ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2010-008

January 5, 2011

STAPLES CANADA INC.

Case File Number P1105

Office URL: www.oipc.ab.ca

Summary: The Complainant complained to the Commissioner that the hard drive containing her family's personal information had gone missing from her family's laptop computer when she had given it to Staples Canada Inc. (the Organization) to repair. She asked the Commissioner to review whether the Organization's security measures, as they applied to the personal information of customers located on their computer hard drives, were in accordance with the *Personal Information Protection Act* (PIPA).

The Adjudicator found that it was more probable than not that the Complainant's hard drive, and the personal information it contained, had been removed and destroyed while it was in the custody of the Organization. She also found that the Organization had not made reasonable security measures to protect the personal information contained in the hard drive from unauthorized loss or destruction, as required by section 34 of PIPA. She ordered the Organization to make reasonable security arrangements to prevent against the unauthorized destruction of personal information on computer hard drives given to it by customers for repair.

Statutes Cited: AB: *Personal Information Protection Act* S.A. 2003, c. P-6.5 ss. 34, 36, 49, 52

I. BACKGROUND

[para 1] On September 19, 2008, the Complainant complained to the Commissioner that the hard drive had gone missing from her family's laptop computer when she had given it to Staples Canada Inc. (the Organization) to repair. She explained that the personal information of her family members was on the hard drive, including financial information and records. The Complainant requested that the Commissioner review whether the Organization's security measures, as they applied to the personal information of customers located on customers' hard drives, were in accordance with its duties under the *Personal Information Protection Act* (PIPA).

[para 2] The Commissioner authorized a portfolio officer to investigate and attempt to mediate the Complainant's complaint under section 49 of PIPA. As mediation was unsuccessful, the matter was scheduled for a written inquiry.

[para 3] A Notice of Inquiry was prepared by this office on March 2, 2010 and sent to the parties. This notice states the issues for inquiry as the following:

> Without limiting the Commissioner, the issues in this inquiry are:
>
> 1) Does the evidence in this case establish that the Organization removed the hard drive from the laptop computer and failed to return it to the Complainant?
>
> 2) If the answer to number 1 is yes, was this a function of the fact that the Organization failed to make reasonable security arrangements to protect personal information in its custody?

[para 4] After the parties had provided submissions for the inquiry, I reviewed the issues for inquiry and decided that the issues for inquiry were not properly stated. As the Complainant's complaint is made under section 36(2)(f) of PIPA, which states that a Complainant may make a complaint that an organization is not in compliance with PIPA, the requirement to answer question 2 should not appear to be conditional on a positive answer to question 1. Rather, the answer to question 1 would serve only to illustrate how the security arrangements operated in a specific circumstance. It is clearly possible to envision circumstances where inadequate security arrangements are made to protect personal information, but personal information is not lost. It is equally possible to envision circumstances in which reasonable security measures are made to protect against risk, but personal information is lost despite them.

[para 5] Moreover, I was concerned that the questions originally posed had the effect of suggesting that the Complainant bore the burden of proof in relation to question 2, when the burden for establishing that a duty imposed by PIPA has been performed lies on the organization on whom the duty is imposed.

[para 6] Accordingly, I proposed that the issues for inquiry are be restated as the following:

1) Does the evidence establish that the Organization had custody or control of the Applicant's personal information, specifically, personal information contained on the Applicant's hard drive?

2) If so, did the Organization make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction of the Complainant's personal information when the Complainant's laptop and hard drive were in its custody?

3) If the answer to question 1 is no, did the Organization make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction of personal information contained on laptops in its custody or control?

[para 7] However, the Organization objected to the restatement of the issues. As the Organization made the objection, and as I have decided that it will make no difference to the outcome of the inquiry whether I answer the questions as originally proposed by this office, or as I later proposed, I will answer the original questions. While I note that it is not strictly necessary to address question 1 as originally stated, I intend to do so, as reviewing the circumstances in which the Complainant's hard drive went missing will illustrate how the Organization's security arrangements functioned in a particular set of circumstances. This, in turn, will assist me to determine whether the Organization's security arrangements are reasonable for the purposes of section 34 of PIPA.

