University of Victoria

SUBMISSION TO THE UVIC BOARD OF GOVERNORS

FOR INFORMATION

To: OPERATIONS AND FACILITIES COMMITTEE

From: UNIVERSITY SECRETARY

VICE-PRESIDENT FINANCE AND OPERATIONS

cc: President and Vice-Chancellor

Meeting Date: January 31, 2012

Subject: **Preliminary Report on January 2012 Theft of Personal Information:**

I. Overview of Incident
II. Privacy Breach Response
III. Operational Response

Basis for Jurisdiction: University Act, s. 27

I. Overview of the Incident:

During a break-in at the Administrative Services Building over the weekend of January 7and 8, a safe, electronic devices and personal information were stolen. The purpose of this report is to provide the Committee with an overview of the incident, the implementation of the Procedures for Responding to a Privacy Incident or Privacy Breach, the university's operational response, and the next steps.

Late in the evening of Saturday January 7, 2012, unknown person(s) entered the B wing (both floors) of the Administrative Services Building.

Among the items stolen was a mobile storage device containing personal information of 11,845 individuals who had received pay through the university's Payroll department since January 2010, i.e. employee names, employee numbers, Social Insurance Numbers, bank account information for direct deposit (name of bank, account number and transit number), employee classification code and amount of last deposit. The personal information was stored on the mobile storage device for business continuity purposes.

The device was in a locked box, which was in a drop-box safe (drill proof), anchored through the carpet to the concrete floor, in an out-of-view cupboard, in a locked room (key pad entry), in a locked building. The B-wing area was not alarmed. The device was not encrypted.

The incident was noticed on Sunday, January 8, 2012 by an employee of Research Services and reported at 4:49 p.m. to Campus Security who contacted the Saanich Police. The Executive Director of Financial Services was informed and he, in turn, notified the Manager, Privacy, Access and Policy, who reports to the University Secretary, at 7 p.m. on the 8th.

II. Privacy Breach Response

Under the *Freedom of Information and Protection of Privacy Act* (FIPPA), the university, as a public body, is responsible for the safeguarding of personal information in its custody or under its control. The university has a Protection of Privacy Policy (GV0235), approved by the Board in June 2008, and associated procedures, effective January 2010. Under the authority of s. 77 of FIPPA, the Board, through the Protection of Privacy Policy, designated the University Secretary as head of the public body for the purposes of FIPPA. As such, she is responsible for the overall co-ordination of privacy functions.

Actions undertaken in respect to the privacy breach were undertaken pursuant to the Procedures for Responding to a Privacy Incident or Privacy Breach.

Given the nature and sensitivity of the information stolen, the number of individuals affected and the risk of identity theft, the immediate steps were to ensure the containment of the breach and the notification of individuals.

At 9:30 a.m. on Monday, January 9, 2012, the Response Team, as set out under the Procedures, was convened, including: the University Secretary; Vice President responsible for and representatives of the impacted area; Manager Privacy, Access and Policy; University Legal Counsel; Information Security Manager; representative of the Director, Communications; Associate Vice-President Human Resources; Associate Vice-President Faculty Relations and Academic Administration; Assistant Director, Campus Security (on behalf of the Director who was off campus); and the Executive Director, Government Relations. The team was joined at later meetings by the Vice-President External Relations, the Assistant Treasurer and the Risk Analyst. The response team met 6 times that week.

The response team reviewed the level of risk and recommended that individuals be notified and informed of the theft of personal information and of the immediate steps they should take.

As detailed below, banks and credit bureaus were contacted to better understand the vulnerability and how to mitigate risks for individuals. Throughout the day Monday, communications to assist affected individuals were drafted including Frequently Asked Questions (FAQs).

The Office of the Information and Privacy Commissioner (OIPC) was notified of the theft verbally at 11:45 a.m., Monday, January 9, 2012, and an investigator from the OIPC was assigned. Later in the afternoon, the OIPC reviewed the draft notification letter and FAQs.

