ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2013-04

October 17, 2013

TD INSURANCE

Case File Number P1435

Office URL: www.oipc.ab.ca

Summary: The Complainant, the sole holder of an automobile insurance policy, complained that the Organization contravened the *Personal Information Protection Act* (the "Act") when it conveyed information about him and his insurance policy to his ex-wife over the telephone and by fax.

The Organization explained that it was the victim of fraud on the part of the ex-wife, and did not argue that it had any authority or consent to disclose the Complainant's personal information. The Adjudicator concluded that the Organization had contravened the Act, and ordered it to stop disclosing personal information in contravention of the Act, or in circumstances that are not in compliance with the Act.

The Adjudicator also found that the Organization had failed to make reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of the Act.

Statutes Cited: AB: *Personal Information Protection Act*, S.A. 2003, c. P-6.5, ss. 1(1)(k), 7(1), 8, 8(1), 8(2), 8(2)(a), 8(2)(b), 8(3), 8(3)(a), 8(3)(b), 8(3)(c), 20, 34, 52, 52(3)(a), 52(3)(e), 52(4) and 60(1); *Personal Information Protection Amendment Act, 2009*, S.A. 2009, c. 50.

Authorities Cited: AB: Orders P2005-001, P2006-008 and P2009-013/P2009-014.

I. BACKGROUND

[para 1] The Complainant has an automobile insurance policy with TD Insurance (the "Organization") and he is the sole policy holder. In a form dated September 27, 2009 with an attached letter dated September 11, 2009, he complained that the Organization contravened the *Personal Information Protection Act* (the "Act" or "PIPA") by providing his insurance policy information, over the telephone and by fax, to his ex-wife without his permission and knowledge.

[para 2] The former Commissioner authorized a portfolio officer to investigate and attempt to resolve the matter. This was not successful, and the Complainant requested an inquiry in forms dated January 25 and February 16, 2012. A written inquiry was set down.

[para 3] The Complainant has also requested access to a copy of an audio recording that the Organization made at the time that one of its representatives spoke to his ex-wife, but that access request is the subject of a different case file number, being P2063.

[para 4] On May 1, 2010, amendments to PIPA came into force by virtue of the *Personal Information Protection Amendment Act, 2009*. While the Organization's alleged contravention of the Act occurred in September 2009, the substance of the relevant provisions was not changed by the 2010 amendments.

II. INFORMATION THAT IS THE SUBJECT OF THE COMPLAINT

[para 5] The information that is the subject of the complaint in this inquiry is information relating to the Complainant and his insurance policy, as contained in a transcript of a telephone conversation between a representative of the Organization and the Complainant's ex-wife, and in an Automobile Insurance Confirmation and a Temporary Automobile Liability Insurance Card faxed to the Complainant's ex-wife by another representative of the Organization.

III. ISSUES AND SUB-ISSUES

[para 6] The Notice of Inquiry, dated December 21, 2012, set out the following issues and sub-issues:

> Did the Organization disclose "personal information" of the Complainant, as that term is defined in PIPA?
>
> Did the Organization disclose the Complainant's information contrary to, or in compliance with, section 7(1) of PIPA (no disclosure without either authority or consent)? In particular,
>
> > Did the Organization have the authority to disclose the Complainant's information without consent, as permitted by section 20 of PIPA?

If the Organization did not have the authority to disclose the Complainant's information without consent, did the Organization obtain the Complainant's consent in accordance with section 8 of PIPA before disclosing the information? In particular,

Did the Complainant consent in writing or orally? or

Is the Complainant deemed to have consented by virtue of the conditions in sections 8(2)(a) and (b) having been met? or

Is the disclosure permitted by virtue of the conditions in sections 8(3)(a), (b) and (c) having been met?

Did the Organization comply with section 34 of PIPA (reasonable security arrangements against unauthorized disclosure)?

IV. DISCUSSION OF ISSUES

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

[para 7] Under section 1(1)(k) of PIPA, "personal information" is defined as follows:

> *1(1)(k) "personal information" means information about an identifiable individual;*

[para 8] I find that the Organization disclosed the Complainant's personal information. A transcript of the telephone conversation that occurred between a representative of the Organization and the Complainant's ex-wife on September 10, 2009 indicates that the representative disclosed the fact that the Complainant had an insurance policy, the type of vehicle that he owned, the amount of insurance coverage that he had, the applicable deductibles, and whether he had rental car coverage. The Organization also acknowledges that a second representative subsequently faxed the Complainant's ex-wife the Automobile Insurance Confirmation and the Temporary Automobile Liability Insurance Card, which included the Complainant's name, his address, the type of vehicle that he owned, the amount of coverage issued to him, the applicable deductibles, and the fact that there was a lien on the vehicle by a particular lienholder, in other words that the Complainant had particular financing on the vehicle.

