable information must be “protected to prevent identity theft” and access to both physical space and information must be “restricted according to business needs.” An Incident Response Team must also be maintained and a breach response protocol is in place. Another recommendation is for a termination agreement so that departing employees are reminded of the requirement to maintain confidentiality after employment ends. The code of ethics requires that:

...all DeVry employees, officers and directors should maintain all proprietary or confidential information in strict confidence, except when disclosure is authorized by the Company or required by law. Unauthorized use or distribution of proprietary or confidential information violates Company policy and could be illegal... Safeguarding Company assets is the responsibility of all employees, officers and directors.

[35] Taken together, these security and conduct standards prohibit improper collection, use and disclosure of personal information and require that it be protected. A reporting and investigation mechanism for security concerns is also in place and consequences for violations are established.

[36] DeVry provided me with its own comprehensive privacy policy for the Calgary Campus which includes a description of accepted collection, use and disclosure practices in greater detail. It complements the overall corporate standards of DeVry Inc. The privacy policy also describes various safeguards that are required to protect personal information in DeVry's custody in Calgary. Highlights from the policy include the following:

- (a) Employees must sign a confidentiality agreement.
- (b) Each department must maintain a "Privacy Information Reference Manual."
- (c) A campus-wide annual review of departmental privacy compliance must be conducted.
- (d) Verbal consent obtained by employees from students must be documented on student files.
- (e) Notification to students about the purposes for any collection of personal information during the financial aid process must be identified in writing.
- (f) All employees must be provided with an "orientation from the Department Head in consultation with the Privacy Officer regarding their responsibilities and requirements under privacy legislation".
- (g) This orientation must be documented on "the new employee checklist."
- (h) Access to personal information must be restricted to designated employees who require the information to perform regular duties of their job.
- (i) All student and employee records must be secured at the end of each business day.

[37] A thorough review of the privacy policy revealed that it is detailed and comprehensive and represents sound practices. Since these are the relevant safeguards already contemplated by DeVry through its own policy, I considered whether together they would constitute "reasonable security arrangements" for protecting photocopied identification, as required by section 34 of PIPA. In doing so, I examined implementation or adherence to these intended safeguards and I found that DeVry's compliance with internal policy was inadequate. For example, with respect to the requirements outlined above, I found the following:

- (a) The Employee involved in this case did not sign a DeVry confidentiality agreement, as required.
- (b) The Student Finance department did not have a "Privacy Information Reference Manual", as required.
- (c) The annual review of departmental compliance with privacy legislation did not include an examination of compliance with DeVry's own privacy policy.
- (d) Verbal consent obtained from the Complainant to photocopy multiple copies of his identification to keep on file was not documented on the Complainant's file, as required by policy.
- (e) There was no written notification to students about the purposes for retaining copies of identification, as recommended by policy.
- (f) The Employee was not provided with an "orientation from the Department Head in consultation with the Privacy Officer regarding responsibilities and requirements under privacy legislation", as required.

- (g) No orientation was documented for the Employee on “the new employee checklist.”
- (h) In the present case, the Employee was authorized to access the student account files.
- (i) Student account files *were* secured in a cabinet that was locked nightly and only the Employee and his supervisor had a key.

[38] Since this issue is related to paper photocopies of identification, I did not consider any technical safeguards or examine DeVry’s specific electronic safeguards. In terms of physical safeguards, the identification photocopies are placed in each student’s account files housed in a file cabinet that is locked nightly. Otherwise, the cabinet remained unlocked in the Employee’s cubicle during the day. Given the sensitivity of the personal information, and the fact that the Student Finance area is accessible to students - albeit to quite a limited extent - and to other staff, I do not find this to be a reasonable physical security arrangement. After this incident, the Organization voluntarily addressed this issue by moving account files to a centralized file room with a door locked by a key punch access mechanism and with locking filing cabinets, representing a more reasonable protection measure.

[39] Generally, administrative safeguards might include ensuring that employees:

- are properly trained in privacy and security,
- are required to review company policy about acceptable activities,
- are trained to understand their particular job duties as they relate to collection, use, and disclosure of the personal information they handle,
- understand the limitations of their access to personal information, and
- are sworn to confidentiality.

Consequences for violations of policy must be established. Administrative safeguards also include periodic compliance audits to ensure the organization is fulfilling its policies to protect personal information. Although DeVry’s policy required these measures, the Organization did not actually implement them.

[40] An organization safeguards personal information through policy requirements that set down security standards; however, DeVry’s lack of compliance with its own policies represented a failure to implement reasonable security arrangements. Although the Organization made some reasonable security arrangements in its policy, when internal policies are not enforced or taken seriously, an environment that inhibits unauthorized collection, use or disclosure cannot be fostered. Policy enforcement is critical for creating a privacy ethos within an organization. Merely having written security policies is not sufficient. Specifically, the Organization is unable to verify whether the Employee reviewed its internal privacy policy, as he was not required to sign it.