In addition, the Deputy Minister of Advanced Education, the campus unions and Faculty Association, connected entities whose employees are on the UVic payroll system and members of the President's Advisory Council were notified of the theft of personal information by 3:30 p.m.

The university sent an email letter to 11,166 affected individuals at 3:38 p.m. As a result of a configuration change made recently by University Systems to address increased phishing attacks, not all the emails were delivered promptly. The technical issues were resolved and the final messages were delivered by 6:26 p.m. University Systems is monitoring bulk mail delivery to ensure there are no further blockages. There were 648 individuals who could not be contacted through email, so paper copies of the letter and media notification were prepared and sent. (Note: The sum of the number of individuals who received email letters and the number of people who received paper copy letters does not equal the number of individuals affected because in some cases two or more individuals share one email address.)

The letter provided details of the theft (as permitted to be released by the Saanich Police), the key personal information data elements that were stolen and the immediate steps that should be taken by affected individuals (contact their bank and the two credit bureaus).

The university continued to communicate to individuals through direct email, regularly updated FAQs, and a dedicated phone number and email address, and also informed the media.

Information on the immediate operational response including mitigation steps is included below.

In addition to the immediate breach and operational responses, the President commissioned a comprehensive external review by a recognized independent expert. This was announced on Tuesday, January 10, via the website and the President communicated this personally to the university community and the media on Wednesday. Draft terms of reference for the external review were shared with the OIPC on Thursday, January 12, 2012.

The external reviewer, Dr. David Flaherty, is a specialist and consultant in the management of privacy and information policy issues. He served as Information and Privacy Commissioner of British Columbia from 1993 to 1999 and has written or edited several books and articles on privacy. Dr. Flaherty will bring the most up-to-date knowledge and expertise to bear on the issues and will provide a report to the President and the Board of Governors with recommendations on the physical security and information security of sensitive personal information in the custody or control of the University of Victoria. His work as external reviewer will include:

- conducting needed interviews and site visits and collecting information as necessary;
- reviewing findings and recommendations arising from the operational response (including communication) that took place and from the internal assessment that is being carried out, as well as actions taken by the university in response to those.

The external review will address whether the university has identified the lessons to be learned from the January 2012 breach and developed appropriate plans or implemented appropriate measures to protect sensitive personal information across the university. Questions to be addressed will include:

- Is the university making all reasonable efforts to identify, review and protect sensitive personal information resources in the custody or under the control of the university?

- Are there storage systems containing sensitive personal information at the University of Victoria that are not adequately protected?

- Are the university's privacy, records management, physical security and information security policies, procedures and practices adequate to meet needs, standards and statutory requirements in 2012?

The external review is expected to be completed within four months. The report will be public, although some associated material may of necessity remain confidential for reasons of security, personal privacy or other grounds permitted under the *Freedom of Information and Protection of Privacy Act.*

At Dr. Flaherty's recommendation, the university is carrying out an internal assessment as part of the process. The terms of reference for the assessment have been approved by the external reviewer. The internal assessment will be led by Professor Jamie Cassels of the Faculty of Law, under the guidance of Dr. Flaherty. Professor Cassels will seek and receive input from members of the university community and will be able to call upon individuals within the institution with intimate knowledge of existing policies, procedures, and practices related to this matter. The terms of reference of the external review and the associated internal assessment are attached.

The OIPC has also announced that it will be conducting an independent investigation. Following the verbal report and consultation on our notification letter, FAQs and subsequent communications, we provided a written report to the office using its Privacy Breach Checklist on January 12, 2012. On Friday, January 13, 2012, the investigator met with the University Secretary and the Manager, Privacy, Access and Policy and did a site visit in the course of which he met with the Executive Director, Financial Services; the Payroll Manager; the Assistant Director, Campus Security and the Manager, Information Security. The investigator has indicated that the result of the OIPC's investigation will be a public report or case summary on its website.