[para 9] Because the disclosure of the Complainant's personal information has been established, the Organization has the burden to show that its disclosure of the information was in accordance with PIPA (Order P2005-001 at para. 8; Order P2006-008 at para. 17).

B. Did the Organization disclose the Complainant's information contrary to, or in compliance with, section 7(1) of PIPA (no disclosure without either authority or consent)?

[para 10] Section 7(1) of PIPA reads, in part, as follows:

> *7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,*
>
> *…*
>
> *(d) disclose that information unless the individual consents to the disclosure of that information.*

[para 11] The above provision is to the effect that the Organization was not authorized to disclose the Complainant's personal information unless he consented, or unless "this Act provides otherwise". The latter means, in the context of this inquiry, that the Organization potentially had the authority to disclose the Complainant's personal information in reliance on section 20.

1. Did the Organization have the authority to disclose the Complainant's information without consent, as permitted by section 20 of PIPA?

[para 12] Section 20 of PIPA reads, in part, as follows:

> *20 An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable:*
>
> *…*

Section 20 sets out an exhaustive list of circumstances in which, or purposes for which, an individual's personal information may be disclosed without his or her consent. The Organization does not argue, and I do not find, that any of them apply so as to have given the Organization the authority to disclose the Complainant's personal information to his ex-wife without his consent.

[para 13] Rather, the Organization says that it was the victim of fraud. It explains that the Complainant's ex-wife, wanting to rent a vehicle in Texas, contacted a representative of the Organization, purporting to be the holder of the insurance policy in question. She elicited information about the insurance policy, convinced the representative to change the gender noted on file by altering the title of the policy holder from "Mr." to "Mrs.", and arranged the purchase of car rental coverage. The Complainant's ex-wife then contacted another representative of the Organization and arranged for the Automobile Insurance Confirmation and the Temporary Automobile Liability Insurance Card to be faxed to her.

2. If the Organization did not have the authority to disclose the Complainant's information without consent, did the Organization obtain the Complainant's consent in accordance with section 8 of PIPA before disclosing the information? In particular,

Did the Complainant consent in writing or orally? or

Is the Complainant deemed to have consented by virtue of the conditions in sections 8(2)(a) and (b) having been met? or

Is the disclosure permitted by virtue of the conditions in sections 8(3)(a), (b) and (c) having been met?

[para 14] Section 8 of PIPA reads, in part, as follows:

8(1) An individual may give his or her consent in writing or orally to the collection, use or disclosure of personal information about the individual.

(2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an organization for a particular purpose if

(a) the individual, without actually giving a consent referred to in subsection (1), voluntarily provides the information to the organization for that purpose, and

(b) it is reasonable that a person would voluntarily provide that information.

…

(3) Notwithstanding section 7(1), an organization may collect, use or disclose personal information about an individual for particular purposes if

(a) the organization

(i) provides the individual with a notice, in a form that the individual can reasonably be expected to understand, that the organization intends to collect, use or disclose personal information about the individual for those purposes, and

(ii) with respect to that notice, gives the individual a reasonable opportunity to decline or object to having his or her personal information collected, used or disclosed for those purposes,

(b) the individual does not, within a reasonable time, give to the organization a response to that notice declining or objecting to the proposed collection, use or disclosure, and

(c) having regard to the level of the sensitivity, if any, of the information in the circumstances, it is reasonable to collect, use or disclose the information as permitted under clauses (a) and (b).

...

[para 15] Section 8 sets out alternative circumstances in which the Organization could have disclosed the Complainant's personal information, as noted by the sub-issues above. Given the facts, as summarized earlier in this Order, none of those circumstances existed in this case. Thn Complainant neither consented to the disclosure of his personal information within the terms of section 8(1) or 8(2), nor was he notified in accordance with section 8(3).

3. Conclusion as to whether the Organization disclosed the Complainant's information contrary to, or in compliance with, section 7(1) of PIPA

[para 16] As the Organization did not have the consent of the Complainant to disclose his personal information, and did not have the authority to do so without his consent, whether on the basis of one of the circumstances or purposes enumerated in section 20 or on the basis of notice under section 8(3), I conclude that the Organization disclosed the Complainant's personal information contrary to section 7(1) of PIPA.

C. Did the Organization comply with section 34 of PIPA (reasonable security arrangements against unauthorized disclosure)?

[para 17] Section 34 of PIPA reads as follows:

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] 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] The Organization says that protecting the privacy and confidentiality of its clients is a fundamental part of the way that it does business, and that it has had a Privacy Policy since 2004. It explains that, following the events that gave rise to the Complainant's complaint, it reviewed and revised its Client Authentication Procedure as well as password-protected the Complainant's account, which I take to mean that an individual calling the Organization would have to provide the password in order to discuss the account with a representative of the Organization. The Complainant responds that the password was in place for only a year, and that the Organization is not taking his privacy seriously.

