CITATION: *Bannister v. Canadian Imperial Bank of Commerce*, 2021 ONSC 2927
COURT FILE NO.: CV-18-76456-00CP
DATE: 20210420

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:	
JEFFREY BANNISTER Plaintiff	Jean-Marc Leclerc and Carsten Jensen and Michael G. Robb, for the Plaintiffs
– and –	
CANADIAN IMPERIAL BANK OF COMMERCE Defendant	Linda Plumpton, Molly M. Reynolds and Shalom Cumbo-Steinmetz, for the Defendant
	HEARD: April 6, 2021

REASONS FOR DECISION ON SETTLEMENT APPROVAL AND DISTRIBUTION PROTOCOL

R. SMITH J.

[1] The parties in both the Canadian Imperial Bank of Commerce ("CIBC") and the Bank of Montreal ("BMO") actions have brought this motion to approve the settlements reached in May 2018. Simplii Financial ("Simplii") is an online consumer brand operated by the CIBC.

[2] The actions arise out of data breaches at BMO, which affected 113,151 clients and the Simplii data breach, which affected 10,101 clients. The parties have agreed to settle the BMO action for $21,223,075.00 and the CIBC action for $1,769,425.00. The parties seek approval of the Settlement Agreement and the protocols to distribute the funds.

Factual Background

As the facts are not contested, I have adopted them from the parties' factum.

[3] On May 28, 2018, BMO and CIBC each issued press releases to announce that a data breach had occurred involving client information. As described in the press releases, hackers had breached the banks' IT systems and demanded ransom payments, failing which the hackers said they would publish client information on the Internet.

[4] Following the incidents, numerous media organizations reported on the data breach. For example, a CBC news article dated May 29, 2018 explained that hackers had shared identifying information about two bank clients, to back up the veracity of their claims. CBC contacted the individuals, who confirmed they were indeed bank clients and described their dismay.

[5] The CBC article also described "a list circulating online containing personal information of 100 BMO customers, which included extensive personal information about them, including names, addresses, phone numbers, account numbers, birth dates and Social Insurance Numbers. CBC News reached out to a number of those individuals, many of whom confirmed the accuracy of the information."

[6] The representative plaintiff in the BMO Action, Melissa Mallette, was among the 100 BMO customers whose personal information was posted online.

[7] The banks' responding certification motion materials described their efforts to notify and compensate customers following the breach.

[8] BMO contacted its customers following the May 28 press release. It issued a customer update on Facebook, in which it stated that the bank would be contacting impacted customers to offer complementary credit monitoring, replace debit or bank cards, reset password and determine the nature of any financial impact. In addition, BMO sent letters to impacted customers to advise them of the data breach.

[9] For some 62,945 BMO clients whose personal information including SIN was accessed, BMO engaged its branch managers across the country to telephone affected customers.

[10] Simplii posted to its Facebook account on May 28, 2018, stating in part: “We take this matter seriously and will be reaching out individually to clients who may be impacted. Updated information will be posted here as it becomes available.”

[11] CIBC sent an e-mail to its customers and began contacting affected individuals by phone on May 30, 2018, three days after the ransom note was received. Ultimately, all individuals were contacted by telephone throughout the month of June until everyone was reached (other than six individuals whose accounts were inactive). Between June 4 and 11, 2018, CIBC couriered letters to all affected individuals, advising them that any money stolen from their accounts would be reimbursed and that they were eligible for free credit monitoring and identity theft insurance.

[12] BMO offered affected customers two years of credit monitoring and identity protection services. BMO advised that after 13 months of offering free credit monitoring, a total of 16,986 affected customers had signed up, and that it had spent approximately $5.45 million on credit monitoring and identity protection services. In addition, BMO reissued and delivered new bank cards for all affected customers.

[13] BMO also committed in its letters to customers to reimbursing them for any financial impact from unauthorized transactions occurring through BMO Online and Mobile Banking. As of July 18, 2019, BMO advised that it had reimbursed customers for over $6.85 million in fraudulent electronic money transfers.

[14] CIBC offered all affected clients two years of free credit monitoring and identity theft insurance from Equifax. As of July 2019, 2,231 affected clients accepted the offer.

[15] CIBC also offered affected customer households a $100 Visa gift card, “as a token of appreciation for time and potential inconvenience associated with the attack.” In total, CIBC distributed 8,743 Visa gift cards to affected customer households, representing a total amount of $874,300.

[16] CIBC advised that the hackers attempted to make electronic money transfers out of affected customers’ accounts. Approximately 12% of affected clients had money stolen from their accounts. CIBC reimbursed Simplii clients for these amounts, totalling $1,786,517, and

established an ongoing process to reimburse affected clients for any additional funds subsequently stolen as a result of the incident.

