Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Shared Services Bureau of Management Board Secretariat, and the Ministry of Finance

Submitted by:

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

December 16, 2004

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
Website: www.ipc.on.ca

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Privacy Complaint Report

Privacy Complaint Nos. PC-040077-1 and PC-040078-1

Institutions: Management Board Secretariat (PC-040077-1)

Ministry of Finance (PC-040078-1)

Summary of Commissioner-Initiated Investigation:

On December 3, 2004, the Office of the Information and Privacy Commissioner (the IPC) was notified by the Ministry of Finance (the Ministry) about a breach of the *Freedom of Information and Protection of Privacy Act* (the *Act*). The Ministry advised that the privacy breach occurred with its November 30, 2004 mail-out of the Ontario Child Care Supplement cheques, which are mailed out on a monthly basis. The Ministry advised that each of the approximately 27,000 cheques mailed out contained the recipient's name, address, amount paid and social insurance number (SIN), along with four additional digits directly following the SIN. The counter-foil (the cheque stub) contained the name and SIN of the recipient as well as the name, address, and the SIN, along with four additional digits, of another recipient. The Ministry advised that the cheques were printed at the iSERV data centre in Downsview and mailed out for the Ministry by the Shared Services Bureau (the SSB) of Management Board Secretariat (MBS).

That same day, the IPC also received a second telephone call in relation to the incident, this time from MBS. MBS confirmed that the cheques were printed by iSERV, a program area for which MBS is responsible, and that MBS was investigating the circumstances leading to the privacy breach. MBS stated that it was now double-checking the cheques printed by iSERV for other programs, prior to mailing them out.

Both the Ministry and MBS expressed their concerns over the privacy breach and assured us of their intention to co-operate fully with our investigation, which they have done.

The IPC initiated privacy investigations under the *Act* with MBS (PC-040077-1) and the Ministry (PC-040078-1). Both investigations are addressed in this report since the privacy breach involved both the Ministry and MBS.

Background

The Ontario government has a number of programs that involve mailing cheques to individuals. The cheques for some programs, such as the Ontario Child Care Supplement for Working Families (OCCS) Program and the Ontario Disability Support Program, are printed at the iSERV data centre in Downsview. However, the cheques for other programs may be printed at a limited number of government buildings.

Regardless of the government program, the process for printing and mailing cheques follows a common chain of events that typically involve the Office of the Provincial Controller (OPC), SSB, and the iSERV data centre in Downsview.

For the OCCS program, the Ministry of Finance first prepares an electronic program file. This file contains data that will ultimately be printed out on each cheque, such as the name, address and identifying number (which includes the social insurance number) of an OCCS recipient. Each cheque includes a stub with similar data that would typically be detached and retained by the recipient before he or she deposited or cashed the cheque at a bank or other financial institution.

The Ministry electronically transmits the OCCS program file to a "holding" server at iSERV. It then notifies the OPC that the file is on the server and requests that the OPC authorize the payments. The OPC approves the issuance of payments by sending "payment reports" to the SSB. The OPC also creates a payment file for the OCCS program, which it transmits to the same "holding" server at iSERV as the program file.

After receiving the payment reports from the OPC, the SSB transfers the payment file from the "holding" server at iSERV to a mainframe computer, which is also housed at the Downsview data centre. SSB subsequently runs a software program on the mainframe computer that creates a "print" file for the OCCS cheque data. It then instructs iSERV to use this file to print the OCCS cheques.

iSERV prints the unsigned OCCS cheques, which are placed in boxes and then put into a secure cage (a wire cage with a padlock) and transported to the SSB payment-processing office in downtown Toronto. The cheques are then loaded into a machine that adds a signature to each cheque and splits the cheques from each other. Finally, the cheques are brought to the SSB's mail branch, where they are put into envelopes, stacked and picked up by Canada Post for delivery.

It should be noted that after the cheques have been printed and delivered to SSB, they are visually inspected for limited purposes before being mailed. For example, a staff person ensures that the cheques are properly aligned and removes and voids the cheques that were used for alignment purposes. Second, a staff person also records the first and last numbers of the issued cheques. Third, the enveloped cheques are put in mailing trays and visually inspected to ensure that the name and address are visible through the envelope window.

