Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F12-02

UNIVERSITY OF VICTORIA

Elizabeth Denham
Information and Privacy Commissioner

March 29, 2012

Quicklaw Cite: [2012] B.C.I.P.C.D. No. 7
CanLII Cite: 2012 BCIPC No. 7
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-02.pdf

TABLE OF CONTENTS

		PAGE
EXECUTIVE SUMMARY		**3**
1.0	**PURPOSE AND SCOPE OF THIS REPORT**	**4**
1.1	Introduction	4
1.2	Investigative process	4
1.3	Application of FIPPA to the University of Victoria	5
1.4	Nature of the Incident	5
2.0:	**ISSUES IDENTIFIED**	**7**
2.1	Were Reasonable Security Arrangements Made?	7
2.2	Were Reasonable Steps Taken in Response to the Privacy Breach?	7
3.0	**REASONABLE SECURITY ARRANGEMENTS**	**8**
3.1	Administrative Safeguards	8
3.2	Physical Safeguards	9
3.3	Technical Safeguards	13
4.0	**RESPONSE TO THE PRIVACY BREACH**	**18**
4.1	What is a Privacy Breach?	18
4.2	Breach Containment	18
4.3	Risk Evaluation	19
4.4	Notification	19
4.5	Prevention Strategies	20
5.0	**SUMMARY OF FINDINGS AND RECOMMENDATIONS**	**22**
5.1	Summary of Findings	22
5.2	Summary of Recommendations	23
6.0	**CONCLUSIONS**	**24**
7.0	**ACKNOWLEDGEMENTS**	**25**

Executive Summary

On Monday, January 9, 2012, the University notified the Office of the Information and Privacy Commissioner of a significant privacy breach. A break-in had occurred sometime during the night of Saturday, January 7th, 2012, at the Administrative Services Building on the University campus in Victoria, British Columbia. The break-in was discovered by a staff member in the afternoon of Sunday, January 8th, 2012, and senior officials of the University as well as members of the Saanich Police were contacted.

Of the items stolen, one was a mobile storage device (USB flash drive) containing a significant amount of personal information relating to current and former employees.

This office decided to investigate the theft of personal information to determine whether the University was in breach of section 30 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") which outlines the obligation of a public body to protect personal information in its custody.

A privacy breach of this magnitude has a significant negative impact on the many individuals affected. Affected individuals are concerned with the potential for bank fraud and identity theft; the trust they have placed in the organization to properly secure their personal information has been damaged.

I have ten findings, the main one being that the University failed to protect personal information in its custody as required by s. 30 of FIPPA. When sensitive personal information is stored on a portable storage device it must be encrypted in order to satisfy the security requirements of FIPPA. The University did meet its obligations under FIPPA in its actions subsequent to this event.

I have made five recommendations that I trust will assist the University in building on its foundations, which will ensure a University-wide ethic of protecting personal information entrusted to its care.

1.0 PURPOSE AND SCOPE OF REPORT

1.1 Introduction

On Monday, January 9, 2012, the University of Victoria ("University") notified the Office of the Information and Privacy Commissioner ("OIPC") that there had been a significant privacy breach. A break-in had occurred sometime during the night of January 7, 2012, at the Administrative Services Building at the University campus in Victoria, British Columbia. The theft was discovered by a University staff member in the late afternoon on Sunday, January 8, 2012.

The thieves went through the two floors of the building, taking laptop computers and other mobile storage devices. They also discovered and removed a small commercial safe. Inside the safe was a mobile storage device containing financial and personal identity information of almost 12,000 current and former employees of the University. As of the date of this report, the device has not been recovered.

1.2 Investigative Process

Given the sensitivity of the personal information and the numbers of individuals affected by the breach, the OIPC immediately initiated an investigation and review pursuant to s. 42(1)(a) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). This section of FIPPA gives the Commissioner the power to conduct investigations to make sure the aims of FIPPA are achieved.

Staff from my office attended at the University of Victoria on Friday, January 13, 2012. My staff first met with the University Secretary and the Manager, Privacy, Access and Policy ("Privacy Manager") and then had a preliminary meeting with most of the principal University staff who had knowledge of the circumstances of the theft and the items that were stolen. With the assistance of the Privacy Manager, my office also collected relevant documentation, such as policies and procedures, notification information and privacy and security information pages from the University website.

