ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2022-03

March 3, 2022

LITTLE A ACCOUNTING and SUSAN WASSON, also known as SUE WASSON, operating as LITTLE A ACCOUNTING

Case File Number 014048

Office URL: www.oipc.ab.ca

Summary: The Complainant complained to the Commissioner that Little A Accounting (Little A Accounting and Susan Wasson, also known as Sue Wasson, operating as Little A Accounting (the Organization)) disclosed her personal information in contravention of the *Personal Information Protection Act* (PIPA). The Complainant complained that an email originating from the Organization's email account was sent to the Complainant's employer, a school board. The email alleged that the Complainant was a heavy drug user. The email also contained the Complainant's name, address, occupation, social insurance number and date of birth.

The Adjudicator found that the Complainant's name, occupation, address, social insurance number and date of birth was personal information in the custody and control of the Organization. The Adjudicator found that the Organization had disclosed the Complainant's personal information when the Organization's owner/operator emailed the Complainant's employer without consent. The Adjudicator found that there was no evidence that the Organization had taken any steps to protect the personal information in its custody or control, as required by section 34 of PIPA. The Adjudicator ordered the Organization to cease disclosing the Complainant's personal information and to develop policies to protect personal information in its custody or control.

Statutes Cited: AB: *Personal Information Protection Act*, S.A. 2003, c. P-6.5, ss. 1, 5, 7, 19, 20, 34, 52

Authorities Cited: AB: Orders P2012-02, P2013-04

1. BACKGROUND

[para 1] The Complainant complained to the Commissioner that Little A Accounting (Little A Accounting and Susan Wasson, also known as Sue Wasson, operating as Little A Accounting (the Organization)) disclosed her personal information in contravention of the *Personal Information Protection Act* (PIPA). The Complainant complained that an email originating from a Hotmail account, with which the Organization had contacted her when it provided accounting services, was sent to the Complainant's employer, a school board. The email alleged that the Complainant was a heavy drug user. The email also contained the Complainant's name, address, occupation, social insurance number and date of birth.

[para 2] The Commissioner authorized a senior information and privacy manager to investigate and attempt to mediate the matter. The Complainant requested an inquiry and the Commissioner agreed to conduct an inquiry. The Commissioner delegated her authority to conduct the inquiry to me.

[para 3] The Organization did not provide submissions for the inquiry and refused correspondence from this office regarding the inquiry. The Complainant provided submissions and evidence for the inquiry.

II. ISSUES

ISSUE A: Did the Organization disclose "personal information" of the Complainant as that term is defined in the Act?

ISSUE B: If the answer to Issue A is "yes", did the Organization disclose personal information contrary to, or in compliance with, section 7(1)(d) of PIPA (no disclosure without either authorization or consent)? In particular, did the Organization have the authority to disclose the information without consent, as permitted by section 20 of PIPA?

ISSUE C: If the answer to Issue B is "yes", did the Organization disclose the information only for purposes that are reasonable and only to the extent that was reasonable, as permitted by section 19 of the Act?

ISSUE D: Did the Organization comply with section 34 of the Act (reasonable security arrangements)?

III. DISCUSSION OF ISSUES

ISSUE A: Did the Organization disclose "personal information" of the Complainant as that term is defined in PIPA?

[para 4] PIPA prohibits organizations from disclosing personal information in their custody or control except in accordance with its provisions. Section 1(1)(k) of PIPA defines "personal information" as "information about an identifiable individual".

[para 5] Section 5(1) of PIPA establishes that organizations are responsible for the personal information in their custody or control.

> *5(1) An organization is responsible for personal information that is in its custody or under its control.*

Organizations must comply with PIPA with regard to personal information in their custody or control; however, Organizations do not have obligations in relation to information that is not in their custody or control.

[para 6] Section 7 sets out the basic rules that organizations must follow when they collect, use, or disclose personal information. It states:

> *7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,*
>
> *(a) collect that information unless the individual consents to the collection of that information,*
>
> *(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,*
>
> *(c) use that information unless the individual consents to the use of that information, or*
>
> *(d) disclose that information unless the individual consents to the disclosure of that information.*
>
> *(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.*
>
> *(3) An individual may give a consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.*

[para 7] The Complainant states:

On April 22, 2019, my former accountant – […] - sent an email to my place of work defaming me in an act of vengeance; she tried to ruin my reputation, with the intention of getting me fired, by accusing me of being a "chronic drug abuser". The email was sent from her business email: […] In this email, she included my full name, address, social insurance number, and my date of birth. I confirm that this is [the owner/operator's] email, as I previously received accounting correspondence from her.