Results of the Investigation:

My investigation focused on the following: 1) the inadvertent disclosure of the personal information involved, 2) notification of the individuals whose personal information was disclosed, 3) retrieval or destruction of the personal information disclosed, and 4) the controls involved in the cheque-processing system.

The investigation included numerous meetings with the Ministry and MBS, as well as a site visit to the iSERV facility in Downsview by my staff. My office was provided with a copy of one of the November 30, 2004 cheques at issue, including the cheque stub. As a result, I obtained the following information.

The Disclosure:

The disclosure occurred with the mailing of 27,258 OCCS cheques dated November 30, 2004. The Ministry advised that there are approximately 113,000 individuals who received an OCCS payment on November 30, 2004, 86,112 of whom received it through a direct deposit of funds into their bank accounts, while 27,258 recipients received payment by way of a cheque. The Ministry advised that cheques for these 27,258 recipients are printed on the iSERV printer and mailed out by the SSB. For recipients who received their supplement by direct deposit, no cheque stub is issued.

The Ministry advised that this incident was triggered as a consequence of a November 17, 2004 software system enhancement to the Integrated Financial Information System (IFIS) payment-processing application, used by the Ministry and MBS, for payment processing.

The Ministry advised that as part of the upgrade enhancement, it conducted a series of tests, the first of which occurred between October 16 and 19, 2004. This test was conducted on the printers at the government's alternative printing facility at a government building in downtown Toronto, as well as on the actual production printers at the iSERV data centre in Downsview. According to the Ministry, the information used for the test run was coded data and not the true personal information of the individuals involved. Apparently, the cheques and cheque stubs produced during this test run not only showed an alignment and spacing problem but also showed that the personal information of another individual, albeit in coded form, was contained on the cheque stub. Unfortunately, only the alignment and spacing problem was identified, not the incorrect content problem, and subsequent e-mail communications were sent between staff at the Ministry and SSB to address the alignment and spacing problem. The disclosure of another individual's personal information and its appearance on the cheque stub was simply not identified. While this could have arisen due to the coded nature of the information, the review of the cheques had been limited to production "spacing-type" problems, as opposed to actual content. Had there been someone present from the program area during the testing process, this problem could have been identified and potentially avoided.

As a result of the alignment and spacing problem having been identified earlier, a test was conducted between November 9 and 17, 2004. The test, however, was conducted on the printers at the government's alternative printing facility at a government building in downtown Toronto, as opposed to the iSERV printers actually used in the production of the cheques. Even though the OCCS cheques and cheque stubs are routinely printed at the iSERV data centre in Downsview, the output for the new software testing was, for some reason, directed to the printers at the government's alternative site. The reason for this is still not clear to us and remains unknown, despite our continued inquiries. SSB officials acknowledged that it is not standard practice to conduct a test run on a different set of printers than the iSERV production printers – the ones that are ordinarily used to print OCCS cheques. Therefore, to the best of our knowledge, no explanation has yet been provided in response to the question, "Why did this take place?"

In addition, unfortunately, unlike the first test, the Ministry has not yet been able to locate a copy of the cheques and cheque stubs that were produced in the test run some time between November 9 and 17, 2004, in order to determine whether the disclosure of personal information continued to be problematic.

However, in addition and unrelated to the above, the Ministry advised that on November 25, 2004, there was a meeting held between Ministry and MBS staff to look at alternative methods for the production of OCCS cheques. At this point, the actual November 30, 2004 production run cheques had been printed and were in the process of being signed and prepared for mailing. At this meeting, a photocopy of one of these cheques was produced for discussion purposes. A Ministry program staff person who was present identified the problem of incorrect personal information appearing on the cheque stub – the problem was raised to those in attendance. Unfortunately, he was assured by someone else at the meeting that those cheques and cheque stubs were VOID and would not be sent out. Had they actually taken a closer look at the cheques, they would have realized that the cheques had not been voided – nowhere were the cheques marked "VOID," as would have been the case had they been voided. This was the second missed opportunity for catching the mistake and taking remedial action.

