ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-03

HINTON WOOD PRODUCTS, A DIVISION OF WEST FRASER MILLS LTD.

February 22, 2013

(Case File #P2214)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* ("PIPA"), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[2] On December 3, 2012, Hinton Wood Products, A Division of West Fraser Mills Ltd. (the "Organization") provided notice of an incident involving the unauthorized access to personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] The Organization is an extra-provincial registered corporation operating in Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information concerning 340 employees (the "Affected Individuals"):

- name,
- address,
- salary,
- year to date earnings,
- overtime earnings,
- deductions (union dues and, if applicable, donations and garnishments), and
- social insurance number and birthdate for 35 of the Affected Individuals.

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] Between December 3, 2012, and February 1, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between December 13, 2012, and February 1, 2013.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- On November 23, 2012, the Organization was notified by an employee that he had been contacted by an unidentified coworker who had commented on the employee's earnings.
- The Organization investigated the matter and determined the following:
    - The personal information at issue was inadvertently stored on a network drive accessible to 435 employees in British Columbia and Alberta. The personal information may have been accessible on the drive since 2007.

        - Between April and November 2012, at least 8 employees accessed documents containing the personal information. The Organization confirmed this using a Microsoft Word feature which tracks documents recently accessed.
        - The Organization is unable to confirm whether or not any other access occurred as no system audit capability was implemented.
- The personal information at issue has since been moved to a secure location.
- A security audit is being conducted.
- The Affected Individuals were notified about the incident in a letter dated December 3, 2012.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[10] In considering whether to require the Organization to notify the Affected Individuals, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[11] Pursuant to section 37.1 of PIPA, I have the power to require the Organization to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require the Organization to notify the Affected Individuals, I must consider if there is a "real risk of significant harm" to the Affected Individuals as a result of the incident.

[12] In order for me to require that the Organization notify the Affected Individuals, there must be some harm – some damage or detriment or injury – that could be caused to those Affected Individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] The Organization reported the following with respect to the harm that could occur to the Affected Individuals in this incident:

- No significant harm could occur as a result of unauthorized access to general information about earnings and deductions. Salary information is published in the collective agreement and is generally known to all employees. Overtime is earned according to the collective agreement and employees are generally aware of overtime earned. Employee deductions, with the exception of donations and garnishments, are standard and known to all employees.
- There is a low risk of embarrassment or damage to reputation as a result of unauthorized access to garnishment information.
- A significant risk of identity theft or fraud exists for the 35 Affected Individuals whose personal information included social insurance numbers and birthdates.

[14] In my view, names, addresses, salary, overtime, year-to-date earnings, and union dues are low to moderately sensitive information. There is no significant harm that could

occur to the Affected Individuals as a result of unauthorized access to this information given that this information is generally known to all employees.

[15] Similarly, information about donations is of low sensitivity. In my view, there is no significant harm that could occur to the Affected Individuals as a result of unauthorized access to this information.

[16] As there is no risk of significant harm that could result from unauthorized access to the above information, I do not need to consider whether there is any real risk of such harm occurring. The Organization is not required to notify those Affected Individuals of this incident.

[17] Information about garnishment deductions, however, is moderately sensitive. The type of harm that could occur as a result of unauthorized access to this information is embarrassment, hurt, humiliation, and damage to reputation. In my view, these are significant harms.

[18] Social insurance numbers and birthdates are highly sensitive information. This information could be used to commit identity theft and fraud. In my view, identity theft and fraud are significant harms.

[19] In order for me to require the Organization to notify these Affected Individuals whose personal information involves social insurance numbers and birthdates or garnishment information there must also be a "real risk" of significant harm to them as a result of this incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.

[20] The Organization reported the incident poses a low risk of harm to the Affected Individuals. The Organization submits that the personal information was accessed by an employee out of curiosity with no evidence of malicious intent.

[21] In deciding whether there exists a "real risk" of significant harm in this incident to the Affected Individuals whose personal information involves social insurance numbers and birthdates or garnishment information, I considered the following factors:

- Garnishment information is moderately sensitive information. Unauthorized access to this information could result in the significant harms of embarrassment, hurt, humiliation, and damage to reputation.
- Social insurance numbers and birthdates are highly sensitive information. Unauthorized access to this information could result in the significant harms of identity theft and fraud.
- At least 8 coworkers of the Affected Individuals accessed the personal information between April and November, 2012.

- The Organization has no way of knowing how many other coworkers accessed the personal information of these particular Affected Individuals.
- The personal information may have been accessible since 2007.

[21] In P2011-ND-016, Commissioner Work found a real risk of significant harm existed as a result of 240 employees having unauthorized access to highly sensitive employee files over a period of 15 months. The personal information at issue in that incident included names and social insurance numbers. Similar to the circumstances in this incident, the organization was unable to determine how many employees accessed the highly sensitive personal information as there was no system audit capability.

[22] In P2010-ND-004 and P2012-ND-10, an important factor in deciding whether a real risk of hurt, humiliation, and damage to reputation existed was proximity in the employment context. In these cases, coworkers having knowledge of garnishment deductions was enough to give rise to a real risk of harm to the affected individuals in the form of embarrassment, hurt, humiliation, and damage to reputation.

[23] Based on the above and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the Affected Individuals in this case whose personal information involved social insurance numbers and birthdates or garnishment information.

V. Decision

[24] I require the Organization to notify the Affected Individuals whose personal information involved social insurance numbers and birthdates or garnishment information in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[25] I understand the Organization has notified those Affected Individuals in accordance with the Regulation in a letter sent on December 3, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner