Federal Court  Cour fédérale

Date: 20120508

Docket: T-987-11

Citation: 2012 FC 550

Ottawa, Ontario, May 8, 2012

PRESENT: The Honourable Mr. Justice de Montigny

BETWEEN:

NEIL JOSEPH TOWNSEND

Applicant

and

SUN LIFE FINANCIAL

Respondent

REASONS FOR JUDGMENT AND JUDGMENT

[1] This is an application pursuant to section 14 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [PIPEDA], in respect of a complaint made to the Office of the Privacy Commissioner of Canada (the "Office") by the Applicant on March 24, 2010. Mr. Townsend alleges that Sun Life Financial disclosed his medical information to a third party without his consent and failed to safeguard his personal information.

[2] On May 13, 2011, the Office issued a decision, concluding that "both the safeguards and use and disclosure complaints are resolved".

[3] The Applicant now seeks the following order:

(i) Payment of $352.56 for costs associated with the closing of the Investors Group retirement plans;

(ii) Declaration that the Respondent breached the PIPEDA and the fiduciary duties owed to the Applicant;

(iii) Declaration compelling the Respondent to publish notices of measures taken to avoid contravening the PIPEDA;

(iv) An award of $25,000.00 in damages;

(v) Costs before this Court; and

(vi) Any other relief this Court deems appropriate.

FACTS

[4] On July 15, 2009, the Applicant applied for Long Term Care Insurance with Sun Life Financial ("Sun Life" or the "Respondent") using the services of an advisor, registered to sell Sun Life products (the "Advisor").

[5] On July 22, 2009, Sun Life received the Applicant's completed application. On July 23, 2009, the application was logged into Sun Life's Policy Issue System for processing. This Policy Issue System generated a confirmation on the company's website for advisors (the "Advisor Site").

[6] On August 4, 2009, Sun Life forwarded Mr. Townsend's application, via secure e-mail, to a third party provider, an underwriter for Sun Life's Long Term Care Insurance applications (the "Underwriter"). The Underwriter, in turn, appointed another third party to obtain additional medical information from the Applicant and/or his physician (the "Medical Information Requester").

[7] On August 14, 2009, Sun Life generated a report on the Underwriter's secure site confirming receipt of the Applicant's medical records from the Medical Information Requester. On August 27, 2009, the Underwriter notified Sun Life by e-mail of its decision to postpone Mr. Townsend's application for Long Term Care Insurance due to a medical condition.

[8] On August 29, 2009, Sun Life's Policy Issue System generated an automated alert message to the Advisor Site indicating that the Applicant's application was outstanding. On September 3, 2009, the Policy Issue System was updated with the Underwriter's decision.

[9] On January 7, 2010, a Customer Relations Consultant at Sun Life responded to an inquiry from the Applicant. The letter contained sensitive medical information. A copy of that correspondence was sent in error to the Applicant's Advisor.

[10] On January 20, 2010, Sun Life's Privacy Office sent a letter to the Applicant informing him of the disclosure. Despite the fact that part of the number of the Applicant's address had been transposed, Canada Post delivered the correspondence to the Applicant's correct address.

[11] On February 12, 2010, Sun Life sent another letter to the Applicant containing the transposed address. That letter was returned to Sun Life. Upon verification, Sun Life re-sent the letter to the correct address on March 1, 2010.

[12] The Applicant subsequently filed a complaint with the Office alleging that the Respondent failed to safeguard his personal information and disclosed his medical information to his Advisor without his knowledge or consent.

IMPUGNED DECISION

[13] The Office first determined that the allegations made by the Applicant triggered Principles 4.3, 4.3.4, 4.6, 4.7, 4.7.1, 4.7.2 and 4.7.4 of Schedule 1 of the PIPEDA. The Office then examined the Applicant's specific allegations against Sun Life.