II. ISSUES

Issue A: Does the evidence in this case establish that the Organization removed the hard drive from the laptop computer and failed to return it to the Complainant?

Issue B: If the answer to number 1 is yes, was this a function of the fact that the Organization failed to make reasonable security arrangements to protect personal information in its custody?

III. DISCUSSION OF ISSUES

Issue A: Does the evidence in this case establish that the Organization removed the hard drive from the laptop computer and failed to return it to the Complainant?

[para 8] In her initial complaint, the Complainant provided the following history of the dispute between herself and the Organization regarding the laptop hard drive:

> My computer was taken to Staples Business Depot (5662 Signal Hill Center SW, Calgary Alberta) on June 27, 2008 due to a faulty power switch (I had to press exceedingly hard on the power button to get the computer to power up). I had purchased extended warranty for this computer.

> At some point (days, weeks?) after I left my computer with Staples, the computer was then sent to their service center (Easy Tech Force) for repair. The service invoice ticket shows it was received by them on July 21, 2008.
>
> Staples Warranty Center or Easy Tech Force (not sure which one?) contacted me on July 24 (approximately) and informed me that it was not cost effective to repair the computer; that they would offer me a "buy out" for the computer. They had calculated that, based on the date that I purchased it (it was 1.5 years old); they would offer me $450 (approx) in compensation. They deemed its value was not worth the repair. Unfortunately, these are the terms of the repair contract, so I reluctantly told them that I would like the computer back so that I could do a back up and remove (wipe) the hard drive that stores all my family & business data and information. I said that I was out of the province for the entire summer (until the Labor Day weekend) but my husband would pick it up when he returned to Calgary and I would deal with it when I returned to Calgary. They said "no problem", we'll process your credit buy out after you delete the hard drive and return the computer to Staples, in September.
>
> As planned, I sat down in the first week of September to get the hard drive wiped of all our information & data. When the computer did not power up, I assumed it was because of the power button (the original problem). I called Staples and explained the situation and was eventually… connected to a senior computer technician [name of Staples' technician]. He told me to come into the store (I was there in 45 minutes) and he would personally take me to their back service area so I could see him put the hard drive into a specific machine to wipe the hard drive. When he unscrewed the back of the computer to get access to the hard drive, it was discovered that the hard drive was missing. He and I were shocked to see that my hard drive was missing! He immediately called the Easy Tech Force and spoke directly with the individual who worked on my computer. This individual had no idea where the hard drive was either.

[para 9] The Organization agrees with this chronology of events. It provided notes made by employees at the time the Complainant's laptop was in its custody which confirm this chronology. I therefore accept that the Complainant dropped off the laptop, and was contacted on July 24, 2008 and told that the laptop would not be repaired, that it was returned so that she could back up the hard drive and erase it, that the laptop was not at Staples from the end of July until September 9, 2008, and that the laptop was found not to have a hard drive on September 9, 2008.

[para 10] The Organization provided the statement of a Manager, Technical Services, to explain the security measures in place regarding computers designated for repair. These measures have been in place since June 2008, when the Complainant's laptop was brought in for repair. The Manager, Technical Services states:

> The following are mandatory security procedures that have been in force in the Organization's retail stores and warranty depots since at least June 2008:
>
> (a) All computers designated for repair must be kept in locked storage accessible only by a manager when not being worked on by a technician.
>
> (b) Each technician must enter details of service activity onto the Service Invoice Ticket every time a computer is worked on.
>
> (c) All associates at each of the Organization's facilities are subject to bag checks by management

> Attached hereto as Schedule "A" is p. 13 of the Organization's "In-Store Repair Skill Builders" manual. The procedures in this manual are followed by retail store technicians and have been since at least June 2008. With respect to "Power Supply", there is no mention of removing the hard drive from a computer in order to resolve an issue.
>
> Attached hereto as Schedule "B" is p.8 from the Organization's Warranty Claim Toolkit. [The procedures] in this manual are followed by warranty depot technicians and have been since at least June 2008. With respect to "Power Supply there is no mention of removing the hard drive from a computer in order to resolve an issue.