We will be sharing pertinent information from the external review and the associated internal assessment with the OIPC investigator and will endeavour to coordinate the university's exercise with the ongoing OIPC investigation.

III. Operational Response

The purpose of this section of the report is to provide an overview of the support that has been provided to the affected individuals, the financial and other implications for the University of Victoria and the operational response that is currently underway, including actions that have already been taken.

Support for Individuals Affected

As noted in the Overview of the Incident, there were 11,845 individuals who had received employment income from UVic during the period since January 2010 and whose information was stolen. An immediate priority was to establish supports to assist individuals in order to reduce their risk of bank fraud and identity theft. Activities undertaken were:

- *Providing Information*: A dedicated telephone phone number and a direct email address to answer questions and provide information were in place by Monday, 3:00 pm. On Monday, the telephone was answered until 7:30 pm. The telephone was answered on Tuesday and Wednesday from 7:30 a.m. to 7:00 p.m., on Thursday and Friday from 7:30 a.m. to 6:00 p.m. and on Saturday from 10:00 a.m. to 3:00 p.m. As of Monday, January 16, there had been over 550 phone calls and 650 emails. Since that time, phone calls and emails have continued but at a lesser volume. The priority throughout was to answer questions as quickly as possible. If at all possible, questions were answered on the day they were received. Information was also provided through broadcast emails and the UVic Website on a dedicated website at http://www.uvic.ca/resources/infobreach . "Frequently Asked Questions" have been prepared, updated regularly and published on the website.

- *Facilitating steps to protect banking information*: One of our recommendations to all affected individuals was to contact their financial institution and follow the recommendations of the financial institution. In summary, recommendations from financial institutions were to close the affected bank account, place an alert on bank accounts and/or take other steps. Many individuals who are current employees have chosen to close their bank account and notified us of the change. Note that this does not include individuals who are not currently employees and accordingly may have closed their bank account but not notified us of the change.

  In order to assist both the affected individuals, as well as the banks and credit unions, we contacted all major banks and credit unions in the Victoria area early in the morning on Tuesday, January 10, to alert them to the theft and to the fact that as a result of the theft there would be a high volume of questions and client support requirements. Our understanding from many individuals is that the banks and credit unions were extremely helpful and proactive. Steps taken included adding additional staff, waiving change fees, providing refreshments while individuals waited and, in some cases, proactively identifying their clients who might be impacted and contacting their clients with offers of support.

- *Support for reducing credit fraud risk—credit alert*: In our early communications we recommended that all individuals affected contact the credit bureaus Equifax and TransUnion, to place an alert on their file. This alert indicates to creditors (credit card companies, etc.) that there could be potential fraudulent activity related to the account. As a result of the alert being put in place, creditors should ask additional identity verification questions although each creditor makes their own determination of the steps to be followed. This alert is provided at no charge and is retained on the file for 6 years.

  Because additional personal information is required in order to put an alert on the file, it is not possible for UVic to contact credit bureaus on behalf of the employees. Accordingly, we are also unable to determine to what extent individuals did contact the credit agencies. While this is the case, we do know that there was significant phone volume between UVic and the credit bureaus.

- *Enhanced support for reducing credit fraud risk—credit monitoring*: A credit monitoring service provides a notification by either email or text message that there has been a change in an individual's credit file including such things as the opening of a new account, changes to existing accounts or credit inquiries or credit applications. There is usually also a credit report that is provided periodically. An individual requesting this service would be required to pay $14.95 per month.

With the advice of our external advisors, Deloitte & Touche LLP (see below), we determined that credit monitoring should be provided for a period of one year at no cost to the individuals affected. As with the credit alert, it is not possible for UVic to do this on behalf of individual employees as additional personal information is required to initiate monitoring. Finalizing the details has been very complex and has resulted in a delay in making monitoring available. An update on the status of credit monitoring will be provided at the meeting.