[14] First, the Applicant complained that Sun Life misplaced his medical information. The Office determined that Sun Life had safe custody of the Applicant's medical information at all times. The problem occurred when the Respondent's staff failed to update its Policy Issue System confirming receipt of all medical records from Mr. Townsend. This failure generated a message to its Advisor Site, which in turn informed the Applicant's Advisor that the application was awaiting "outstanding requirements". Sun Life explained that "outstanding requirements" is a generic response covering numerous possibilities, and that in this instance, it indicated that an underwriting decision had not yet been made regarding the Applicant's Long Term Care Insurance. The Office accepted Sun Life's explanation that in the summer of 2009, it added the Long Term Care Insurance product to its insurance portfolio that could be sold directly by financial advisors. As a result, the Long Term Care Insurance required the issuance of new departmental policies and required staff

members to manually update the company's systems when underwriting decisions were received. The Applicant's insurance application was one of the first processed by the Respondent under the new procedures. The Respondent confirmed that in June 2011 updates would be made automatically.

[15] In respect of its dealings with third parties – the Underwriter and the Medical Information Requester – Sun Life explained that it has contractual agreements with them providing for privacy and security measures to ensure the protection of personal information. Moreover, as a matter of practice, Sun Life informs its customers that their information may be shared with third-party service providers.

[16] The Office saw no breach of Principles 4.7 and 4.7.1. As for any temporary contravention of Principle 4.6, it has been resolved.

[17] Second, the Applicant alleges that Sun Life did not have adequate safeguards to ensure that correspondence be sent to his correct address. On this matter, Sun Life acknowledged that it sent two letters to the Applicant at a wrong address and that this mistake resulted from a human error.

[18] On this issue, the Office concluded that the first letter was, regardless of the error, delivered directly to the Applicant. As for the second letter, it was returned directly to Sun Life. As a consequence, no unauthorized disclosure resulted from the error. In addition, Sun Life took measures to remedy the situation by correcting its records. As a result, the Office believed that Sun

Life had addressed its obligations under Principles 4.6 and 4.7.4 of Schedule 1 and resolved any contravention.

[19] Third, the Applicant complained that Sun Life disclosed his medical information without his consent. In this respect, the Office determined that the letter contained sensitive personal information regarding the Applicant and should have been subject to safeguards as mandated by Principle 4.7.2. Therefore, the Office found that there was a clear contravention of Principe 4.3 of Schedule 1. The letter to the Applicant containing medical information should only have been disclosed to parties with a need to know such information, after obtaining the Applicant's consent. Sun Life therefore failed to comply with its own procedures.

[20] Nevertheless, the Office accepted Sun Life's explanations that procedures were reviewed with the employee responsible for the disclosure. Additionally, Sun Life had contacted the Applicant's Advisor to ensure that the letter had been destroyed. Furthermore, the Office acknowledged that Sun Life had updated its client letter templates by adding pop-up messages to remind consultants to carefully review whether the client's advisor should receive a copy of the correspondence being prepared.

[21] In summary, the Office concluded that Sun Life had resolved any issue pertaining to safeguards, use and disclosure.

ISSUES

[22] This application raises the following issues:

(a) Did the Respondent breach the provisions of the PIPEDA by misplacing the Applicant's medical information?

(b) Did the Respondent breach the provisions of the PIPEDA by sending a copy of the January 7, 2010 letter to the Applicant's Advisor?

(c) Did the Respondent breach the provisions of the PIPEDA by addressing letters to the Applicant using an incorrect address?

(d) If the Respondent breached the provisions of the PIPEDA, did the Applicant suffer any damages?

ANALYSIS

[23] The parties made no submissions with respect to the applicable standard of review. Nevertheless, my colleague Justice Mosley accurately set it out in *Randall v Nubodys Fitness Centres*, 2010 FC 681, 371 FTR 180 [*Randall*] wherein he stated that an application under section 14 of the PIPEDA is not a judicial review of the Commissioner's decision. In fact, it is a *de novo* review of the conduct of the party against whom the complaint was made (*Randall*, above at paras 32-33). Accordingly, if this Court finds that the Respondent violated the provisions of the PIPEDA, it must then consider the remedies available to the Applicant (*Randall*, above at para 35).