On February 17 and 20, 2012, staff from my office interviewed University staff to obtain background into the privacy breach. We were also given a report prepared for the Board of Governors and a draft of the internal review conducted by the University into the incident. My staff also met with the Saanich Police officers involved in the criminal investigation of the theft.

This report is the result of our investigation.

1.3 Application of FIPPA to the University of Victoria

The University of Victoria is a "public body", and so is subject to the provisions of FIPPA by way of the following definitions. The University of Victoria is a "university" under s. 3(1) of the *University Act,* and Schedule 1 of FIPPA defines "educational body" to include a "university" as defined in the *University Act.* Schedule 1 of FIPPA defines "local public body" to include "an educational body", and "local public body" is included in the definition of "public body".

The Commissioner has a statutory mandate to monitor compliance of public bodies with FIPPA to ensure the purposes of the legislation are achieved. The purposes, as stated in s. (2)(1) of FIPPA, are to make public bodies more accountable to the public and to protect personal privacy by, among other things, preventing the unauthorized disclosure of personal information by public bodies.

1.4 Nature of the Incident

On the night of January 7, 2012, thieves removed a glass panel from a door and entered the Administrative Services Building at the University of Victoria. The entrance to the building was not alarmed. The thieves then moved upstairs to the second floor of the building, entering some of the offices. In one of the offices, they found two laptops and a mobile storage device, which they took with them to the lower level. The University has stated that neither the laptops nor the storage device contained personal information. The thieves examined some other areas of the second floor, but did not try to enter the section of that floor where the offices of the President and Vice-Presidents of the University are located. That section of the floor was alarmed.

The University believes that the thieves then returned to the main floor, and once again did not try to enter the section of that level occupied by the University Secretary and other officers, which also has an alarm. Instead, the thieves proceeded to the half of the floor occupied by Financial Services and the Payroll Department. The thieves entered the Financial Services area by breaking a window panel beside the locked door.

Once inside, they inspected a number of cabinets, breaking open a metal storage cabinet and a hanging file cabinet. They also took a tower desktop computer from underneath the front workstation. The University has stated that the computer was used only to access a server, and so did not store any personal information or other data.

The thieves proceeded to remove a wood panel beneath the front workstation. Behind the panel was a small commercial safe. The safe had been secured to the concrete floor, but the thieves were able to readily dislodge the safe from its moorings on the floor and remove it through the back entrance.

Inside the safe was a **mobile storage device**, which contained significant amounts of personal information of past and present employees. The personal information included names, social insurance numbers, banking information and other information associated with the staff payroll. While the payroll data was backed up regularly on a different computer server in a separate secure location, the mobile device was intended, in case of an emergency, to be a "fail-safe" backup in order to continue payroll processes in a normal manner. The mobile device was not encrypted.[1]

Upon discovery of the theft, the University realized the extent of the privacy breach. Officials notified the police, and the criminal investigation is still underway. On January 9, 2012, the University notified my office of the breach, and we provided the Privacy Manager with advice on preparing a notice to individuals affected by the breach.

The University then developed and carried out a comprehensive notification plan to affected individuals, including advice and information about mitigating the risk of identity theft. The University President also commenced an internal investigation and engaged an external consultant to conduct a university-wide review of policies and procedures related to the University's handling of personal information. That review was not complete at the time of writing this report.

[1] Encryption is a process used to make data unreadable to anyone except those who know how to reverse the encryption process. This is usually accomplished by encoding the data with one key and decoding the data with either the same key or a related key.

2.0 ISSUES IDENTIFIED

The issues in this investigation are:

2.1 Were Reasonable Security Arrangements Made?

Did the University fulfill its duty to make reasonable security arrangements to protect the personal information of its past and present employees as required under s. 30 of FIPPA?

2.2 Were Reasonable steps taken in response to the privacy breach?

Did the University take reasonable steps in response to the January 7, 2012, privacy breach as required by s. 30 of FIPPA?