[17] In addition to the cases initially commenced by Sotos LLP, JSS Barristers and Siskinds LLP investigated and commenced separate claims against BMO and CIBC. These claims, called *Wilson* and *Steinman*, were issued in Ontario on June 15, 2018.

[18] On September 26, 2018, Siskinds Desmeules s.e.n.c.r.l. commenced an action against BMO in the Quebec Court on behalf of Quebec residents. Siskinds Desmeules represents the proposed class of Quebec residents in the BMO class action.

[19] Sotos LLP, Siskinds LLP and JSS Barristers ultimately agreed to enter into a co-counsel agreement to jointly advance the cases. Counsel agreed to amend the proposed class proceedings started by Sotos LLP in Ottawa and to proceed with those actions, while staying the balance of cases started in Ontario. On February 14, 2019, the Quebec Court stayed the Quebec case pending the outcome of the Ontario BMO action.

[20] In conjunction with the commencement of the actionss, Class Counsel were contacted by numerous class members. Some class members simply sought to register their contact information with counsel, while others sought more detailed information about the claim and sought information about how to best protect themselves in light of the data breach. A total of 1,767 class members across Canada registered their contact information with Class Counsel to obtain more information about the cases.

[21] The plaintiffs' certification motion record contained an expert report prepared by Dr. Eric Cole, an expert in cybersecurity. Because the precise nature of the breach had not been disclosed by the defendants, counsel determined that it would be prudent to engage Dr. Cole for the purposes of the certification motion to explain that there are industry standards and best practices for the protection and safeguarding of electronically stored personal information. Dr. Cole's report discussed these standards and explained that he could use reliable methods to assess the nature and extent of a cybersecurity breach. His report also described the type of information that would be required to determine the nature and extent of the alleged security breach, and whether he expected the banks to have retained those records.

[22] BMO's materials indicated that "the Personal Information accessed by the Criminal Attackers included, depending on the affected customer, one or more of the customer's name, mailing address, email address, phone number, date of birth ("DoB"), Social Insurance Number ("SIN"), bank card and account numbers, transaction information, employment, and security questions and answers." BMO also categorized impacted customers into three groups, as follows:

Group	Number of customers	Type of information accessed
1	3,190	Personal Information including DoB and SIN was accessed and posted online.
2	59,755	Personal Information including DoB and SIN was accessed.
3	50,209	Personal Information was accessed, not including DoB and SIN.

[23] CIBC's record explained that while the hackers stated that they had accessed the information of some 40,000 Simplii clients, CIBC's subsequent investigation confirmed that "the total number of affected clients was 10,111." CIBC's record explained that impacted customers fell into one of two categories:

(a) For 7,023 clients, "the hackers would have been able to access a customer's account numbers, balances, transaction history, information about any payees the accountholder had set up for bill payments or electronic transfers, and basic identifying information such as name and address."

(b) For 3,088 clients, "the hackers could have seen one or several of three additional pieces of identifying information: (i) Social Insurance Number, (ii) date of birth and (iii) employment information, if Simplii had it on file (this could have included some or all of: employer name and contact information, length of employment, occupation, industry, job title, and employee number)." Affected clients who fell within this category "were specifically notified and told what information may have been compromised."

[24] The defendants' responding records also contained reports from two experts, Julia Ferguson and Christopher Sears.

[25] Ms. Ferguson's was described as an expert in fraud prevention, identity theft and data breach response in the financial services sector. Her report addressed a number of questions, including the following:

(a) Assuming that the material facts pleaded in the Amended Statements of Claim are true, what is your risk assessment for the affected bank customers as to an economic loss? The risk of economic loss to affected bank customers should be low, and in any event will vary from customer to customer based on their own personal characteristics.

[26] Dr. Sears is a professor of psychology at the University of Calgary. He prepared a report for the defendants' responding certification motion record, entitled "Psychological Reactions to Data Breach Events." The report addressed the following questions: "(1) whether individuals typically have the same or comparable psychological reactions when they are notified that they are affected by a data breach […] and (2) whether all individuals whose personal information is exposed as a result of a data breach are likely to suffer clinically significant psychological distress." Dr. Sears concluded as follows:

(a) There is a great deal of variation in how people react to data breach events and there is no evidence of a universally negative reaction to such events; and

(b) In light of the variation in people's reactions, it is unlikely that all the individuals whose personal information was exposed a result of the data breach will suffer clinically significant psychological distress.

[27] The parties reached agreement in principle in October 2019. In conjunction with this, the parties also negotiated and finalized the notices of certification and proposed distribution protocols.

[28] The parties attended before the Ontario Superior Court of Justice in Ottawa via telephone conference on October 7, 2020 to seek consent certification and notice approval orders. In conjunction with the motions, both representative plaintiffs swore affidavits, in which they stated

that they agreed with the proposed settlement agreement and believed that its terms were fair, reasonable and in the best interests of the class. On October 7, 2020, the Court certified the actions for settlement purposes and approved the proposed notices in each action.