A week prior, on April 15, 2019, I had questioned [the owner/operator] about her accounting fees, and she was very ambiguous and curt in her responses. I had referred four friends to her, and three of them ended up using her accounting services […]; we had our taxes filed through her home-based business called, "Little A Accounting". After speaking with my friends, we realized that [the owner/operator] did not honour her word of a 10% discount for referrals or being a repeat customer. Both […] and myself were repeat customers, plus had referred my friends to her. [The owner/operator] and I exchanged a number of text messages about the matter, and I addressed the issue of her charging me $388.00 as opposed to $350.00 the previous year (clearly, no discount was applied on top of the fact that I had minimal investing transactions in 2018 as opposed to 2017); however, no resolution came about. [Two acquaintances of the Complainant] were charged $1000 for her services (significantly higher than the previous year), and [one acquaintance]was rightfully upset; he subsequently sent her an email stating that he was not happy with her service and exorbitant fee and that he would be taking his business elsewhere.

Shortly after my text conversations with [the owner/operator], and after […] sent his termination email (to [the owner/operator's] Hotmail account), [the owner/operator] deleted me, my mom […] and […] (the fourth potential client that did not end up using her services) from her Instagram and Facebook accounts. Her Instagram account is: […]. We were all shocked at the immediacy of her deleting us. Essentially, she was upset that she lost six clients in one day. A week later (on April 22), she sent the defamatory email to my place of work […] with my personal information. I do not know what else she is doing with my SIN number, and I fear she may do more with both my information and that of my friends.

Today (April 30), my mom and I both asked [the Organization's owner /operator] (via text message) why she sent the email, and she denied any responsibility, stating that "her account was hacked a while ago". However, if this is true, she never informed any of her clients of this breach and the potential of their data being compromised — this is a serious violation of both privacy and security. [The owner/operator] was extremely defensive in her responses (see the text message log), and she did not respond like that of a person who just discovered that her email account had been "hacked" — never once did she apologize about the breach, nor did she mention that she must be vigilant in informing her clients of this update. Additionally, [the owner/operator] continues to use her Hotmail account, as she recently (on April 20) sent a tax invoice to a friend of my mom's (despite claiming that her account has been supposedly hacked). The fact that [the owner/operator] continues to use her Hotmail account, with the knowledge of a supposed breach, is very alarming. She denies all wrongdoing, but her stories do not make any sense. [The owner/operator] even denies having an Instagram account now.

Back to the email that was sent to my place of employment - I find that [the owner/operator's] "hacker" explanation does not make any sense, as the message is targeted specifically towards me, sans extortion. The sender has the intent of harming my reputation, with no intention of monetary gain; it is clear that the sender simply wants to cause turbulence in my life. I believe the motive is that [the owner/operator] was bitter about losing clients. Consequently, [the owner/operator's] actions are undermining my ability to focus at work, and I have suffered mental distress; her correspondence could potentially damage my career.

Ultimately, I am concerned that [the owner/operator] is still operating an accounting business, despite her own acknowledgement of an apparent "breach of security". Even more concerning is that this woman continues to handle her clients' personal information in a haphazard and

> potentially criminal manner. She has shared my personal information without my consent, and she has acted vindictively.

[para 8] The Complainant submitted a copy of the email that had been sent to her workplace, a board of education. The email contains her address, occupation, date of birth, and social insurance number. It states: "Chronic drug abuse. Her ex-husband has photos of her doing cocaine with her friends. She's an avid magic mushroom user, among other things." The email address of the sender is that of the owner/operator of the Organization. The title of the email is "One of your teachers is doing drugs."

[para 9] The Complainant's uncontested evidence is that an email was sent from the owner/operator to the school where the Complainant worked. This email contained the Complainant's name, occupation, address, date of birth, and social insurance number. This information is about the Complainant as an identifiable individual and information that the Organization would have in its custody or control, as it would need to collect this information from the Complainant in order to provide accounting services.

[para 10] I find that the allegations regarding drug use do not have as their source personal information in the custody or control of the Organization. While it is unclear what the source of these allegations is, I take notice that tax preparation and accounting do not involve collecting or using this kind of information.

[para 11] PIPA is engaged by this disclosure because the email contains personal information that was collected by the Organization when it provided accounting services to the Complainant: specifically, the Complainant's name, occupation, address, date of birth, and social insurance number. PIPA is not engaged by the allegations of drug use contained in the email.

[para 12] As the email was sent from Hotmail account used by the Organization in order to provide accounting services to the Complainant in the past, and as the Complainant's name, occupation, address, date of birth, and social insurance number were contained in the email, and as the Complainant's evidence is uncontested, I find, on the balance of probabilities, that the Organization sent the email to the Complainant's employer, and that it disclosed the Complainant's personal information when it did so.

ISSUE B: If the answer to Issue A is "yes", did the Organization disclose personal information contrary to, or in compliance with, section 7(1)(d) of PIPA (no disclosure without either authorization or consent)? In particular, did the Organization have the authority to disclose the information without consent, as permitted by section 20 of PIPA?