3.0 REASONABLE SECURITY ARRANGEMENTS

Issue 1: ***Did the University fulfill its duty to make reasonable security arrangements to protect the personal information of its past and present employees as required by s. 30 of FIPPA?***

Section 30 of FIPPA requires public bodies to make reasonable security arrangements to protect personal information in their custody or under their control. Section 30 states:

> **Protection of personal information**
>
> 30 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.

"Personal information" is defined in FIPPA as recorded information about an identifiable individual, other than contact information. The personal information compromised in this incident included employee names, social insurance numbers and bank account information for direct deposit (including names of banks, account numbers and transit numbers), along with the amount of the last deposit.

In terms of **personal information**:

> I find that the information contained on the stolen mobile storage device is "personal information" under FIPPA.

Section 30 of FIPPA states that public bodies have a mandatory duty to make reasonable security arrangements that protect against the risks of inappropriate collection, use or disclosure of personal information in its possession.

In the past seven years we have investigated almost 500 privacy breaches, many of which involved the loss or theft of portable storage devices. We have published twelve investigation reports that have considered the meaning of s. 30 of FIPPA. In the most recent investigation report examining the security of facial recognition technology, I summarized the meaning of "reasonable security arrangements" as follows:[2]

[2] Investigation Report F12-01, [2012] B.C.I.P.C.D. No. 5, at paras. 83-85.

> [83] [R]easonableness is measured on an objective basis and while it does not mean perfect, depending on the situation, it may signify a high level of rigor.[3] More recently, I identified two circumstances where a high level of rigor was required.
>
> [84] In Investigation Report F11-01, I examined the standard of reasonableness for an online platform. In determining that a high level of diligence was required I considered the nature of the known security risks to online platforms and the level of understanding of these risks by typical customers. I also took into account, the fact that government involvement increases the public's trust in the security and that the online environment is one of constant change that public bodies must respond and adapt to.
>
> [85] More recently I examined the reasonableness of the security associated with the BC Hydro Smart Meter and Infrastructure Initiative in Investigation Report F11-03[4] and noted:
>
> > [84] Given the increasing sophistication of hackers, all public bodies and organizations need to exercise due diligence in protecting the security of personal information in their custody or under their control. Security of systems requires ongoing vigilance. Public bodies must respond quickly to any identified privacy and security risks. Failure to do so would certainly not meet the requirements of FIPPA. However, reasonableness extends beyond a measure of responsiveness to identified risks. Public bodies must be proactive and implement ongoing monitoring and testing of the security of their systems. Public bodies also must ensure their policies are kept current and that their staff receives regular training.

To meet the reasonableness standard for security arrangements, public bodies must ensure that they have appropriate administrative, physical and technical safeguards. The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, how the costs of security are estimated, the relationship between the public body and the affected individuals and how valuable the information might appear to someone intending to misuse it.

3.1 Administrative Safeguards

The University was aware of its privacy obligations under FIPPA. In June, 2008, the Board of Governors approved the Protection of Privacy Policy. In the same year, the University identified the need for a privacy lead and created the position of Manager, Privacy, Access and Policy, which was filled in December, 2008.

[3] Investigation Report F11-01, [2011] B.C.I.P.C.D. No. 6, at paras. 30-34.
[4] [2011] B.C.I.P.C.D. No. 43.

Appointing someone to be responsible for overseeing the public body's compliance with privacy legislation is critical to establishing a privacy protection program and ensuring that privacy and security controls are in place. It is also critical that senior management support a culture that respects privacy, and this support is reflected in the fact that the Privacy Manager reports to the University Secretary, who reports directly to the University President.

The Privacy Manager, the Information Security Manager and the Associate Archivist developed, and the University adopted, a number of major policies related to Privacy, Information Security and Records Management that are the foundation of a privacy management program. The specific policies were the result of an extensive consultation process. The process began in February, 2009, most of the policies were approved by the Board of Governors in December 2009, and the remainder were approved in December 2010.

Following the adoption of these policies, the Privacy Manager and the Information Security Manager prepared and carried out a series of training workshops, particularly focused on managers and supervisors, to raise the awareness of privacy and security matters related to the university.

Over the past two years, the University has continued to carry out training sessions related to privacy in the classrooms, social media, health services, emails, and cloud computing. The development of a strong policy framework and training program are critical factors in ensuring reasonable security for personal information. The development of these policies and follow up training represents important building blocks in a privacy management program.