The November 30, 2004 cheques were subsequently mailed out. The cheques contained the correct name, address and SIN, along with four additional digits, of the recipient; the cheque stub contained the correct name and SIN of the recipient but also contained the name, address and SIN, along with four additional digits, of the person next on the list of recipients. As a result of new information later learned on December 10, 2004, several additional disclosures were identified, as outlined in the "Additional Disclosure and Notification" section below.

On December 1, 2004, the Ministry received 33 calls from recipients stating that their cheque stubs were incorrect in that they contained the information of another individual.

It is the Ministry's view that the source of the error was human error in the implementation of a computer software upgrade, which caused a spacing problem in the cheque stub, resulting in information of the next recipient being added to the stub, in the majority of cases.

It is important to note that the above information was provided to my office from the Ministry's audit team. However, that audit has yet to be completed. It is possible that additional facts uncovered by the final audit may vary from the facts noted above.

Steps Taken by the Ministry and MBS upon Learning of the Disclosure:

The Ministry immediately notified the IPC, as did MBS. MBS issued a news release advising the general public.

As a precaution, the Ministry contacted Social Development Canada and obtained information on how recipients can protect themselves against the possibility of improper use of their SINs. Social Development Canada alerted its call centres and SIN co-ordinators about the issue. In this regard, the Ministry also contacted the credit bureaus, Equifax and TransUnion, for additional information that could be provided to recipients who suspected misuse of their personal information. As a result, an information notice for OCCS cheque recipients, based on this information and containing contact information for Equifax and TransUnion, was posted to the Ministry website and was also used by Ministry staff to assist callers.

A series of questions and answers were provided to the Ministry's information centres and program staff to assist with calls from OCCS recipients.

MBS issued a "Backgrounder" on its Internet website, providing an update to the public on the OCCS disclosure of personal information and measures taken by the government.

The Ministry and MBS advised that a static list of recipients referencing which recipient had received another recipient's personal information has been generated and will be maintained by the Ministry.

Over the first weekend, the Ministry consulted with the IPC on the drafting of its letter notifying the 27,258 recipients affected by the disclosure and incorporated the IPC's advice. Work on preparing this notification began on the day the breach was discovered – a Friday. Ministry staff worked over the weekend, in consultation with the IPC, to ensure that the letters were the first in the postal system on the morning of Monday, December 6, 2004. In its notification letters, the Ministry advised recipients of the error that had resulted in the name, address and SIN, with four additional digits, of the person next on the recipient list, appearing on the cheque stub. The Ministry apologized for the error and asked the recipients to securely destroy any personal information on the cheque stub that did not belong to them

(suggesting shredding as an example). The Ministry recommended that they monitor all bank accounts, credit card and other financial transactions for any suspicious activity and provided a toll-free telephone number for recipients to use if they needed to contact the Ministry. The Ministry assured recipients that the source of the error had been identified, the problem resolved and that steps were being taken to protect the personal information in the future. On December 6, 2004, the Ministry confirmed to the IPC that its notification process was complete and notification letters had been mailed to the 27,258 recipients.

As previously mentioned, MBS halted the mailing of cheques over the weekend for recipients under other programs while it checked the accuracy of that information. MBS stated that the printing problem was corrected on December 5, 2004, and eight test cycles had been performed, completed and signed off. Subsequently, MBS confirmed to the IPC that all other programs had been tested for accuracy; the mailing continued on Monday December 6, 2004.

Remedial Steps taken by MBS:

On December 3, 2004, MBS conducted a test run of the iSERV production printer in Downsview to ensure that the printing error did not re-occur. The IPC was provided with documentation confirming this test run.

On December 8, 2004, my staff conducted a site visit to the iSERV facilities and observed all of the processes leading to the final printing of cheques. A test run was conducted and the cheques and cheque stubs that were printed showed no errors.

In addition, in order to achieve quality assurance in the future, iSERV has appointed a dedicated staff person to monitor the cheque run outputs and provide manual checks at regular intervals.

On December 10, 2004, I was provided with the terms of reference for the internal audit currently being conducted by the Corporate Audit Cluster of the Internal Audit Division. Objectives of the investigation included investigating how and why this disclosure occurred, including any system, operational or human factors that contributed to the disclosure, and completely reviewing the change management procedures pertaining to testing, implementation and initial review of production for the November 2004 software upgrade. The audit team anticipates issuing a draft report by December 24, 2004.