[para 11] The Organization argues that there was no need to remove the hard drive from the Complainant's laptop in order to repair it or to make the decision to "buy out" the Complainant. The Organization provided the notes of the technician who examined the laptop. The notes state:

> Rec'd w/ adapter / cord / batt in used condition scratches / scuffs/ on top / sides. Touchpad worn. Tested unit draws power from ac adapter and charges, power button unresponsive, unit doesn't post. Unable to test sound. Recommend shipping to HP. Called cust 11:53 am left msg on machine advising. Sent auth for strep.
>
> ESTIMATE DENIED WE WILL BUYOUT THE CUSTOMER

[para 12] The Organization argues:

> In summary, for that portion of the period from June 25, 2008 to September 9, 2008 during which the subject computer was in Staples possession, there was no reason for Staples' technicians to access the hard drive or even to ascertain that the hard drive was present. Secondly, each Staples technician involved in the assessment of the computer specifically denies accessing or removing the hard drive. We have come to no firm conclusion, based on our investigation and the facts known to us, about the whereabouts of the Complainant's hard drive. We have no knowledge of who may have had access to the computer from the time it was picked up at our store in late July / early August to September 9, 2008.

[para 13] The Organization argues that it is possible that the hard drive may have been missing from the laptop when the Complainant originally brought it in for repair, or was removed from the laptop during the summer when it was at the Complainant's home.

[para 14] In response to my request that the Complainant provide evidence from her family members to support her statement that no one in her family had removed the hard drive from the laptop and lacked the requisite knowledge to do so, the Complainant provided statements from her family members. Each member of the family explained that they did not remove the hard drive from the laptop and have never removed the hard drive from a laptop before. The Complainant also explained that she did not remove the hard drive and does not know how to remove a hard drive in any event. She and her husband also stated that their home has an alarm system and that there has been no evidence of a break in at their home.

[para 15] Having reviewed the evidence of the parties, I am satisfied that the Complainant has established that it is unlikely that the hard drive was removed from the laptop while in the custody of her family. I believe the evidence of the Complainant and

her family members that none of them removed the hard drive from the laptop and lack the necessary knowledge to do so. I also accept the evidence of the Complainant that the hard drive of the laptop contained the personal information of her family members, including financial information.

[para 16] The Organization states in argument that "each Staples technician involved in the assessment of the computer specifically denies accessing or removing the hard drive." However, the Organization did not submit statements of this kind in its evidence and I therefore do not have the benefit of them for the inquiry.

[para 17] Counsel for Staples asked the technician who diagnosed the laptop the following questions:

> Was the case of the computer removed in the course of making the diagnosis and decision to ship to HP?
>
> If so, did the technician notice if the hard drive was there?
>
> Are there any written log entries or notes other than what appears on the Ticket?

The technician who diagnosed the laptop problems answered: "No reason to open to make that diagnosis".

[para 18] The technician's response does not answer counsel's questions directly. However, I accept that the technician may not remember the details of diagnosing the Complainant's laptop, but is able to state that his practice in diagnosing problems such as those presented by the Complainant's laptop never involves accessing the hard drive. I accept that this statement is true, and have no reason to doubt that the technician followed his usual practice in relation to the Complainant's laptop.

[para 19] As noted above, the Organization keeps computer hardware to be repaired in a locked area accessible only by managers. In addition, the technician has indicated that it was unnecessary to remove the hard drive in order to repair the computer. Therefore, it is unlikely that the hard drive was removed from the laptop while it was categorized by the Organization as "to be repaired." However, the Organization also decided that it would not repair the Complainant's laptop and instead told her it would buy her out. The question becomes whether the Organization's security arrangements and procedures are the same in relation to computers it categorizes as "buy outs" and computers it intends to repair.

