

ALBERTA

**OFFICE OF THE INFORMATION AND PRIVACY
COMMISSIONER**

ORDER P2012-12

December 14, 2012

FAST LIFE INTERNATIONAL

Case File Number P1761

Office URL: www.oipc.ab.ca

Summary: The Complainant complained that her e-mail address was disclosed by Fast Life International (“the Organization”) contrary to the *Personal Information Protection Act* (“the Act”) when the Organization sent her e-mail address to an individual she met, but who she did not indicate was a “match” at a speed dating event.

The Adjudicator found that the Complainant’s e-mail address was her personal information and that it had been disclosed without her consent contrary to section 7 of the Act. The Adjudicator also found that the Organization had met its burden to prove that it had made reasonable security arrangements in compliance with section 34 of the Act. Finally, the Adjudicator found that the Organization had some policies and practices in compliance with section 6(1) of the Act but decided that the Organization needed to ensure that its employees were aware of the Organization’s obligations under the Act.

Statutes Cited: AB: *Personal Information Protection Act*, S.A. 2003, c. P-6.5, ss. 1, 6, 7, 8, 9, 20, 34, and 52.

Authorities Cited: AB: Orders P2009-013/014, P2010-021, P2012-02, and P2012-03.

I. BACKGROUND

[para 1] The Complainant attended a speed dating event organized by Fast Life International (“the Organization”). At the conclusion of the speed dating event, the Complainant was asked if there were any individuals at the event with whom she felt she

had a “match”. She did not, and was sent an e-mail by the Organization the following day confirming that she did not find a match.

[para 2] A few days later the Complainant received two e-mails from an individual who also attended the speed dating event. In one of the e-mails the individual stated that he had received the Complainant’s e-mail from the match results. The Complainant informed the individual that she did not select him as a match.

[para 3] The Complainant contacted the Organization and complained that her e-mail address had been shared with an individual that she did not select as a match. She received a response from the Organization that she did not find satisfactory, and when she followed up again with the Organization, she received no response at all.

[para 4] As a result, the Complainant complained to the Office of the Information and Privacy Commissioner (“this Office”) that the Organization had contravened the *Personal Information Protection Act* (“the Act”). The former Commissioner authorized a Portfolio Officer to investigate and attempt to resolve the issues between the parties. According to the submissions of the Organization, communications from the Portfolio Officer or the Complainant were not reaching the proper person due to the improper actions of a former employee. When the Portfolio Officer’s recommendations were brought to the attention of the right person at the Organization, they were apparently implemented, though, by this time, the Complainant had already requested an inquiry.

[para 5] The Notice of Inquiry was sent to both parties on December 14, 2011. I received initial submissions from the Complainant and Organization.

II. INFORMATION AT ISSUE

[para 6] The information at issue is the Complainant’s e-mail address.

III. ISSUES

[para 7] The Notice of Inquiry dated December 14, 2011 lists the issues for this inquiry as follows:

Did the Organization collect, use and/or disclose “personal information” of the Complainant as that term is defined in the Act?

Did the Organization collect, use and/or disclose the information contrary to, or in compliance with, section 7(1) of the Act?

If the Complainant consented to the collection, use, and/or disclosure of her personal information, did the Complainant withdraw consent within the terms of section 9(1) of the Act?

If the Complainant withdrew or varied any consent she had given, did the Organization comply with section 9(4) of the Act, or with section 9(4)(b) of the Act?

Did the Organization comply with section 34 of the Act by making reasonable security arrangements to protect personal information that is in its custody or under its control?

Did the Organization comply with section 6(1) of the Act by developing and following policies and practices that are reasonable for the Organization to meet its obligation under this Act?

IV. DISCUSSION OF ISSUES

A. Did the Organization collect, use and/or disclose “personal information” of the Complainant as that term is defined in the Act?

[para 8] Personal information is defined in section 1(k) of the Act as follows:

1(k) “personal information” means information about an identifiable individual;

[para 9] The information the Complainant submits was disclosed by the Organization was her personal e-mail address which appears to contain her first initials and her last name.