While developing comprehensive privacy policies is a vital step in ensuring compliance with appropriate legislation, it is equally important for a public body or organization to continue to bring the program to life. Monitoring and updating personal information inventories, reviewing training programs, continuing to refresh knowledge of staff and making sure that privacy impact assessments and risk assessments are kept as "evergreen" documents are some of the challenges that must be met to ensure that the program accomplishes the required purposes. The University privacy policies have mandated reviews every seven years.

In my opinion, changes in privacy and technological security happen at a more rapid rate, and a seven year period between reviews is too long. I believe that conducting a formal review at a minimum of every three years would enable the University to maintain policies that would meet the accelerating pace of change in information technology. While it may not be necessary to have a formal review on an annual basis, it would be reasonable for the Privacy Manager and the Chief Information Officer to informally review the policies annually.

RECOMMENDATION 1:

I recommend that the University formally review the privacy and security policies at a minimum of every three years.

The policies with associated procedures most relevant to this investigation are:

Protection of Privacy Policy

- Procedures for Responding to a Privacy Incident or Privacy Breach
- Procedures for the Management of Personal Information
- University Information Security Classification Procedures

Information Security Policy

- Procedures for Responding to an Information Security Incident
- Procedures for Addressing Security Vulnerabilities of University Information Resources and Information Systems
- University Information Security Classification Procedures
- Procedures for Responding to the Loss or Theft of Mobile Computing Device

The University Information Security Classification Procedures ("ISCP") provide a way to establish reasonable security arrangements by classifying information with regard to its sensitivity. There are four classes of information: public, internal, confidential and highly confidential. The procedures state that if any information in a system or record is deemed to be at a higher classification level, all the information in the system or the record must be managed at that level of security.

The Procedures for the Management of Personal Information - 52.00 Safeguarding Personal Information recognize that information related to "hiring, termination, or managing the employment relationship" must be treated as confidential. Much of information contained on the stolen mobile storage device would be included in this security classification. The level of safeguards required for confidential information under the ISCP is for it to be "*stored within a controlled-access system* (*e.g.*, password protected file or file system, locked file cabinet)." This is considered a *minimum* standard for the protection of confidential information.

The policy provides examples of security measures, such as password protection and storage of laptops in secured cabinets. However, the policy does not recognize the risks involved with personal information contained on laptops and other portable devices. It does not provide specific guidance on how to reduce or

eliminate the risk by ensuring the security of personal information, and it does not reference the need for encryption of sensitive data. Loss and theft of these devices is a risk well known to privacy and security experts. In fact, the theft of laptops seems to be a virtual epidemic. When the stolen devices also contain personal information, the costs to a public body and the individuals involved can be enormous.

Laptops and other mobile storage devices are, by their very nature, intended to be moved from location to location. However, their portability increases their vulnerability to being stolen or lost. All information security procedures should recognize that the physical characteristics of these electronic devices require more extensive security protection, including encryption, when storing personal information on them. Mere password protection of a device does not create the same level of security as encryption.

A further area of discussion is the amount of personal information contained on the mobile storage device. The University's internal review also raised this issue. The University's Protection of Privacy policy, section 21.00 states that "employees must only seek access and use Personal Information necessary for the performance of their duties." This means that information no longer necessary for the performance of duties should be deleted.

Limiting the amount of data stored on a mobile device or in other information systems reduces the negative effect of a privacy breach. The device contained the information of a large number of past employees. I understand that the Financial Services group that created the mobile storage device considered the question of how long personal information should be stored on such devices. However, the Financial Services group did not have clear criteria for what data to retain or delete, and they erred by including the data of too many former employees. I believe that it would have been prudent to minimize the number of individuals whose data was stored on the recovery device. I also cannot see that any process had been established to review the amount of personal information stored and make alterations.

In my view, the University stored more information than was necessary on the device. It is vital that public bodies and organizations limit the amount of personal information stored on mobile electronic devices to the minimum necessary for current operations, frequently review what is being stored and delete unnecessary information.