[41] The Employee did not sign a confidentiality agreement which informs staff that unauthorized copying, use or disclosure of personal information is prohibited. DeVry’s confidentiality agreement requires signatories to commit to

keeping personal information confidential, but in this case the Employee made no such commitment. Requiring employees to do so can demonstrate the importance placed on privacy by an organization. DeVry Inc.'s security standards also require termination agreements that serve a similar purpose, but this was not generally enforced.

[42] The Employee did not receive required training about his responsibilities under privacy legislation which would have addressed proper consent, collection, and security practices for personal information. An employee trained in privacy or with a working knowledge of DeVry's policies may have recognized that the procedure related to identification photocopies did not adhere to policy mandating that consent be documented and notice of purpose for collection be provided in writing. Perhaps the fact that the collection did not meet statutory requirements might have been raised by staff better acquainted with privacy. One aspect of security arrangements under section 34 includes making reasonable security arrangements to protect against unauthorized collection of personal information.

[43] Although DeVry's policies dictated that departments must maintain their own privacy reference manual, none existed in the Student Finance department. Such a document would address specific aspects of the department's business and describe authorized collection, use and disclosure procedures. A departmental manual would bring clarity to the abstraction of corporate security standards and campus wide privacy policies that are difficult for employees to put into practice. This would avoid confusion about what the authorized practices are with respect to protecting personal information maintained in that department.

[44] DeVry's mandated compliance audits should have also identified the fact that consent was not being documented, as policy required, for collection of photocopies of identification. Moreover, during the audit, the question of whether there was authority to collect the information in the first place might have been raised. This suggests an insufficient audit mechanism to identify security threats.

[45] I also examined other issues not specifically cited in the Organization's policy and found other deficiencies. For example, DeVry's hiring practices do not require thorough past employer reference checks for employees with access to sensitive personal information, such as those in Student Finance. I also found no privacy and security policy reminders or refresher training offered to Student Finance employees. All of these would constitute reasonable administrative safeguards.

[46] I acknowledge that these measures may not have prevented an employee from using personal information accessed from DeVry to commit identity theft. Even with a confidentiality agreement or privacy training, an employee may choose to misuse personal information or break the law. I do not suggest that an employee would not know that his suspected actions were illegal or at least unethical because these measures were not in place. However, had DeVry actually employed the measures I described, it would have at least represented

due diligence on the Organization's part and demonstrated to employees a corporate intolerance for privacy violations. The impact of organizational initiatives to express the weight given to privacy and security should not be underestimated. I submit that employees working for organizations that place due emphasis on privacy and security might be more likely to reconsider misusing personal information than those whose employers do not.

[47] The Employee in this case had legitimate, authorized access to the Complainant's account file and other student account files in order to perform his duties. He was specifically required to process payments and loans and needed access to student account files to do so. Thus, I do not find that the Employee's access to the Complainant's loan file itself represents a contravention of PIPA. Similarly, loan documents must be accompanied with proof of identity and SIN cards, so the Employee presumably had authorized access to the Complainant's SIN and personal information contained on his driver's license.

[48] It is recognized that an employee would have had opportunity to make a photocopy of the Complainant's identification even if extra copies were not being made for the DeVry file. It is unclear whether the Employee did so, or simply may have taken an existing file copy. Regardless, DeVry's customer service initiative resulted in most student loan files containing multiple copies of students' social insurance cards and drivers' licenses. Students were made especially vulnerable by the utility of this information for the commission of identity theft. Since the collection of these photocopies is not reasonable in the first place, it poses an unreasonable security risk that does not comply with section 34 of the Act. Employees of DeVry simply do not require access to identification unless a student requests that identification be photocopied on his or her behalf. In such cases, access is only limited to the time between making the photocopy and sending loan documents. Thus, DeVry's practice creates unauthorized year round access to personal information by employees that ought to have been avoided for compliance with section 34 of PIPA.

[49] It is important to note that section 34 may be contravened without actual unauthorized access or real incidents of misuse occurring. The Act requires an organization to make reasonable security arrangements to protect personal information. That a case of identity theft actually arose here clearly demonstrates the consequences of improper security, but it did not need to transpire for a finding of non-compliance. In other words, my findings would be the same whether or not an employee committed this offence. Conversely, an employee's improper access, use or disclosure of personal information does not necessarily result in a finding of non-compliance. Despite reasonable security measures, a rogue employee may still take advantage of his or her rightful access for improper purposes, as was the case in Investigation Report P2006-IR-004 issued by this Office. In that case, an organization was found to be in compliance with section 34 of the Act despite the actions of a rogue employee. PIPA does not impose strict liability, but the duty to take the reasonable steps it does impose was not met here.