Additional Disclosure and Notification

On Friday, December 10, 2004, at 4.30 pm, I was contacted by the Ministry and a conference call ensued. The Ministry advised that its further investigations had led it to conclude that in fact, the disclosures of personal information were somewhat more complex than it had previously believed.

The Ministry stated that it had received telephone calls from recipients, the majority of whom confirmed the Ministry's earlier position that the disclosure was limited to one recipient who had received the personal information of the recipient next in line on the recipient mailing list. However, some of the callers offered different scenarios.

As a result, the Ministry conducted additional tests, which confirmed the following:

- 26,026 recipients' name, address and SIN, along with four additional digits, appeared on one other recipient cheque stub;
- 1,225 recipients' name and/or address only appeared on one other recipient cheque stub; and
- seven recipients' personal information, in various computations, appeared on more than one other recipients' cheque stub.

The Ministry provided the following breakdown of the personal information that was disclosed, relating to the seven recipients above:

- One recipient's name, address and SIN, with four additional digits, appeared on 220 other cheque stubs;
- One recipient's name, address and SIN, with four additional digits, appeared on 20 other cheque stubs, but 19 of those had first name only with the SIN and four additional digits;
- One recipient's name, address and SIN, with four additional digits, appeared on nine other cheque stubs, but one of those had first name only with the SIN and four additional digits; and
- Four recipients' respective name, address and SIN, with four additional digits, each appeared on two other cheque stubs, but one of those had the SIN with four additional digits with a different name.

The Ministry advised that it intended to notify these individuals by telephone that evening (December 10, 2004). The Ministry further advised that its Director of the Income Tax Related Programs Branch (the director) would telephone the seven recipients. The director

would identify himself, confirm whether the recipient had received the first letter of notification, apologize for the error and ask if the recipient had any questions. The director would then inform the recipients that upon further review of the computer file, the Ministry had discovered that his/her personal information, including the SIN, if applicable, had appeared on more than one other recipient's cheque stub.

With respect to six of the recipients, the director would assure them that there was a low risk or probability of the misuse of his/her personal information as the Ministry knew precisely who had received their personal information. The recipients should monitor and verify all bank accounts, credit card and financial-transaction statements for suspicious activity, such as unauthorized transactions. The recipients would be asked to contact the director directly if they had any additional concerns.

With respect to the sole recipient whose personal information appeared on 220 cheque stubs, in addition to providing the above information, the director would advise her that her personal information had appeared on 220 cheque stubs. In addition to providing the above information, the director would provide the recipient with the name and direct telephone number of the director of SINs at Social Development Canada, who would be able to advise her of the options available to her, including the possibility of obtaining a new SIN. The individual would also be provided with the contact number for Equifax.

A copy of the script used to notify the recipients was provided to my office.

On Monday, December 13, 2004, the Ministry confirmed that its director had established contact with five of the seven recipients for whom the Ministry had telephone numbers on file.

The Ministry advised that it was not able to notify two of the recipients. One of the recipients was the individual whose personal information appeared on two cheque stubs. The Ministry advised that it had sent a letter by courier, asking the recipient to contact the director immediately in regard to the recent privacy breach and as a follow-up to the original notification letter sent last week.

The other recipient was the individual whose personal information appeared on 220 cheque stubs. The Ministry explained that this recipient only had a post office box address on file and the telephone number provided was no longer in service. The Ministry sent a letter by priority courier to the recipient, asking her to immediately contact the director. The Ministry further advised that a personal contact for this recipient with the director of SINs, Social Development Canada, has been established, should she wish to obtain a new SIN. In addition, this recipient will also be advised to contact Equifax's Fraud Centre; staff at the centre have been alerted to this situation and upon the consent of the individual, Equifax will flag this recipient's credit file and enter her SIN into their "Safe Scan" system, which monitors unusual activity.

The following issues were identified as arising from the investigation:

1. Was the information disclosed in the cheque stub "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part: "personal information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

…

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

I have reviewed the record at issue, which consists of a cheque and cheque stub. The cheque contained the name, address, amount paid and SIN (with four additional digits) of the recipient. The cheque stub contained the name of the recipient identified as the "payer" on the cheque, together with that individual's SIN. The cheque stub also contained the name, address and SIN, with four additional digits, of another individual. I conclude that the record clearly contains information which qualifies as personal information under sections 2(1)(a), (b), (c), (d) and/or (h) of the *Act* set out above.