In terms of **administrative safeguards:**

> I find that the University has established a strong data governance program, including designating an individual as being responsible for its privacy program. It has developed critical policies and training in its overall approach to the protection of privacy as required under s. 30 of FIPPA.
>
> I find that the University information security policies failed to distinguish between the methods of storage for personal information and to use a sufficiently high standard when rating storage devices such as laptops and other mobile storage devices as required under s. 30 of FIPPA.
>
> I find that the University stored more than the minimum personal information necessary on the mobile storage device and failed to have a process by which the device would be reviewed periodically to limit the amount of personal information to the minimum necessary as required under s. 30 of FIPPA.

3.2 Physical Safeguards

The University has done some good administrative work in building its privacy management program. However, in addition to policy and training, it is necessary to carry out risk assessments of highly vulnerable repositories of sensitive personal information. Physical and technical safeguards must be commensurate with the risks associated with the type of personal information. Moreover, it is important to take a layered approach to physical security. Use of alarms, locks and safes can help ensure that personal information is properly protected.

The University recognized the need for physical security for the mobile storage device containing payroll information. It had installed a safe in the Financial Services area, although primarily for other reasons, such as for storing cash. Nevertheless, the device was stored in the safe, because staff recognized the risk associated with the sensitive data.

I acknowledge that the University placed the device in what was deemed to be a secure physical location. Of course, in the actual event, what was perceived to be a very secure location was not, because the safe was not properly fixed in place. The anchors were not appropriate to prevent the safe being dislodged, and the thieves were able to remove it.

I have an additional concern that the University staff did **not** make a decision to alarm the premises of Financial Services. Although we were informed that a break-in of the premises was considered an unlikely occurrence in the past, I believe that the amount of personal information housed in the Financial Services and Payroll areas should have led to the recognition of the need to alarm those areas. As well, since the other half of the building already had alarms in place, all areas of the building could have been easily alarmed.

In terms of **physical safeguards**:

> I find that the University's physical safeguards were not reasonable within the meaning of s. 30 of FIPPA because the University failed to properly secure the safe or to alarm an area where significant amounts of personal information were stored.

RECOMMENDATION 2:

I recommend that the University re-assess the physical security of the Financial Services area to determine whether or not it is necessary to alarm the entire building and to assess other buildings on the campus where personal information is stored.

3.3 Technical Safeguards

In Investigation Report F06-01,[5] former Commissioner Loukidelis provided a number of factors to consider when conducting risk assessments to determine if certain practices meet the definition of reasonable security. In relation to technical safeguards, I believe that there are four factors with particular relevance to this event: the sensitivity of the personal information; the medium and format of the records; the interest in the data for criminal activity; and the cost of security measures.

Firstly, the sensitivity of the personal information compromised in this incident is a vital consideration. The information was of extreme sensitivity, because of both the large number of data elements and the various ways that the data could be misused if it were lost or stolen. The personal information is valuable not only as separate items, but can also be much more valuable when a number of data elements are combined.

It is also significant that the information was collected by the University as an employer. The information was supplied by employees as part of the employment relationship. Employees are required to supply this sensitive

[5] [2006] B.C.I.P.C.D. No. 7.

personal information – they cannot get paid if they do not supply such information as their social insurance numbers. Employees trust employers to protect this sensitive personal information. In these circumstances employers must take particular care to guard the personal privacy of their employees.

Secondly, the medium and format of the records must be considered. Personal information held on a small electronic device is at particular risk of loss or theft, and it is possible to widely transfer such information in a very short period.

I am aware that physical security measures were in place to prevent a loss, but the device was not always in a completely secure location, because there were times when it was used in the office areas. For each payroll period, the device was removed from the safe to be updated on a computer in the Payroll Department. When these transfers occurred, the device was vulnerable to theft or loss. A small electronic device will always be susceptible to theft or loss.

Thirdly, it is clear that the type of personal information stored on the mobile storage device is valuable to criminal organizations. In addition to using it for identity theft, criminals can also exploit personal information to impersonate another individual, obtain medical treatment or use the basic information to create a fictitious identity. Reports from world-wide police organizations have demonstrated that identity theft and fraud using stolen personal data have become major criminal activities.[6] Given the nature and volume of the personal information at issue in this instance and its desirability to criminal organizations, my view is that an increased level of security arrangements was required.