[para 13] Cited above, section 7(1)(d) of PIPA prohibits an organization from disclosing an individual's personal information, unless the individual consents to the disclosure, or a provision of section 20 of PIPA authorizes disclosing the information without consent.

[para 14] I am unable to identify a provision of section 20 that would authorize the disclosure of the Complainant's personal information in this case without her consent. Moreover, the Complainant did not provide her consent to the Organization to disclose the information in the email to her employer. The disclosure contravened section 7(1)(d) of PIPA.

[para 15] As I have found that the Organization disclosed the Complainant's personal information without consent in contravention of section 7(1)(d) of PIPA, I must order the Organization to cease disclosing the Complainant's personal information in contravention of PIPA.

ISSUE C: If the answer to Issue B is "yes", did the Organization disclose the information only for purposes that are reasonable and only to the extent that was reasonable, as permitted by section 19 of the Act?

[para 16] I have already found that the Organization contravened section 7(1)(d) of PIPA when it sent the email to the Complainant's employer. As a result, I need not answer this question.

ISSUE D: Did the Organization comply with section 34 of the Act (reasonable security arrangements)?

[para 17] Section 34 of PIPA requires an organization to make reasonable security arrangements regarding the personal information in its custody or 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.*

[para 18] In Order P2013-04, the Adjudicator reviewed past orders interpreting section 34 and said:

> An organization has the burden of proving that it made reasonable security arrangements to protect personal information in its custody or under its control, as it is in the best position to provide evidence of the steps that it has taken (Orders P2009-013/P2009-014 at para. 109). To be in compliance with section 34, an organization is required to guard against reasonably foreseeable risks; it must implement deliberate, prudent and functional measures that demonstrate that it considered and mitigated such risks; the nature of the safeguards and measures required to be undertaken will vary according to the sensitivity of the personal information (Order P2006-008 at para. 99).

[para 19] As noted above, the Organization did not make submissions for the inquiry. As set out in Order P2013-04, the Organization bears the burden of demonstrating that it has taken deliberate, prudent and functional measures to protect personal information in its custody or control. The fact that the Organization has not provided evidence or submissions makes it impossible for it to meet its burden. This is especially so, given my finding that it disclosed personal information without authority

under PIPA to do so. Moreover, the fact that the Complainant's personal information is contained in an email that appears to have been written from purely personal motives, supports concluding that the Organization has no policies in place to protect personal information from risks such as unauthorized access and disclosure.

[para 20] In Order P2012-02, the Adjudicator determined that the reasonableness of measures necessary to protect personal information relates directly to the sensitivity of personal information and the likelihood of the risk to personal information. He said:

> However, section 34 of PIPA does not require an organization to comprehensively investigate all privacy breaches and conclusively determine what happened in every respect. What constitutes reasonable security arrangements depends on the magnitude of risk and the likelihood that it will materialize. An individual whose personal information has been compromised will no doubt want the utmost to be done to prevent any possibility of harm whatsoever. However, as noted by the Organization, the standard required by section 34 must be viewed objectively, not subjectively through the eyes of the individual whose personal information is at issue. Indeed, this is the standard effectively set out in section 2.
>
> I conclude that, due to the nature of the Complainant's personal information that was disclosed and other relevant circumstances suggesting that the risk of identity theft, humiliation or damage to reputation was minimal, the Organization was not required to describe the envelope to the third party and instruct that it not be opened, and was not required to contact the third party to determine whether anyone else had seen its contents. In order to make reasonable security arrangements as required by section 34 of PIPA, it was sufficient for the Organization to take steps to ensure that the mail was returned to it in a timely manner

[para 21] The Organization provides accounting services and completes tax returns for its customers. Providing these services necessitates collecting personal information such as social insurance numbers and income information. In this case, the information that was disclosed to the Complainant's employer – the Complainant's address, occupation, employer, social insurance number and date of birth – is information that could be used to steal the Complainant's identity. I find that this information is highly sensitive, as described in Order P2012-02. Moreover, the risk that the security of client information could be compromised by representatives of the Organization using and disclosing personal information for unauthorized purposes is a foreseeable risk, contemplated by section 34.

[para 22] As there is no indication that the Organization has policies in place to assist it to comply with PIPA, or to safeguard the Complainant's personal information, or that of other clients, I must direct the Organization to develop policies to assist it to protect personal information in its custody or control.

IV. ORDER

[para 23] I make this Order under section 52 of PIPA.

[para 24] I order the Organization to cease disclosing the Complainant's personal information in contravention of PIPA.

[para 25] I order the Organization to develop policies regarding the disclosure of personal information in its custody or control as a reasonable measure to protect the information against the risk of unauthorized disclosure.

[para 26] I order the Organization to inform me within 50 days of receiving this order that it has complied with it.

_____

Teresa Cunningham
Adjudicator
/kh