[para 20] The Organization's Client Authentication Procedure, dated September 2012 and revised October 2012, requires its representatives to authenticate a client by asking a question about one of the client's particular relationships, such as with a lienholder, mortgagee, dealership or lawyer's office, and by asking another question about one of the client's past transactions with the Organization, such as a payment, last time of contact, or amount of a deductible. More than just two questions may be asked, but if the caller answer three questions incorrectly, does not sound confident in his or her answers, is being assisted by someone in the background, or has a voice that does not appear to match the demographics of the client such as his or her age (and I would add gender, given the facts of this particular inquiry), the representative must inform the caller that the transaction or inquiry cannot be completed, make notations in the data system accordingly, and transfer the caller to a team leader for further steps to be taken. The team leader might ask a different set of questions, refer to the physical file for further questions in order to authenticate the client, or pass the matter along to a manager. The Client Authentication Procedure does not state what steps the manager is to take.

[para 21] It is not my role in this inquiry to decide whether the Organization's current Client Authentication Procedure complies with section 34 of PIPA. Any changes to the Procedure made after the events that gave rise to the Complainant's complaint are not relevant to the issue of whether the Organization complied with section 34 in September 2009. Still, I commend the Organization for taking measures to strengthen the way in which it authenticates clients.

[para 22] I find that, at the time of the events that gave rise to the Complainant's complaint in September 2009, the Organization did not comply with section 34. While the Organization's first representative made attempts to authenticate the identity of the caller, she did so by asking for the Complainant's name, telephone number, mailing address, postal code and date of birth. Correct answers to these questions are quite likely where the caller knows the client of the Organization, or has obtained the personal documentation of the client, as found, for instance, in a wallet (e.g., a driver's licence, birth certificate) or in mail (e.g., bills, tax information). In reference to the test set out above, it is reasonably foreseeable that a caller who is not actually a client of the Organization would know the answers to the questions that were asked by the first representative of the Organization who spoke to the Complainant's ex-wife. The Organization therefore did not take appropriate measures to guard against the possibility of disclosing the Complainant's personal information to an unauthorized caller.

[para 23] Further, the Organization acknowledges that its representative who first spoke to the Complainant's ex-wife by telephone "felt uncomfortable" sending her the Automobile Insurance Confirmation and the Temporary Automobile Liability Insurance Card, so the representative did not proceed with that request. Nonetheless, the second representative, who was subsequently contacted by the Complainant's ex-wife, sent the documentation. This was despite the fact that the first representative not only foresaw that something may be awry but actually believed that something was awry. The first representative does not appear to have contacted a team leader or manager, or to have made a notation in the data system about her discomfort in dealing with the caller, such that a different representative would be aware of that discomfort and pursue the matter if the caller contacted the Organization again.

[para 24] I conclude that the Organization did not make reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of PIPA.

D. Comments on remedy

[para 25] I have concluded that the Organization improperly disclosed, and failed to protect, the Complainant's personal information. In his requests for inquiry and inquiry submissions, the Complainant asks for a letter of apology from the Organization, for a fine to be levied against the Organization, and for damages in the amount of $30,000 to be paid by the Organization.

[para 26] To my knowledge, this Office has never ordered an apology. While there may be legal or factual arguments to the effect that I have the authority to order one, I do not find this an appropriate case in which to explore those arguments. This is because the Organization has already formally apologized to the Complainant in its submissions of February 20 and April 5, 2013.

[para 27] As for the possibility of a fine or damages, I have no jurisdiction to levy or award these things. Having said this, section 60(1) of PIPA allows the Complainant to rely on this Order and pursue a cause of action against the Organization for damages for loss or injury that the Complainant has suffered as a result of the breach by the Organization of its obligations under the Act. At the same time, I note that the Organization has expressed its willingness to discuss the Complainant's request for compensation directly with him, if he provides evidence to support the requested amount.

V. ORDER

[para 28] I make this Order under section 52 of PIPA.

[para 29] I find that the Organization disclosed the Complainant's personal information in contravention of PIPA, or in circumstances that were not in compliance with PIPA. Under section 52(3)(e), I order the Organization to stop disclosing personal information in contravention of the Act, or in circumstances that are not in compliance with the Act.

[para 30] I find that the Organization did not make reasonable security arrangements to protect the Complainant's personal information, as required by section 34 of PIPA. Under section 52(3)(a), I order the Organization to perform its duty to protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized disclosure.

[para 31] Under section 52(4), I specify, as a term of this Order, that the Organization ensure that all of its officers and employees who routinely interact with members of the public are made aware of the foregoing obligations of the Organization under PIPA.

[para 32] I further order the Organization to notify me and the Complainant, in writing, within 50 days of receiving a copy of this Order that it has complied with the Order. The notification should indicate the Organization's acknowledgement of each of my orders in the preceding paragraphs, as well as describe the way in which the Organization has communicated its obligations under PIPA to the relevant officers and employees.

Wade Raaflaub
Adjudicator