Finally, public bodies often raise the issue of the prohibitive cost of security measures as a rationale for not implementing technical security solutions. In Investigation Report F06-01, we noted that these costs are not necessarily a determining factor in ensuring that reasonable security arrangements are used. Indeed, in this event, costs were **not** an issue. The low cost of data security measures, specifically encryption of the mobile storage device, would have allowed this protection to be easily implemented. The personal information contained on the device was highly sensitive.

The decision to use a mobile storage device as a "fail-safe" backup arose out of a security audit of the new enterprise information system, "Banner". The audit expressed concerns that the business continuity plans and disaster recovery plan were not properly implemented. The main issue for the Payroll Department was having the ability to run a manual payroll. An informal group met over several months and decided that a mobile storage device would meet their needs. Interviews with various University staff made it clear that senior staff in Financial Services had considered using encryption on the storage device and in fact had received advice from others that encryption should be used. Further, they

[6] Federal Trade Commission. Consumer Sentinel Network Data Book for January to December, 2010. March 2011.

agreed that encryption was an appropriate security measure. However, although there appears to have been an intention to encrypt the data, it was not carried out.

At the time of this incident, the University had developed a program to offer encryption for laptops that were sold to faculty and staff through a central location. The program was initiated in early 2010. However, the program did not require that an encryption solution be installed on any new laptop and did not address any older model laptop or any other mobile storage device that might have contained personal information. In the end, the University did not have a comprehensive policy, procedure or an institutionally supported encryption solution for all mobile storage devices at the time of the incident. The result was that encryption was **not** a requirement for the Financial Services mobile storage device. A University program that required the use of encryption would have prevented the thieves from accessing the stolen personal information.

When my office investigates privacy breaches involving laptops and mobile storage devices, it has been our practice to consider that properly encrypted devices have sufficient protection from unauthorized access. As far back as 2005, the ISO standard 17799 (Code of Practice for Information Security Management) identified encryption as a best practice for mobile storage devices. Both Investigation Reports F06-01 and F06-02,[7] issued by my office in 2006, identified encryption as a method that should be used for laptops and other mobile storage devices.

Other jurisdictions, such as Ontario and Alberta, have also required that personal information held on mobile storage devices be encrypted. In "*Securing Personal Information: A Self-Assessment Tool for Organizations*," jointly prepared by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and my office, encryption is considered a minimum security requirement for the transportation and storage of personal information

Given the amount and sensitive nature of personal information contained on the University mobile storage device, coupled with the ease of encrypting the information, there is simply no rationale for failing to encrypt this information. Without doubt, encryption is the standard when storing personal information on a laptop or any mobile storage device. The use of encryption must be combined with a strong encryption key. Training of staff must ensure that, if the encryption key is a password, it is properly formatted to contain a minimum of eight characters, employing uppercase, lowercase, numbers and symbols.

[7] [2006] B.C.I.P.C.D. No. 17.

In terms of **technical standards**:

> I find that the University failed to provide proper technical safeguards for the protection of personal information in its control as required under s. 30 of FIPPA.

RECOMMENDATION 3:

I recommend that the University develop a comprehensive policy, procedure, training and technical solution to ensure that personal information stored on laptops and other mobile devices is protected as required by s. 30 of FIPPA. The policy and training program should address data limitation, standard of encryption, appropriate password maintenance, physical security, wireless security and proper disposal.

4.0 RESPONSE TO THE PRIVACY BREACH

Issue 2: ***Did the University take reasonable steps in response to the January 7, 2012 privacy breach as required by s. 30 of FIPPA?***

A privacy breach of the magnitude that occurred at the University has a significant impact on those individuals affected. Whether they are employees, clients or customers, individuals have to put their faith in public bodies and organizations to properly secure the personal information these individuals are required to provide.

When a public body fails to protect this trust, it creates a negative impact which is beyond the control of affected individuals. In this breach, the stolen device contained names, social insurance numbers and banking information. Affected individuals have expressed great worry and frustration about the compromise of this data. They have rightly experienced significant concern about the potential for bank fraud and identity theft.

4.1 What is a Privacy Breach?

A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information that is in the custody or under the control of a public body. Such activity is "unauthorized" if it occurs contrary to the provisions of FIPPA.