[29] Approval for the BMO settlement agreement was also obtained from the Quebec court. At the Quebec hearing, Justice Chatelain requested several changes to the draft settlement agreement which resulted in an addendum to the BMO agreement, dated December 14, 2020. The addendum clarifies that the distribution process is subject to supervision of both the Ontario Court and the Quebec Court. In addition, changes were made to certain deadlines specified in the distribution protocol.

[30] Consistent with the notice approval orders, class members were given notice of the proposed settlement approval, distribution protocol and fee approval hearings in Ontario and Quebec.

[31] The primary method of notification involved the banks sending e-mails and/or letters to their customers:

(a) On or about December 11, 2020, Epiq (the Court-appointed claims administrator) sent out notice by regular mail to 113,028 Class Members whose addresses BMO had on file. The letters advised Class Members the settlement group in which the class member was determined to fall within. BMO calculates that there was a 94.5% assumed receipt rate, with roughly 5.5% of the notices returned undeliverable.

(b) On December 15, 2020, Simplii sent 10,101 copies of the notice as follows: 9,627 via email; and 474 letters by courier.

[32] The deadline for opting out of these actions was February 15, 2021. Counsel received 94 opt-out requests in the BMO Action and 3 opt-out requests in the CIBC Action. In addition, Class Counsel received eleven objections from BMO class members.

[33] As described above, the BMO data breach impacted personal information of some 113,151 BMO clients. The proposed settlement contemplates the resolution of those claims (subject to optouts) for a potential aggregate amount of $21,223,075.

[34] The Simplii data breach impacted personal information of some 10,101 clients. The proposed settlement contemplates the resolution of those claims (subject to opt-outs) for a potential aggregate amount of $1,769,425.

[35] Both settlements contemplate categorizing class members into different groups, depending on the nature of the personal information exposed in the breach. Different levels of compensation are proposed to different group members. For example, in the case of the BMO Settlement Agreement, for persons who had their personal information posted online, they are to be paid $1000 (subject to Class Counsel fees, disbursements, interest and taxes). The settlement amounts paid to the different group members are intended to reflect notional compensation at $18 per hour for inconvenience and for time spent to address issues arising from the breach.

[36] In both settlements, larger amounts are proposed for persons who had their SIN and date of birth information compromised, compared to class members who did not. This distinction is warranted because SIN information is particularly sensitive information that can be used to obtain further personal information to invade privacy.

[37] However, the net settlement amount relating to BMO fixed funds is estimated to be $9,041,116.55. The net settlement amount relating to the CIBC Settlement Agreement is estimated to be $1,158,041.48.

BMO class members

Claimant Group	Settlement funds – fixed per claimant	Estimated net fixed settlement payments per class member	Settlement Funds – Claimant per Claimant	Estimated net claimable settlement payments per class member
Group 1 (3,195 class members whose personal information, including DOB and SIN, were posted online)	$1,000 in two parts: i. compensation for the first 20 hours spent at $18/hr; and ii. a $640 amount for inconvenience.	$701.86	Up to 3.5 additional hours at $18/hr for persons who certify they spent in excess of 20 hours addressing issues arising from the Data Breach.	$45.10
Group 2 (59,750 class members whose DOB and SIN were accessed)	$144: compensation the first 8 hours spent at $18/hr.	$101.07	Up to 3.5 additional hours at $18/hr for those who certify they spent in excess of 8 hours addressing issues arising from the Data Breach.	$45.10
Group 3 (50,206 class members whose personal information was accessed, not including DOB and SIN)	Nil – only claimable funds are allowed	NIL	Up to 5 hours at $18/hr for those who certify they spent time addressing issues arising from the Data Breach.	$64.43
Group 4 (3,566 members of Groups 1, 2 or 3 who also had unauthorized transactions recorded in their accounts, which were reimbursed in full by BMO)	$270: compensation for 15 hours spent at $18/hr.	$189.50		-
Total	**$12,757,540.00**		**$8,465,535.00**	

Simplii class members

Claimant Group	Settlement Funds – Fixed per Claimant	Estimated settlement payments per class member, net of legal fees, taxes and disbursements
Group 1 (3,027 class members who had SIN information accessed)	$192.80 (compensation for approximately 12.5 hours spent at $18/hr)	$135.52
Group 2 (7,074 class members who did not have SIN information accessed)	$120.50 (compensation for approximately 6.5 hours spent at $18/hr)	$84.70
Group 3 (1,797 members of Group 1 or 2 who had an unauthorized transaction recorded in their account, all of which have been reimbursed by CIBC)	$185.50 (compensation for approximately 10 hours spent at $18/hr)	$129.62
Total	**$1,769,425.00**	

Analysis

[38] In *Mancinelli v. Royal Bank of Canada*, 2016 ONSC 6953 at para. 31, the court stated that on a settlement approval motion, "the court, without making findings of fact on the merits of the litigation, must examine the fairness and reasonableness of the proposed settlement and whether it is in the best interests of the class as a whole having regard to the claims and defences in the litigation and any objections raised to the settlement."