[para 10] In Order P2010-021, the Adjudicator found that an e-mail address was information about an identifiable individual. I find the same in this instance and note that neither party argued to the contrary.

B. Did the Organization collect, use and/or disclose the information contrary to, or in compliance with, section 7(1) of the Act?

[para 11] Section 7(1) of the Act prohibits an organization from collecting, using, or disclosing an individual’s personal information without consent. In this inquiry, the Complainant is complaining that her personal information was disclosed without her consent. Therefore, the relevant portions of section 7(1) state:

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 12] In her submissions, the Complainant states that she had consented to the disclosure of her e-mail address to individuals with whom she made a match. However, she did not consent to the disclosure of her e-mail address to individuals with whom she

did not make a match. The Organization did not contradict the Complainant's submissions in this regard and stated:

...I acknowledge that [the Complainant's] email address was given to someone without her permission at a speed dating event...

[para 13] Section 8 of the Act sets out the form consent may take. Based on the information provided to me by the parties, the portions of section 8 of the Act relevant to this inquiry state:

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.

....

[para 14] I have no evidence that the Complainant consented orally or in writing to the disclosure of her e-mail address. However, based on the evidence before me, I can infer that she did voluntarily give her e-mail address to the Organization for the purposes of the Organization communicating with her and also so individuals with whom she made a match could contact her. I believe it is reasonable that a person attending speed dating events hosted by the Organization would provide e-mail addresses for these particular purposes. Therefore, even if the Complainant did not consent orally or in writing to the disclosure of her e-mail address to persons with whom she made a match, there was deemed consent to disclose her e-mail address to those she chose as a match.

[para 15] However, the Organization disclosed the Complainant's e-mail address to an individual that she did not choose as a match. Therefore, the Organization disclosed the Complainant's personal information without her consent.

[para 16] Section 20 of the Act lists circumstances in which an organization is permitted to disclose individuals' personal information without consent. None of the provisions of section 20 of the Act are applicable in this inquiry.

[para 17] As no other provision potentially conferring authority for the disclosure was put forward by the Organization and I have found that section 20 of the Act is not applicable, I conclude that the disclosure of the Complainant's e-mail address to an individual to whom she did not make a match was contrary to the Act.

C. If the Complainant consented to the collection, use, and/or disclosure of her personal information, did the Complainant withdraw consent within the terms of section 9(1) of the Act?

[para 18] Given my finding that the Complainant did not consent to the disclosure of her personal information, section 9 is not applicable in this inquiry.

D. Did the Organization comply with section 34 of the Act by making reasonable security arrangements to protect personal information that is in its custody or under its control?

[para 19] Section 34 of the Act 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 20] In order to comply 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).

(Order P2012-03 at para 29)

[para 21] Organizations have the burden to prove that they made reasonable security arrangements against the risks listed in section 34 of the Act (Order P2012-02 at para 22, P2009-013/014 at para 109).

[para 22] However, in Order P2012-02, the Adjudicator stated:

The fact that the Complainant's personal information was improperly disclosed does not automatically or necessarily mean that the Organization failed to make reasonable security arrangements to protect it. I have explained that I must determine what steps were reasonable for the Organization to take, bearing in mind all of the relevant facts and circumstances.

(Order P2012-02 at para 29)

[para 23] According to the “Host Manual” provided to me by the Organization, following an event the, “...host accesses the Fastlife Client Management System online to input the data directly and send the matches.” This involves taking data from folders that are handed in at the end of an event and inputting “yes” votes into the system and clicking on an icon to send match e-mails, which are automatically generated by the system.