Our office has several publications on our website to assist public bodies in dealing with a privacy breach. These include "Key Steps in Responding to Privacy Breaches", "Privacy Breach Management Policy Template", "Breach Notification Assessment Tool" and "Privacy Breach Checklist". The University was aware of these publications and used them to assist in the management of the privacy breach. In looking at the response of the University to the privacy breach, I will also rely on these guidance documents. In particular, I will examine how the response of the University met the four key steps in responding to a privacy breach.

4.2 Breach Containment

The University took immediate steps to contain the breach following the discovery of the loss of employee personal information. On the afternoon of January 8, the employee who discovered the break-in alerted the Campus Security office, who in turn notified the Saanich Police. Senior administration staff were made aware of the theft and came into the office to identify what might be missing. They quickly realized that the loss of the safe from the Financial

Services area meant the loss of a significant amount of sensitive personal information. The building was physically re-secured. As the information at risk was already in the possession of the thieves, there was little that could be done to further contain the breach. Mitigation was the only available step.

In terms of **breach containment**:

> I find that the University took all steps available to contain the breach following the incident.

4.3 Risk Evaluation

The mobile storage device that was stolen contained substantial amounts of sensitive personal information dating back to early or mid-2010. Major data elements, such as names, social insurance numbers, banking information and other information associated with the staff payroll were on the device. The University quickly recognized the significant risk to its employees of identity theft and realized that the notification of all affected past and present employees was necessary.

In terms of **risk evaluation**:

> I find that the risk evaluation by the University was reasonable.

4.4 Notification

On Monday, January 9, 2012, the day following the discovery of the theft, the University created a response team, which met that day and each day for the rest of the week, then as necessary for the next two months. Its purpose was to identify the affected individuals, the extent of possible harm and the steps necessary to mitigate any harm. My office, as well as senior University officials, was notified of the breach in the morning of January 9, 2012.

During the day of January 9, 2012, the response team prepared a notification statement to all affected present and past employees and obtained as many email addresses as were available for those individuals. The notification provided some details of the incident, identified the information at risk and recommended a number of steps employees could take to protect their information against identity theft. The statement was provided to our office for review and was delivered by email to approximately 94% of affected individuals by 6:30 p.m. of that day.

Over the subsequent days, the University provided more information via email and an information section on its website to assist its present and past staff in dealing with the privacy breach. The assistance included making credit monitoring available to affected individuals. In addition, the University attempted to contact by mail any individuals whom they were not able to contact by email. On February 6, 2012, the University also confirmed that it would provide credit monitoring through the two main Canadian credit bureaus for all affected individuals for one year.

In terms of **notification:**

> I find that the University met its obligations under FIPPA in notifying the affected individuals in a timely fashion and in providing appropriate information regarding the nature of the breach, the risks associated with the breach and recommended mitigation strategies.

4.5 Prevention Strategies

Since the incident, the University has undertaken an internal review of the events that resulted in the privacy breach and the subsequent steps taken to mitigate the effects of the breach. The review also looked at short term strategies to deal with the risk of such an incident occurring again. In addition, the University has hired an external consultant to identify repositories of personal information that may be at risk throughout the University, to ensure that they are adequately protected and to examine the policies and procedures to identity a method to prevent any further breaches.

As these reviews are on-going and the scope of my investigation is limited to the events of January 8th and its aftermath, I will not comment on these approaches except to commend the University for recognizing the substantial negative impact that the event had on individuals and providing timely and clear notification to the affected parties. The University is undertaking significant efforts to prevent a re-occurrence.

In terms of **prevention strategies**:

> I find that the prevention strategies adopted by the University following the incident were reasonable.

While I recognize that the University has hired an external consultant to carry out a review of its personal information and data privacy safeguards, it is important that the University does not simply accept any forthcoming recommendations and then assume it has carried out its responsibilities to the individuals whose information it holds.

Privacy compliance is not a paper exercise. Organizations must remain vigilant on an on-going basis to ensure that there are appropriate controls, that the controls are being implemented, and that there is adequate employee awareness of the controls and associated procedures.

RECOMMENDATION 4:

I recommend that the University develop a policy that requires the Privacy Manager to conduct risk assessments of personal information data banks on an annual basis and report to the University President on the result of these assessments.