[50] I find that DeVry contravened section 34 of PIPA by failing to make reasonable security arrangements to protect personal information. The

Organization created an unnecessary security risk by collecting highly sensitive photocopies of identification without authority, which created unauthorized access to personal information by employees. Once collected, the Organization failed to properly protect the personal information by implementing adequate administrative and physical safeguards.

VI. RECOMMENDATIONS

[51] In light of my findings, I make recommendations to DeVry as listed below. Many were identified as improvement opportunities by DeVry itself during the course of this investigation. Several were underway before my investigation concluded.

[52] My recommendations are as follows:

1. Cease photocopying student identification for loan files and restrict any photocopies to that which is required to be appended to the loan documents.
2. Securely destroy all photocopies of students' social insurance cards, drivers' licenses and other identification currently maintained on loan files.
3. Move loan files to a secure, centralized location, as opposed to allowing employees to maintain them at their private work stations.
4. Remind any students concerned about having their identification photocopied that they also have the choice of making the photocopy themselves and mailing it with loan documents, or, authenticating their identity at Canada Post.
5. Ensure that prospective employees being considered for positions that require handling sensitive personal information are properly qualified and DeVry takes reasonable steps to be satisfied of their trustworthiness.
6. Ensure that all employees who manage personal information receive periodic privacy and security refresher training (alternative formats such as computer training modules can be considered) which includes reminders about organizational policy. New employees should be trained on hire and informed of how to access DeVry's privacy and security policies.
7. Require all current staff, including faculty, to sign a confidentiality agreement. As a reminder, all employees should sign these agreements annually (perhaps as part of their performance reviews). These confidentiality agreements should address post employment with a pledge not to remove or copy personal information during or after employment.
8. Enhance annual compliance audits to include a review of compliance with DeVry policy and DeVry Inc. standards, rather than strictly minimum legislative requirements.
9. Ensure that employees' fulfilment of the applicable requirements above can be tracked for compliance.
10. Provide the Commissioner's Office with its next privacy compliance audit results.

[53] In response to this incident, DeVry also chose to notify students whose personal information was accessible to the Employee about this incident and offered them free credit monitoring services. Letters updating these students are also planned. The Organization also notified other students about the incident even though their information was not deemed to be at risk.

[54] It is my view that these recommendations will improve DeVry's compliance with not only PIPA, but the Organization's own privacy policy, and will assist in demonstrating to staff and students the seriousness with which DeVry treats privacy and security.

[55] DeVry was cooperative during this investigation and was responsive to the incident. The Organization took the matter seriously and accepted the findings and recommendations outlined. The Complainant was also satisfied with this outcome.

VII. CONCLUSIONS

[56] Only the least amount of personal information necessary to fulfill a reasonable purpose should be collected and it should be retained for the minimum period of time that respects specific business or legal needs. Each of the organization's purposes for collecting personal information must be reasonable. If an organization acts on behalf of an individual in the short term, the organization's authority is limited to the immediate transaction.

[57] Some businesses are in the practice of photocopying identification or collecting identification numbers. The Commissioner's Office has investigated many complaints arising from such practices. In almost all of these cases, this Office's investigations have found that the practice is not in compliance with PIPA. Organizations must carefully consider whether they have a reasonable business purpose for such collection of personal information and whether the activity is otherwise in compliance with the Act. Due consideration should be given to the security risk posed by retention of this information.

[58] This incident demonstrates that copies of identification cards can be used to perpetrate identity theft because some public bodies or other organizations such as banks, must legitimately collect this information prior to granting credit, loans or social benefits.

[59] The Complainant in this case was unusually fortunate that a friend happened to be employed at the very store where his identity was being misused. This matter may have gone undetected were it not for this coincidence. The Complainant could have suffered serious consequences as a victim of identity theft. The Organization took responsibility for protecting other students by notifying them and offering them credit monitoring services. Police also conducted an investigation into the Employee's conduct.

[60] Employees of organizations often have access to highly sensitive personal information. Unauthorized employee access can be addressed with specific

security measures. However, some employees will have legitimate or authorized access to sensitive personal information to perform their jobs. An organization must make reasonable efforts to ensure that these employees receive periodic privacy training, sign confidentiality agreements and are actively held accountable for adhering to security policies. A privacy or security policy is meaningless if employees are not trained to implement and adhere to it. Internal policies should address specific aspects of business and describe particular collection, use and disclosure procedures in terms that are relevant to an employee, rather than platitudes or general statements that employees are expected to interpret. If corporate privacy and security policies are meaningful, relevant and enforced, organizations will consistently succeed in creating a corporate culture that values those broader principles.

Preeti Adhopia
Portfolio Officer