- *Ensuring all employees are paid*: There was a regularly scheduled payroll on Friday, January 13. Steps were taken to ensure that all banking information changed prior to payroll was implemented accurately and in sufficient time to facilitate direct deposit of the pay. We also know that banks increased their monitoring and took exceptional steps to prevent a "bounce-back" of funds. As of Friday, January 20, there were 82 "bounce-backs" from the bank accounts that were changed. A total of 171 manual cheques were issued, including the 82 "bounce-backs." The next payroll date – for time-sheet employees – was January 23, and further steps were taken to ensure that all employees received their pay.

- *Time required to Deal with Banking Arrangements*: Employees were given the opportunity to meet with their bank during work hours if necessary.

- *Reimbursement of Direct Expenditures:* We will reimburse individuals for costs directly related to changing their bank accounts and for one month of credit monitoring charges if individuals signed up in advance of the notification that UVic is making the service available. We have also had the occasional request for other items that are out-of-pocket costs and are directly related to mitigating the risk from the theft of personal information. These requests are being considered on a case by case basis.

- *Provision of other information and support*. We have been in contact with organizations such as Service Canada, SIN Management Services, to obtain additional information. We have also engaged Deloitte & Touche to assist with answering questions and determining the appropriate steps that should be taken to reduce the risk to the individuals affected of bank, credit and identify theft.

By Monday January 16, the extent of questions and activities related to the loss of personal information had significantly subsided. Throughout the process all of the staff involved, particularly those in Payroll Services, Treasury Services and the Office of the VPFO, were extremely committed, professional and supportive. Their friendly, personal service was extremely helpful during this difficult time.

Potential Financial Implications of the Loss of Personal Information

As noted above, the University has agreed to compensate individuals for any direct costs incurred in changing their bank account. By January 20, we had received a small number of requests for reimbursement. For the most part, the requests are relatively small and the limited extent of requests is due in part to the support of the banks where changes were made without any fees. Other costs may include the cost of credit monitoring and the cost for Deloitte & Touche. A full reporting of costs paid by UVic will be provided in the future, once costs are accumulated.

UVic has broad insurance coverage through Canadian Universities Reciprocal Insurance Exchange ("CURIE"). At this time we have been in discussions with CURIE regarding losses but we do not know to what extent we will receive insurance compensation.

In addition to the above costs, there is a significant amount of staff time, as well as the costs of the external review and the internal assessment.

Components of the Operational Response

The objectives of the Operational Response are to identify and implement, as appropriate, steps to mitigate significant risks and to provide information that will be available to and inform the External Review and the Internal Assessment. Components of the Operational Response, which is led by Vice-President Finance and Operations Gayle Gorrill, with input and assistance from other portfolios, are as follows:

1. obtain a factual description of the incident and the security in place at the time;
2. assess and mitigate immediate risks arising from the incident (e.g., identity theft) and risks associated with the incident (e.g. building and information security);
3. quickly identify other significant confidential or highly confidential personal information resources on campus and mitigate any significant risks;
4. recommend to the internal assessor a process and time-frame for identifying all confidential or highly confidential personal information resources in the custody or control of the university, assessing associated risks, and reviewing the appropriateness of the collection and use of the data and the adequacy of the storage and disposition;
5. share findings and outcomes and any systemic questions or issues identified with the internal assessor.

Questions that are being addressed in connection with items 1 and 2 above include:

- What is the current physical security of ASB? What opportunities are there for improving the physical security of the building?
- How often did Campus Security patrol the building? Should the patrols of the building be increased?
- How should the data that was stolen, but is required for business continuity purposes, be stored?

Steps that have been taken to date or are in progress include:

1. Assessment and installation of alarms for all of the ASB.
2. Increased building patrols of ASB by Campus Security.
3. Change in storage of Business Continuity data for payroll .
4. Change in standards for newly acquired computers to include encryption.
5. Support and recommendations on selection and use of encryption.