2. Was the disclosure of the "personal information" in compliance with section 42 of the *Act*?

Section 42 sets out a number of circumstances under which an institution may disclose personal information. None of these circumstances are present in this case, where personal information was inadvertently disclosed. Accordingly, I find that the disclosure of the personal information of other individuals who were not the payer contained in the cheque stub by the Ministry and MBS was not in compliance with the *Act*.

Conclusions:

I have reached the following conclusions based on the results of my investigations:

1. The information disclosed in the record is "personal information" as defined in section 2(1) of the *Act*.

2. The disclosure of another individual's personal information to the recipient of the cheque by the Ministry and MBS was not in compliance with section 42 of the *Act*.

3. I am satisfied that all persons affected by the disclosure, with the exception of the two individuals referenced above, have been notified by the Ministry. I am also satisfied that the Ministry is making every effort to contact these two individuals.

4. I am satisfied that the source of the technical problem is being addressed. I note that MBS has appointed a dedicated staff person to oversee the printing at iSERV for the sole purpose of providing a manual check for quality assurance purposes.

I commend the Ministry and MBS staff for their prompt response after learning of the improper disclosure of personal information, and for the steps that they have taken to address this matter. It is clear that both the Ministry and MBS appreciate the seriousness of the matter and have given considerable thought and priority to taking immediate and appropriate actions. I also commend the Ministry and MBS for offering the IPC their full co-operation throughout this investigation.

It must be said, however, that the absence of controls and the existence of control weaknesses contributed to and exacerbated the problem. In addition, the absence of a manual inspection being conducted of the cheques and cheque stubs produced, to ensure the accuracy of all of the information appearing on the cheques and cheque stubs, was an obvious weakness in the process.

Two procedures could have prevented this privacy breach from occurring: 1) maintaining the standard practice of using the same printer for the testing of a software upgrade on the production printer – the printer used in the actual production of the cheques and cheque stubs; and 2) conducting a manual inspection of the initial cheques produced to ensure the accuracy of the content of all of the information appearing on the cheques and cheque stubs.

Other Matters:

The Use of the SIN as a Unique Identifier

My investigation of this case concerns the disclosure of the personal information of over 27,000 individuals, which occurred directly as a result of human error in the implementation of a computer software upgrade, but also as noted above, indirectly from the absence of the appropriate controls and inspection procedures. The SSB, an integral program area of MBS, is responsible for providing business support services to the Ontario Public Service and necessarily deals with highly sensitive personal information. Personal information such as the SIN is a significant data-linkage tool and, with advances in computer technology, may be increasingly used for linking personal information in ways that can compromise personal privacy. In the current environment, inadvertent disclosure increases the potential for such compromise. One very real threat is that of identity theft.

In this day and age, the greatest threat to privacy from the accidental disclosure of personal information comes in the form of identity theft. Identity theft is one of the fastest growing forms of fraud in North America. The improper disclosure of personal information, whether by government institutions, businesses, or individuals themselves, provides the opportunity for perpetrating such a crime. Once an individual's identity has been compromised, the results can be truly catastrophic – leading to financial loss, ruined credit ratings and protracted efforts on the part of victims to re-establish their credit-worthiness, their good name, and securing their identity.

The potential of identity theft arising in the present case through the improper disclosure of SIN numbers was immediately recognized by the Ministry, and appropriate actions were taken. However, if the use of universal personal identifiers such as the SIN number can be limited by government institutions, then the potential for inadvertent disclosure may also be limited and, in turn, the threat of identity theft reduced.

The Ministry and MBS have stated that a unique identifier is necessary for means of identification and to ensure effective and efficient service to their clients. The Ministry and MBS state as follows:

> The name is not, on its own, sufficient as a means of identification as there can be many duplicated names on our database. We have even had instances of two clients with the same name and same addresses (apartment building). Therefore, in order to be able to clearly and quickly identify and serve the client, each OCCS client is assigned a unique identifier. The SIN serves as the unique client identifier for the OCCS program.