[para 20] A note of a Staples employee states:

> Hello, as per ticket number D11D595255 for customer [name of Complainant] we received an email from ESP that the unit was to be bought out and as per usual updated the ticket and removed the unit from the shelf and put it into the buyouts.

This note indicates that once the Organization made the decision to buy out the Complainant's laptop on July 22, 2008, the laptop was put into the buyouts. The

Complainant was then contacted regarding the decision to buyout her laptop on July 24, 2008.

[para 21] A note made by a claims manager of the Organization on September 11, 2008 indicates that the depot was contacted in order to try to locate the Complainant's hard drive. This note states:

> I also called the depot and they advised me that even if they had somehow misplaced this hard drive (which they say they didn't) with the time lag of over a month they had no idea where it possibly might be.

[para 22] An email created by the Winnipeg Depot suggests that if the hard drive had been removed from the laptop, it would no longer be there. This email states:

> This 2nd section was only an assumption that if we'd ever taken the HDD out by now it would have been sent back to vendor… Unfortunately, the hard drive would either be in a large unmarked box full of drives or possibly ended up going to one of our vendors. If it went back to a vendor it would have been a company called Nexicore and I have an email sent to us from Nexicore regarding hard drives being shipped back to them.

[para 23] In my letter of October 19, 2010, I asked the Organization the following questions in relation to the preceding notes:

> A. Staples provided evidence regarding its security arrangements for computers designated for repair. However, an email note in its evidence dated October 08, 2008 at 8:14 AM indicates that once the Complainant's computer was no longer designated for repair, but buyout, it was removed from the shelf and put "into the buyouts". What security arrangements were in place for the buyouts?
>
> B. A note in Staples's evidence dated September 11, 2008 states, in part:
>
> *I called store 110 and spoke with [an employee] and the store technician and they both advised that when they opened up the customer's laptop there was no hard drive in the unit. I also called the depot and they advised me that even if they had somehow misplaced this hard drive (which they say they didn't) with the time lag of over a month they had no idea where it possibly might be.*
>
> Staples has told me in its submissions and evidence that laptops scheduled for repair were kept in locked storage, accessible only by a manager or technician. How, then, would the time lag affect employees' ability to locate a hard drive? In other words, why would a time lag of over a month affect their ability to state conclusively whether a hard drive was located in locked storage?

[para 24] The Organization provided the following response to these questions:

> The answer to question A is that "buyouts" are kept in the same secure area as computers in for repair.
>
> With respect to question B, the comment about the time lag relates to a purely hypothetical circumstance – that the depot had misplaced the hard drive. In that hypothetical circumstance the hard drive may have been destroyed during the time lag. Destruction of hard drives on bought out units is standard procedure.

[para 25] The Organization placed the Complainant's laptop with the "buyouts" two days before the Organization contacted her to notify her of its decision to buy her out, according to its evidence. Moreover, it states that it has a practice of destroying the hard drives of laptops that are bought out. The Organization has not explained what measures are in place in the "buyout" area to prevent the inadvertent removal and destruction of laptop hard drives once the laptop has been placed there. While the Organization states that the laptop was kept in a secure area, it has not established that it made arrangements to ensure that the laptop's hard drive was not subjected to its standard procedure of destruction while in that area. On the contrary, its evidence is that it never ascertained whether the laptop had a hard drive. In addition, it placed the laptop in the buyout area without any special instructions regarding the hard drive.

[para 26] As noted above, I accept the evidence of the Complainant and her family members that none of them removed the hard drive from the laptop and that while the laptop was in their custody it remained in their home, which has an alarm system.