(a) Did the Respondent breach the provisions of the PIPEDA by misplacing the Applicant's medical information?

[24] There is no indication that Mr. Townsend's medical information had ever been misplaced. The Respondent explained that the generic, automated message to Mr. Townsend and his Advisor indicating that Sun Life was still awaiting requirements, did not mean that any of Mr. Townsend's

medical information had been misplaced. It may be, as the Respondent acknowledged, that its staff failed to update the Policy Issue System confirming receipt of the medical information requested. However, that does not amount to a breach of the Applicant's privacy. Indeed, Mr. Townsend appeared to accept, both at the hearing and in his July 20, 2011 affidavit, that his medical information was safeguarded and not misplaced. Accordingly, this is no longer an issue.

(b) Did the Respondent breach the provisions of the PIPEDA by sending a copy of the January 7, 2010 letter to the Applicant's Advisor?

[25] Principle 4.3 of Schedule 1 provides that the knowledge and consent of the customer is required prior to disclosing personal information. Furthermore, Principle 4.3.4 makes it clear that medical information is almost always considered to be sensitive, calling for a rather more explicit form of consent.

[26] In the case at bar, Sun Life readily acknowledges a contravention of Principle 4.3 in copying its January 7, 2010 letter to Mr. Townsend's Advisor.

[27] That being said, I accept the Respondent's submission that, but for the fact that the letter contained personal medical information, the copying of the letter to the Advisor was understandable. It would be in Mr. Townsend's interests for his Advisor to know that Sun Life's consideration of the application was merely being postponed. Copying the letter to the Advisor would therefore have been acceptable had the one sentence about Mr. Townsend's medical condition been deleted.

(c) Did the Respondent breach the provisions of the PIPEDA by addressing letters to the Applicant using an incorrect address?

[28] Sun Life acknowledges that it sent two letters to the Applicant at the wrong address as a result of an inadvertent mistake. A number was transposed in the Applicant's address due to human error. This is clearly a breach of Principle 4.6 of the Schedule 1, which states that the personal information gathered must be accurate.

[29] That being said, this minor breach was of no consequence in the case at bar. The January 20, 2010 letter was delivered by Canada Post to Mr. Townsend at his correct address. The February 12, 2010 letter was returned to Sun Life, unopened, by Canada Post. As a result, no unauthorized disclosure actually resulted from the error.

(d) If the Respondent breached the provisions of the PIPEDA, did the Applicant suffer any damages?

[30] Section 16 of the PIPEDA gives discretion to the Court to grant remedies, including damages for humiliation. In *Randall*, above, Justice Mosley expressed the view that an award for damages should not be made lightly, but only in the most egregious of circumstances (at para 55).

[31] There is very little jurisprudence with respect to the determination of damages for breach of privacy, particularly in the context of PIPEDA. One of the most comprehensive reviews of this matter is to be found in *Nammo v TransUnion of Canada Inc*, 2010 FC 1284, 379 FTR 130 [*Nammo*]where my colleague Justice Zinn provided some helpful guidelines. Referring to the

decision of the Supreme Court in *Vancouver (City) v Ward*, 2010 SCC 27, [2010] 2 SCR 28, Justice Zinn mentioned three rationales for awarding damages: compensation, deterrence and vindication. He then listed a number of non-exhaustive factors for determining whether damages should be awarded and the quantum of such damages:

> (i) Whether awarding damages would further the general objects of PIPEDA and uphold the values it embodies;
>
> (ii) Whether damages should be awarded for deterring future breaches; and
>
> (iii) The seriousness or egregiousness of the breach.
>
> (*Nammo*, above at para 76)

[32] In turn, the seriousness or egregiousness of the breach can be assessed by way of the following considerations:

> (i) The impact of the breach on the health, welfare, social, business or financial position of the applicant;
>
> (ii) The conduct of the respondent before and after the breach; and
>
> (iii) Whether the respondent benefited from the breach.
>
> (*Randall*, above at para 47).