RECOMMENDATION 5:

I also recommend that the University provide a copy of the report of the external consultant to my office for review and comment prior to its finalization.

5.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

5.1 Summary of Findings

I have made the following findings in this investigation:

I find that the information contained on the stolen mobile storage device is "personal information" under FIPPA.

I find that the University has established a strong data governance program, including designating an individual as being responsible for its privacy program. It has developed critical policies and training in its overall approach to the protection of privacy as required under s. 30 of FIPPA.

I find that the University information security policies failed to distinguish between appropriate methods of storage for personal information and to use a sufficiently high standard when rating storage devices such as laptops and other mobile storage devices as required under s. 30 of FIPPA.

I find that the University stored more than the minimum personal information necessary on the mobile storage device and failed to have a process by which the device would be reviewed periodically to limit the amount of personal information to the minimum necessary as required under s. 30 of FIPPA.

I find that the University's physical safeguards were not reasonable within the meaning of s. 30 of FIPPA because the University failed to properly secure the safe or to alarm an area where significant amounts of personal information were stored.

I find that the University failed to provide proper technical safeguards for the protection of personal information in its control as required under s. 30 of FIPPA.

I find that the University took all steps available to contain the breach following the incident.

I find that the risk evaluation by the University was reasonable.

I find that the University met its obligations under FIPPA in notifying the affected individuals in a timely fashion and in providing appropriate information regarding the nature of the breach, the risks associated with the breach and recommended mitigation strategies.

I find that the prevention strategies adopted by the University following the incident were reasonable.

5.2 Summary of Recommendations

RECOMMENDATION 1

I recommend that the University formally review the privacy and security policies at a minimum of every three years.

RECOMMENDATION 2

I recommend that the University re-assess the physical security of the Financial Services area to determine whether or not it is necessary to alarm the entire building and to assess other buildings on the campus where personal information is stored.

RECOMMENDATION 3

I recommend that the University develop a comprehensive policy, procedure, training and technical solution to ensure that personal information stored on laptops and other mobile devices is protected as required by s. 30 of FIPPA. The policy and training program should address data limitation, standard of encryption, appropriate password maintenance, physical security, wireless security and proper disposal.

RECOMMENDATION 4

I recommend that the University develop a policy that requires the Privacy Manager to conduct risk assessments of personal information data banks on an annual basis and report to the University President on the result of these assessments.

RECOMMENDATION 5

I also recommend that the University provide a copy of the report of the external consultant to my office for review and comment prior to its finalization.

6.0 CONCLUSIONS

The events that occurred at the University were extremely unfortunate and avoidable. The University was aware of the importance of protecting the privacy of its employees and students. In the past few years, it had taken some major steps to improve privacy awareness through policy and training. It had invested in a privacy program by establishing a Privacy Manager position. It had put in place a number of policies and training programs to raise the profile of privacy protection.

Despite all these good efforts, the University failed to prevent an unauthorized disclosure of personal information, because it failed to ensure that encryption was a standard practice for the storage of personal information on mobile storage devices.

While there is no doubt that human error or malicious activity cannot be totally prevented, proactive decisions, such as a requirement for encryption of all mobile storage devices, would have ensured a much more benign outcome. In this event, the highly sensitive nature of the data elements and their attractiveness to use for criminal activity should have alerted the University that an extremely high level of security should have been used. Moreover, the minimal cost of encryption for mobile storage devices should have been another factor in deciding to use encryption, as well as providing physical security by storing the device in a safe that could not be removed. Properly deployed encryption of mobile storage devices is no longer simply desirable; it is the required standard.

In the end, a relatively simple but preventable error has resulted in a significant privacy breach and enormous costs in time and money for the University and past and present employees. The critical message arising from this incident is that, when dealing with highly sensitive personal information, public bodies and organizations must ensure that they have carefully assessed the privacy and security risks associated with the information and employ all reasonable methods to protect it.

7.0 ACKNOWLEDGEMENTS

The University of Victoria cooperated fully with our investigation.

Jim Burrows, Senior Investigator, conducted this investigation, was the primary author of this report and was assisted by other team members.

March 29, 2012

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

OIPC File No.: F11-47178