The Ministry and MBS go on to say that "[t]he SIN serves as the basis for matching federal data supplied by Canada Revenue Agency with our OCCS data."

I accept that the SIN must be used for the purpose of data matching in accordance with information sharing and other agreements with Canada Revenue Agency and other federal agencies. However, I do not accept that the SIN must be used as the unique identifier within provincial government departments.

I agree with the Ministry and MBS that there is a clear need for a unique identifier for the purpose of safely and quickly serving their clients. I do not agree, however, that it must be the SIN. A purpose-specific unique identifier may be created for file and client identification purposes, to be used on cheques and cheque stubs. This was done by MBS for the Workforce Information Network (WIN) where a unique identifier was created for each government employee to enable them to safely access their own personal information, without compromise or risk to the protection of other employees' personal information. I will address this further in my recommendations below.

The Need for An Independent, Comprehensive Audit

Over the past two years, my office has been involved in a number of privacy investigations, primarily involving the inadvertent disclosures of personal information by SSB in various situations. These include the following:

1. In October 2003, the SSB notified us of an inadvertent breach. The SSB is responsible for a web-based integrated human resource software application called WIN. Employees of the government can enter and access their own personal information. Modifications were made to the WIN system in October 2003. Several government employees notified SSB that they were inadvertently able to view the personal information of another employee. The system was temporarily taken offline and SSB notified the IPC of the privacy breach. SSB then notified the individuals affected by the breach and provided a general notice to WIN users on the WIN intranet site. Subsequently, considerable efforts were made on the part of MBS to strengthen the WIN system.

2. In December 2003, the IPC received a privacy complaint from a government employee regarding the provincial government's use of the Social Insurance Number (SIN) as an employee identification number with respect to the processing of employees' health insurance claims. Similar complaints have been received in the past. The complaint was resolved based on the government's commitment to eliminate the use of the SIN in non-payroll systems and that the WIN system, which provides each employee with a separate unique identification number, may offer an appropriate remedy.

3. In December 2003, the IPC received a complaint from a government employee who was concerned about the posting of employee electronic pay stub information on WIN, as well as general concerns relating to the security of WIN. When contacted about the complaint, MBS indicated that the record at issue is employment-related information (Bill 7) as described in section 65(6)(3) of the *Freedom of Information and Protection of Privacy Act* (the *Act*). As a result MBS took the position that the information fell outside the coverage of the *Act*. MBS chose to have further discussions with the complainant, without the intervention of my office.

4. In December 2003, the IPC was notified by MBS that a privacy breach occurred at the SSB. The problem occurred when a small calendar was inserted into the envelope including government employees' bi-weekly pay stubs. The result was that two employees received the wrong pay stub. MBS included a notice with a subsequent pay stub that advised employees of what had happened and what to do if they received someone else's pay stub, in error. The IPC was also informed that as of January 2004, the SIN number no longer appeared on employees' pay stubs.

5. In February 2004, the Ministry of Finance contacted the IPC to advise of a privacy breach relating to the mailing of the Ontario Child Care Supplement (OCCS) by SSB. A client contacted the Ministry to advise that she had received another client's OCCS cheque in the envelope that contained her own cheque. The Ministry worked together with SSB and MBS to have the OCCS mailing conducted on a new mail inserter. Notice was provided to clients advising what to do if privacy issues arose in future cheque mailings.

6. In February 2004, a former employee of the Province of Ontario Savings office contacted the IPC to advise that she had received another person's T4A statement that contained the name, SIN and personal data of that person, but had her home address. The statement was in an envelope from the Ministry of Finance. The Ministry determined that there were only two such occurrences. The statements were mailed to recipients by SSB's mail office on behalf of the Ministry.

7. In April 2004, MBS notified the IPC about a privacy breach that involved a collection agency retained by the SSB, the Ministry of Training, Colleges and Universities and the Ontario Student Loan Program. A debtor had requested information in support of her loan and received a report containing the personal and financial information of 38 other debtors.

8. In June 2004, MBS notified the IPC of a similar breach involving a collection agency retained by the SSB and the Ministry of Training, Colleges and Universities where an OSAP debtor received the personal and financial information of another debtor.