[33] In the case at bar, the Applicant alleges damages in the amount of $25,000.00. However, apart from the Applicant's assertions, he has not provided any evidence or detailed the humiliation suffered as a result of the Respondent's conduct.

[34] In fact, contrary to the Applicant's bald assertions, I do not accept that the Respondent has acted in an intentional, callous or egregious manner or in any other way that would indicate a complete disregard for the Applicant's privacy interests. The fact that the Respondent has never denied having committed the errors is commendable. Plus, there is no evidence that the Respondent acted in bad faith or benefited commercially from the error, as acknowledged by the Applicant. It is also duly noted that the Respondent has apologized to the Applicant on numerous occasions (Respondent's Record, Affidavit of Rosemary Knez, Exhibit "B", p 8; Exhibit "D", pp 11-12; Exhibit "F", p 14) and even informed the Applicant of the measures implemented to avoid the re-occurrence of such errors (*Ibid*, Exhibit "D", p 11). In my opinion, the Respondent promptly and effectively corrected its errors. It may be, as alleged by the Applicant, that the Respondent should have put these measures in place before the error occurred. Nobody should be held to a standard of perfection, and the Respondent already had a detailed protocol before the occurrence of what can only be considered as a human error.

[35] Moreover, the amount of damages sought is greatly out of proportion to the jurisprudence of this Court. Even in cases where the Court has found evidence of bad faith on the part of a respondent, the quantum of damages has been lesser than the order sought by the applicant.

[36] For example, in *Nammo*, above, Justice Zinn found that the respondent had breached the provisions of the PIPEDA by providing inaccurate financial information to the Royal Bank of Canada, which resulted in the applicant's loan application being denied. In addition, the respondent failed to promptly correct its error and acted in bad faith in failing to take responsibility for the error. In that situation, the Court only awarded damages in the amount of $5,000.00.

[37] In *Landry v Royal Bank of Canada*, 2011 FC 687 at para 32, 391 FTR 153, the Court solely awarded damages in the amount of $4,500.00 for what it found to be a "serious breach committed by the respondent's employee and its subsequent cover-up".

[38] Taking into consideration the facts of this case, I am of the view that the disclosure of personal information was minimal and the inaccuracy in the Applicant's address caused no injury. I accept that medical information is of the utmost sensitivity and should receive the highest degree of protection. In the instant case, and without diminishing the Applicant's grief, the extent of the disclosure was minimal and was only disclosed to Mr. Townsend's Advisor, who appeared not to have noticed the personal information and then promptly destroyed the letter upon request. Moreover, the Respondent genuinely apologized for the breach and promptly took steps to correct its policies and procedures. For those reasons, I do not consider it necessary to order the Respondent to correct its practices or to publish a notice of any action taken or proposed to be taken to correct its practices, or to award damages to the Applicant.

[39] Moreover, the Applicant has not provided any arguments or evidence for disbursing $352.56 for costs, associated with the closing of the Investors Group retirement plans. In any event, I see no plain and obvious link between these costs and the Respondent's conduct. Accordingly, the Court exercises its discretion not to award these costs.

[40] For all of the foregoing reasons, this application is dismissed and each party shall bear its own costs.

JUDGMENT

THIS COURT'S JUDGMENT is that this application is dismissed. The parties shall bear their own costs.

"Yves de Montigny"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-987-11
STYLE OF CAUSE:	NEIL TOWNSEND v SUN LIFE FINANCIAL
PLACE OF HEARING:	Regina, SK
DATE OF HEARING:	December 15, 2011
REASONS FOR JUDGMENT AND JUDGMENT:	de MONTIGNY J.
DATED:	May 8, 2012

APPEARANCES:

Neil Townsend	FOR THE APPLICANT (ON HIS OWN BEHALF)
Paul Harasen	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Neil Townsend Regina, SK	FOR THE APPLICANT (ON HIS OWN BEHALF)
Kanuka Thuringer LLP Regina, SK	FOR THE RESPONDENT