Attachment: Terms of Reference for an External Review of January 2012 Theft of Employee Personal Information at the University of Victoria

University
of Victoria

January 20, 2012

Terms of Reference for an External Review of January 2012 Theft of Employee Personal Information at the University of Victoria

The University of Victoria is intent on avoiding any repetition of the recent theft of employee personal information that alarmed the university community and the general public.

To this end, it is commissioning a comprehensive external review by a recognized international expert. The review will be conducted by Dr. David Flaherty, a specialist and consultant in privacy and information policy issues who served as Information and Privacy Commissioner of British Columbia from 1993 to 1999. Dr. Flaherty will bring the most up-to-date knowledge and expertise to bear on the issues and will provide a report to the President and the Board of Governors with recommendations on the physical security and information security of sensitive personal information in the custody or control of the University of Victoria. His work will include:

- conducting needed interviews and site visits and collecting information as necessary;
- reviewing findings and recommendations arising from the operational response (including communication) that took place and from the internal assessment that is being carried out, as well as actions taken by the university in response to those.

The external review will address whether the university has identified the lessons to be learned from the January 2012 breach and developed appropriate plans, or implemented appropriate measures, to protect sensitive personal information across the university. Questions to be addressed will include:

- Is the university making all reasonable efforts to identify, review and protect sensitive personal information resources in the custody or control of the university?
- Are there storage systems containing sensitive personal information at the University of Victoria that are not adequately protected?
- Are the university's privacy, records management, physical security and information security policies, procedures and practices adequate to meet needs, standards, and statutory requirements in 2012?

The external review is expected to be completed within four months. The report will be public, although some associated material may of necessity remain confidential for reasons of security, personal privacy or other grounds permitted under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

At Dr. Flaherty's recommendation, the university is carrying out an internal assessment as part of the process. The terms of reference for the assessment have been approved by the external reviewer. The internal assessment will be led by Professor Jamie Cassels of the Faculty of Law. Professor Cassels will seek and receive input from members of the university community and will be able to call upon individuals within the institution with intimate knowledge of existing policies, procedures, and practices related to this matter. Operating under the guidance of the external reviewer, the internal assessment will:

1. identify and assess the steps leading up to the incident, commencing with the decision to create the stolen data storage device.

2. analyse the business processes related to the incident (e.g., data management, business continuity planning) and their oversight and identify what changes should be made in the future related to decision-making processes, accountability, and implementation;

3. review information security, physical security, privacy and records management policies, procedures and practices related to the incident:
   - were the relevant policies and procedures followed in this instance?
   - do the policies and procedures appear to be adequate?
   - what changes are recommended?

4. ascertain and review:
   - the steps taken since the incident to identify storage systems containing sensitive personal information at the university and to mitigate any significant risks;
   - the university's plans for: identifying other sensitive personal information resources on campus; assessing the levels of risk associated with them; and reviewing their collection, use, storage and disposition;

5. seek input and receive questions from the campus community regarding the treatment of sensitive personal information at the university and recommend how the university should address the issues raised;

6. determine whether the university has appropriate plans for reviewing information security, physical security, privacy and records management policies and procedures on an ongoing basis and assessing and achieving compliance;

7. identify any systemic questions or issues that might best be addressed by the external reviewer;

8. report findings and recommendations to the external reviewer and the university.

The findings from the internal assessment are expected to be ready within three months. The internal assessor's report and the administration's response to it will be public, although some associated material may of necessity remain confidential for reasons of security, personal privacy or other grounds permitted under FIPPA.

The University of Victoria is also cooperating fully with an independent investigation initiated by the Office of the Information Privacy Commissioner of British Columbia (OIPC). Information from the

external review and the internal assessment pertinent to the OIPC's investigation will be shared with that office as it becomes available.

Note: Sensitive personal information is personal information that is confidential or highly confidential under UVic's University Information Security Classification Procedures. The University is aware that FIPPA requires it to have reasonable security for all personal information in its custody or control.

University community members who wish to provide input into the review process may do so through Prof. Cassels, by e-mail at privacyreview@uvic.ca .