[para 27] The evidence establishes that the only other entity besides the Complainant and her family to have custody of the laptop during the relevant period was the Organization. I accept the Organization's evidence that it is not its practice to access the hard drive in order to repair the type of problem experienced by the Complainant's laptop. However, the Organization's evidence is also that once the decision to buy out the Complainant's laptop was made, it stored the Complainant's laptop for two days, between July 22, 2008 and July 24, 2009, in an area where hard drives are removed and destroyed as a standard procedure. The Organization has provided no evidence that it took any measures to ensure that the Complainant's laptop was not subjected to its standard procedure of hard drive destruction in the two days the laptop was located in that area. The Organization raises the possibility -- in its words, "a hypothetical circumstance" -- that the hard drive may have been removed and destroyed, but has not submitted any evidence regarding the arrangements in place to prevent against this possibility that would have the effect of discounting it.

[para 28] In weighing the evidence of the parties and for the reasons above, I find that it is more probable than not that the hard drive containing the Complainant's family's personal information was removed by an employee of the Organization, once the laptop was placed with the buyouts, and was destroyed according to the Organization's standard practice.

Issue B: If the answer to number 1 is yes, was this a function of the fact that the Organization failed to make reasonable security arrangements to protect personal information in its custody?

[para 29] As I have found that it is likely that the hard drive containing the Complainant's family's personal information was removed from the Complainant's lap top by an employee of the Organization, I must consider whether this was a function of

the fact that the Organization failed to make reasonable security arrangements to protect the Complainant's personal information.

[para 30] Section 34 of PIPA imposes a duty on organizations to protect personal information in their custody or under their control. It states:

> *34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.*

It is not enough for an organization to make security arrangements to protect against unauthorized access; it must also protect personal information from such things as unauthorized disposal or destruction. In an inquiry, an organization usually bears the burden of proving on a balance of probabilities that it has met its duties under PIPA, such as the duty imposed by section 34.

[para 31] In the present case, the Organization has not provided any evidence to establish that it has reasonable security arrangements in place to protect against the unauthorized disposal or destruction of the personal information contained on hard drives located in its buyout area. For that reason alone, I find that the Organization has not established that it has made reasonable security arrangements to protect against the risk of unauthorized disposal or destruction for the purposes of section 34 of PIPA.

[para 32] However, the question originally posed for the inquiry is whether the removal of the hard drive was a function *of the fact* of the Organization's failure to make reasonable security arrangements. Consequently, even though the burden of proof on the Organization would normally be to establish that it met its duty on the balance of probabilities, the wording of this question suggests that an absence of evidence is not enough to find that the Organization failed to make reasonable security measures under PIPA. I say this because according to the question, I must find as a fact that the Organization failed to make reasonable security arrangements, which suggests that I must find that it actually failed to do so. This is somewhat different than finding that an Organization hasn't proven that it made reasonable security arrangements.

[para 33] However, in this case, I find that the Organization's evidence establishes that when it took custody of the Complainant's laptop, it did not make reasonable security arrangements to protect against foreseeable risks such as unauthorized disposal and destruction of personal information.

[para 34] I make this finding because the Organization never determined whether it had custody of the Complainant's personal information, and if so, whether she authorized disposal or destruction of such personal information. Specifically, the Organization did not ask the Complainant whether:

1) The Complainant's laptop contained a hard drive

2) The Complainant authorized disposal or destruction of any personal information on the hard drive in the event it was to be bought out, or whether the Complainant wanted the personal information to be returned to her.

[para 35] In order to protect against unauthorized disposal or destruction of personal information, when there is a risk that this kind of information could be disposed of or destroyed, as is the case with information contained on hard drives located in the Organization's buyout area, it is necessary to determine whether one has custody or control of personal information and whether one has authorization to dispose of or destroy it. The Organization's evidence establishes that it did not know whether it had custody of the Complainant's hard drive and does not determine whether a laptop has a hard drive when it accepts laptops with power up problems for repair.