[para 24] Therefore, from the information that I was provided with in the Organization's initial submission, there are two possible ways that the Complainant's e-mail could have been improperly disclosed. The first is if the host erroneously entered that the Complainant had voted "yes" to an individual that had also voted "yes" to her. It is my understanding that in order to have a match, two people have to vote "yes" to each other. Therefore, possibly the host erroneously entered that the Complainant voted "yes" to the individual to whom the Organization disclosed her e-mail. The second possible way the Complainant's e-mail was improperly disclosed was if there was a system error. The Organization submits:

There are no records of any bugs in our server logs from the period concerned so it seems that the issue was simple human error on behalf of the event facilitator...

[para 25] The Complainant submits that she did not select any matches following the event. As evidence of this, the Complainant provided me a copy of an e-mail from the Organization that she received following the speed dating event which states:

Since you didn't select any of the people you met on Thursday night you didn't match with anyone this time around.

[para 26] As I did not understand why the e-mail was sent confirming there had been no matches, yet the Complainant's e-mail was provided to the other individual as a match, I asked the Organization for a further explanation. The Organization advised that the individual to whom the Complainant's e-mail was disclosed had not registered for the event but was allowed to participate regardless. The host at the event did not have the proper authority to add the unregistered individual in the computer system. However, the host entered, correctly, that the Complainant had no matches. The confirmation of 'no matches' was sent on the basis of this information. Subsequently, all the information (including the unregistered individual's information) was sent to another employee of the Organization who had the authority to enter the unregistered individual's information. It was during the course of entering the unregistered individual's information that the unregistered individual was mistakenly matched with the Complainant, with the consequence that the Complainant's e-mail address was sent to the unregistered individual.

[para 27] I find that the disclosure in this case was an instance of human error. Based on this explanation and on the information before me, the Organization did make reasonable security arrangements. If there was evidence of more frequent errors, I might recommend that the Organization institute a system that provides for data entries to be double-checked by someone other than the person inputting the data. However, I do not have evidence that this is a widespread problem. It is not reasonable to expect an Organization to be able to protect against all human error. The Organization provided information that indicates that it trains its hosts and employees, and I have no evidence that human error is commonplace or that the Organization's disclosure of the Complainant's personal information was the result of a larger problem with the way the

Organization secures personal information in its custody. Therefore, I cannot find the Organization failed to comply with section 34 of the Act.

E. Did the Organization comply with section 6(1) of the Act by developing and following policies and practices that are reasonable for the Organization to meet its obligation under this Act?

[para 28] Section 6(1) of the Act states:

6(1) An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.

[para 29] The Organization provided me with a link to its privacy policy, which is found on its website. The policy outlines the personal information of users which will be kept confidential and for what purpose it will be used. As well, it outlines when personal information will be disclosed.

[para 30] In addition, its “Host Manual” also indicates, in two sections, the importance of keeping client information confidential. Since, this incident has occurred, the Organization now requires Hosts to acknowledge that they have read the sections of the “Host Manual” relating to privacy and understand that any failure to comply with these policies are grounds for dismissal. Though this measure was not in place at the time of the breach which is the subject of this inquiry, I acknowledge that this is a positive step taken by the Organization to ensure that its obligations under the Act are met, and one I would have recommended if it had not already been in place. However, the Organization should also ensure that all of its employees who deal with personal information are made aware of and acknowledge the Organization’s specific obligations under the Act.

[para 31] The Complainant made no submissions regarding the Organization’s privacy policy or its compliance with section 6(1) of the Act. Based on the information before me as to the policies and practices in place at the time of the breach, I find that the Organization complied with section 6(1) of the Act to some degree, but order the Organization to ensure that its employees are aware of the Organization’s obligations under the Act.

V. ORDER

[para 32] I make this Order under section 52 of the Act.

[para 33] I find that the Organization disclosed the Complainant’s personal information without the Complainant’s consent contrary to section 7 of the Act.

[para 34] I find that the Organization made reasonable security arrangements within the terms of section 34 of the Act.

[para 35] I impose the following term on the Organization:

The Organization is to ensure that it does not disclose personal information that it is not authorized to disclose by ensuring that its employees are made aware of the Organization's obligations under the Act.

[para 36] 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.

Keri H. Ridley
Adjudicator