9. In October 2004, MBS notified the IPC that, during the mailing of the October 7, 2004 government employee pay stubs, an insert was included regarding the new $20.00 bill. Subsequent to the mailing, SSB was notified that four individuals had received another person's pay stub in their own envelope. The practice of inserting any additional materials into envelopes has now been discontinued.

10. Also in October 2004, MBS notified the IPC of two incidents where a problem involving human error relating to the resetting of employee passwords to access the WIN system, allowed two government employees to view the electronic pay stubs of two other employees.

This series of privacy breaches points to an ongoing problem of a systemic nature that, in my view, can no longer be addressed on a one-off basis, as isolated incidents.

I applaud the Ministry and MBS for proactively contacting my office whenever privacy breaches are experienced. I believe this approach shows their commitment to addressing privacy issues immediately and to doing the right thing. I acknowledge that the above incidents involved relatively small numbers of individuals and, to the best of our knowledge, have not resulted in any particular harm to the individuals involved. The Ministry and MBS moved quickly to identify and notify the individuals involved, retrieve or destroy personal information that had gone astray, and work with my office to find and implement viable solutions.

The SSB is the steward of a large volume of sensitive personal information, whether as part of its role in printing cheques for government programs such as OCCS, or as the division responsible for employee information contained in WIN. In many cases, this personal information is very sensitive, including the human resource information of government employees and the financial information of Ontario citizens. To give you some idea of the volume of the numbers involved, we have been advised of the following: 1) WIN is accessed approximately 30,000 times every month; 2) approximately 100,000 pay stubs, 30,000 OCCS cheques, and 3.8 million mail inserts are mechanically inserted into envelopes every month; and 3) the resetting of 13,000 passwords is performed every year, while 55,000 Ontario public servants have passwords administered annually.

I have had a growing concern with the number of incidents involving this personal information, as seen from the 10 incidents noted above. Until now, the timely action taken by the government to address these incidents, and the involvement of my office, have satisfied me that appropriate steps were being taken by SSB to protect the security and privacy of the personal information in its possession. However, the present report deals with a much larger incident affecting thousands of citizens. Fortunately, the potential for serious damage appears to be limited. However, this may not be the case should a future breach occur.

I am pleased that an internal audit of the processes relating to the November 30, 2004 incident has been undertaken. However, in my view, that is not enough. Given the previous history of privacy breaches involving SSB, I am not satisfied that an internal audit focusing narrowly on this particular program will ensure that additional breaches involving SSB do not occur in the future. Therefore, I am recommending that MBS undertake a comprehensive and independent end-to-end audit of SSB's functions, operations and privacy practices involving the handling of personal information. The goal of such an audit should be to strengthen the security and privacy of personal information in the custody of SSB and flowing to it, through the Ministry of Finance, and other Ministries and agencies, and reviewing systems and procedures to diminish the possibility of future breaches. Weaknesses must be identified, controls must be strengthened and best practices must be developed. It is also possible that such an audit will provide additional answers to questions that remain unanswered. We reserve the right to revisit this investigation in the event that new information surfaces. We will await the results.

Recommendations:

1. I recommend that MBS initiate a comprehensive and independent end-to-end audit of SSB's functions, operations and privacy practices involving the handling of personal information. Upon completion, the audit report should be made available to the public.

2. I recommend that the Ministry and MBS discontinue the practice of using the SIN number and create a purpose-specific unique identifier for each of their clients to replace the use of the SIN.

3. Pending the outcome of the independent audit referred to in Recommendation 1 above, I recommend, as an additional security and quality assurance measure, that MBS ensure that a trial run printing of several sample cheques on the production printer be conducted and the cheques be manually examined, by someone from the program area involved, before each monthly printing of cheques and stubs is commenced.

The Ministry of Finance and MBS should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations as follows:

1. Within **two months from the date of this** report, provide a copy of the terms of reference and the name of the company that has been retained to perform the audit referred to in Recommendation 1 above;

2. No later than **six months from the date a company has been retained**, provide a copy of the audit report, containing recommendations on improvements considered to be necessary and best practices proposed; and

3. Within **12 months from the date of this report,** provide this office with proof of creation of the purpose-specific unique identifier intended to replace the SIN.

December 16, 2004

Ann Cavoukian, Ph.D.
Commissioner