[para 36] In my view, the Organization ought to have determined whether the laptop contained a hard drive when it first took custody of it and documented that it had a hard drive. By this I do not mean that the Organization should have accessed the contents of the hard drive; rather, it should have asked the Complainant whether the laptop had a hard drive or observed whether the laptop had a hard drive. It should also have determined the Complainant's wishes regarding the information the hard drive contained and documented them. Once the laptop was diagnosed by the technician, he too should have documented whether the Complainant's laptop had a hard drive and noted the Complainant's instructions regarding the information on the hard drive. Prior to being removed to and stored in an area where hard drives are routinely destroyed, the status of the hard drive and the Complainant's wishes regarding the information on the hard drive should have been clearly documented to protect against the risk of unauthorized destruction through employee error. Finally, the Organization should also have determined, by referring to its documentation, whether the laptop contained the hard drive when it returned it to the Complainant.

[para 37] That employee error is possible and that employees are not always aware of procedures in this Organization is documented by the following statement from its submissions:

> The incident was not reported to the Privacy Officer, in contravention of the direction of senior management to all stores and other facilities that all incidents involving possible privacy breaches be reported immediately to the Director of Operations. The Director of Operations is responsible for consulting with the Privacy Officer about the appropriate response to each potential privacy issue.

The above indicates that even though the Organization has a procedure in relation to possible privacy breaches, these were not followed in relation to the incident that is the subject of this inquiry. As employees do not always follow procedures, it can be necessary to take steps to lessen the risks posed by employee error, particularly in relation to the security of personal information.

[para 38] If the Organization had taken steps to determine whether it had possession of the Complainant's hard drive and her wishes regarding the personal information it contained when it took possession of the laptop, insured that the status of the hard drive was documented at each stage of its treatment of the laptop, and had confirmed that it was returning the hard drive to her with her laptop, it would have reduced the risk that the personal information on the hard drive would be subject to unauthorized destruction or disposal. Moreover, documenting possession of the hard drive through all stages of its procedures would have assisted the Organization to locate the hard drive once it was determined to be missing. However, it did not take steps of this kind, and has explained that its practice is not to determine whether a laptop has a hard drive when dealing with "power up" problems on laptops. Finally, if the Organization had documented the Complainant's wishes regarding the hard drive and created written instructions to staff members not to destroy the hard drive before it placed the laptop in the buyout area, it could have guarded against the risk that the laptop would become subject to the Organization's standard practice of hard drive removal and destruction.

[para 39] For the reasons above, I find that the loss of the Complainant's hard drive was a function of the fact that the Organization failed to make reasonable security arrangements to protect her personal information from unauthorized disposal and destruction. As the Organization has explained that the practice its employees followed regarding the Complainant's hard drive is standard in relation to computer hard drives it intends to buy out, I find that the evidence establishes that it has failed to make reasonable security arrangements to protect against disposal of destruction of customers' hard drives in similar circumstances.

[para 40] I find that the Organization has failed to make reasonable security arrangements to protect against the unauthorized disposal and destruction of personal information located on hard drives, in situations where it intends to buy out the computer. I therefore find that the Organization is not in compliance with its duty under section 34 of PIPA.

IV. ORDER

[para 41] I make this Order under section 52 of the Act.

[para 42] I order the Organization to make reasonable security arrangements to protect against the unauthorized disposal and destruction of personal information contained on the hard drives given to it by its customers to repair. Compliance with this portion of the order includes asking the following questions when the Organization receives computers for repair from customers and documenting the answers:

1) Does the customer's computer contain a hard drive?
2) Does the customer authorize disposal or destruction of any personal information on the hard drive in the event the computer is to be bought out or does the customer require it to be preserved?

Compliance with this portion of the Order also requires documenting the presence or absence of the hard drive, and the customer's wishes regarding the hard drive, if present, through all stages of the repair or buyout process.

[para 43] I further order the Organization to notify me, in writing, within 50 days of receiving a copy of this Order, that it has complied with the Order.

_____

Teresa Cunningham
Adjudicator