[39] In *Mancinelli* at para. 32 the court held that a settlement must fall within a zone of reasonableness. "Reasonableness allows for a range of possible resolutions and is an objective standard that allows for variation depending upon the subject-matter of the litigation and the nature of the damages for which the settlement is to provide compensation."

[40] In *Mancinelli* at para. 30 the court stated the following factors were relevant in determining whether a settlement is in the best interests of the class:

(a) the likelihood of recovery or likelihood of success;

(b) the amount and nature of discovery, evidence or investigation;

(c) the proposed settlement terms and conditions;

(d) the recommendation and experience of counsel;

(e) the future expense and likely duration of the litigation;

(f) the number of objectors and nature of objections;

(g) the presence of good faith, arm's-length bargaining and the absence of collusion;

(h) the information conveying to the court the dynamics of, and the positions taken by, the parties during the negotiations; and

(i) the nature of communications by counsel and the representative plaintiff with class members during the litigation.

[41] In these class proceedings there is some risk of success to the class. In *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315 Perell J. held that the disclosure of merely "contact information" like a person's name, address and telephone number did not qualify as information in which class members would subjectively or objectively have an expectation of privacy.

[42] In *Kaplan v. Casino Rama*, 2019 ONSC 2025, Belobaba J. refused to certify an action where a hacker stole the personal information of the defendant's employees, customers and suppliers. The personal information included one or more of name, address, date of birth, SIN bank account details and photo. The court held that after 2 ½ years, there was no evidence that anyone had experienced fraud or identity theft as a result of the cyber attack. In the case before me, money was taken from bank accounts, but the banks have replaced all money stolen.

[43] The issue of whether a third-party hacker intrusion qualifies for the tort of intrusion upon seclusion, which requires intentional or reckless conduct by the defendant remains an outstanding issue.

[44] In *Condon v. Canada*, 2018 FC 522 at para. 26 the Federal Court held that the quantum of damages in breach of privacy litigation was uncertain. I agree with this assessment.

Objections

[45] A number of the BMO class members objected to the group to which they were assigned, stating that they should have been in Group 4 because they believed there were unauthorized transactions in their accounts. I accept the statement by BMO that they have diligently and in good faith investigated the assignment to the correct group into which each claimant fell.

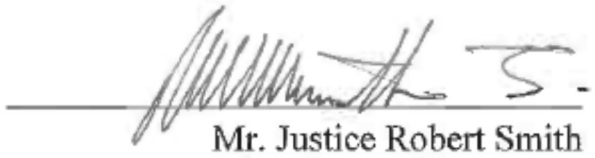
[46] Some class members also expressed concern that their personal information would be posted online in the future. This risk remains a possibility, but it is mitigated because the police have made arrests of accused persons in Canada regarding these data breaches. In addition, the Banks have offered free credit monitoring services for 2 years and relatively few customers took up the offer, approximately 22% for both CIBC and the BMO customers. The vast majority of class members (99% for BMO) have not expressed any concern about the proposed settlement.

[47] Considering the objections, I find that the amount of the settlement and the amounts already paid to class members that the settlement is a reasonable compromise and is in the best interests of the class.

[48] The proposed settlements compare favourably with those in *Lozanski v. Home Depot*, 2016 ONSC 5447 which involved a hacker breach of e-mail addresses and where possibly credit card numbers of 58,605 customers were stolen. A fund of $250,000 was created to compensate customers with documented losses up to $5,000. Class members were allowed to claim up to 5 hours at $15.00 per hour to a maximum of $75.00 for time spent remedying the breach. This settlement adopts this approach to compensation using a rate of $18.00 per hour up to a maximum number of hours.

Disposition of Approval of Settlements and Distribution Protocols

[49] Based on the evidence provided as summarized above, I am satisfied that the proposed settlement agreement is fair, reasonable and in the best interest of the class, and as such it is approved. I also approve the proposed distribution protocol.



Mr. Justice Robert Smith

Released: April 20, 2021

CITATION: *Bannister v. Canadian Imperial Bank of Commerce*, 2021 ONSC 2927
COURT FILE NO.: CV-18-76456-00CP
DATE: 20210420

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:

JEFFREY BANNISTER

Plaintiff

– AND –

CANADIAN IMPERIAL BANK OF COMMERCE

Defendant

REASONS FOR JUDGMENT

R. Smith J.

Released: April 20, 2021