Form 4.02A

2020 Hfx No. 500912

SUPREME COURT OF NOVA SCOTIA

Between:

CHRISTOPHER PURVIS

PLAINTIFF

- AND -

DELL USA L.P., a body corporate, and **DELL CANADA INC.**, a body corporate

DEFENDANTS

Proceeding under the *Class Proceedings Act*, S.N.S. 2007, c. 28

SECOND FRESH AS AMENDED NOTICE OF ACTION

TO: **Dell USA L.P.**
211 E. 7th Street, Suite 620
Austin, Texas 78701
United States of America

AND TO: **Dell Canada Inc.**
155 Gordon Baker Road, Suite 501
North York, ON M2H 3N5

Action has been started against you
The plaintiff takes action against you.

The plaintiff started the action by filing this notice with the court on the date certified by the prothonotary.

The plaintiff claims the relief described in the attached statement of claim. The claim is based on the grounds stated in the statement of claim.

Deadline for defending the action
To defend the action, you or your counsel must file a notice of defence with the court no more than the following number of days after the day this notice of action is delivered to you:

- 15 days if delivery is made in Nova Scotia
- 30 days if delivery is made elsewhere in Canada
- 45 days if delivery is made anywhere else.

Judgment against you if you do not defend
The court may grant an order for the relief claimed without further notice, unless you file the notice of defence before the deadline.

You may demand notice of steps in the action
If you do not have a defence to the claim or you do not choose to defend it you may, if you wish to have further notice, file a demand for notice.

If you file a demand for notice, the plaintiff must notify you before obtaining an order for the relief claimed and, unless the court orders otherwise, you will be entitled to notice of each other step in the action.

Rule 57 - Action for Damages Under $150,000
Civil Procedure Rule 57 limits pretrial and trial procedures in a defended action so it will be more economical. The Rule applies if the plaintiff states the action is within the Rule. Otherwise, the Rule does not apply, except as a possible basis for costs against the plaintiff.

This action is not within Rule 57.

Filing and delivering documents
Any documents you file with the court must be filed at the office of the Prothonotary, 1815 Upper Water Street, Halifax, Nova Scotia (telephone # 902-424-4900).

When you file a document you must immediately deliver a copy of it to each other party entitled to notice, unless the document is part of an *ex parte* motion, the parties agree delivery is not required, or a judge orders it is not required.

Contact information
The plaintiff designates the following address:

Wagners
1869 Upper Water Street
Suite PH301, Historic Properties
Halifax, NS B3J 1S9

Documents delivered to this address are considered received by the plaintiff on delivery.

Further contact information is available from the prothonotary.

Proposed place of trial
The plaintiff proposes that, if you defend this action, the trial will be held in Halifax, Nova Scotia.

Signature
Signed October 6th, 2021.

Raymond F. Wagner, Q.C.
Counsel for the Plaintiff

Prothonotary's certificate

I certify that this second amended notice of action, including the attached second amended statement of claim, was filed with the court on October 7, 2021.

Prothonotary

Joseph Parks
Deputy Prothonotary

Form 4.02B

SECOND FRESH AS AMENDED STATEMENT OF CLAIM

Proceeding under the *Class Proceedings Act*, S.N.S. 2007, c. 28

I. DEFINITIONS

1. The capitalized terms used in the Second Amended Statement of Claim have the meanings and refer to the definitions indicated below:

   a. "**Class**" and "**Class Members**" is comprised of the following subclasses:

      i. **June 2017 Breach Subclass**: all persons residing in Canada who provided their Personal Information to the Defendants or any of their affiliates or subsidiaries when purchasing the Defendants' products or speaking with the Defendants' customer service or tech support between January 2008 and June of 2017, and who have received Targeted Tech Support Scam calls, emails or other correspondence pertaining to their Dell product or service in or after June 2017, but excluding members of the November 2017 Breach Subclass.

      ii. **November 2017 Breach Subclass**: all persons residing in Canada whose Personal Information and Private Customer Information was determined by the Defendants to have been breached in November 2017.

   b. "**Personal Information**" means information about an identifiable individual, including but not limited to name, address, email address, telephone numbers, credit card numbers, social insurance number, and private correspondence.

   c. "**Private Customer Information**" means information generated by the Defendants or any of their affiliates or subsidiaries arising from interactions with customers, including but not limited to non-public information about Dell product model numbers, service tags, express service codes, prior product service histories and interactions, and warranty information.

   d. "**Provider**" means the third-party company located in India that the Defendants contracted with to carry out technical support services on their behalf, as their agent, and in furtherance of their enterprise, and to whom the Defendants provided unmonitored access to the Personal Information and Private Customer Information.

   e. "**Targeted Tech Support Scams**" refer to scenarios where scammers have both Personal Information and Private Customer Information and use this information to convince their

target that they represent a trusted company, thereby facilitating solicitation of money or information. The use of both Personal Information and Private Customer Information increases the effectiveness of the scam and likelihood that the victim will fall prey to it.

II. OVERVIEW

2. An individual's privacy interest is a fundamental value that warrants protection. Information collected, created and stored by a technology and security company is inherently private in nature. Individuals have a reasonable expectation of privacy in their Personal Information and Private Customer Information. The combination of Personal Information and Private Customer Information is not publicly available, and customers do not expect such information to be known by individuals or entities other than the trusted company to whom they provided such information.

3. The Defendants utilized the Provider to deliver support to customers from a call centre located in India – an area known to be prolific for tech support scams. The Defendants remained responsible for the information transferred to the Provider and were obligated to ensure the Personal Information and Private Customer Information were protected with sufficient safeguards appropriate to the sensitivity of the information.

4. Yet, due to the Defendants' negligence and inadequate safeguards, in June and November of 2017, two employees of the Provider inappropriately exfiltrated, breached and disclosed the Plaintiff's and Class Members' Personal Information and Private Customer Information, causing *inter alia* harm, damages, significant inconvenience, lost time, and exposure to a real and substantial increased risk of identity theft, cybercrime, and phishing scams, including Targeted Tech Support Scams.

5. This invasion of privacy was highly offensive to the Plaintiff and Class Members, and to any reasonable person, due to:

   (i) the identity of the Defendants as leaders in the technology and security industry;

   (ii) the Defendants' knowledge of the risks of Targeted Tech Support Scams;

   (iii) the nature of the Personal Information and Private Customer Information breached, which in combination greatly increases the risk and effectiveness of successful scams;

   (iv) the Defendants' negligence in choosing to employ inadequate safeguards to protect their customers' information; and

   (v) the resultant breach and sale of the Personal Information and Private Customer Information to cybercriminals.

6. In July 2020, the Office of the Privacy Commissioner of Canada (the "OPC") issued a report arising out of its investigation into the Defendants' privacy breaches in June and November 2017. The OPC found that the information transferred to the Provider was sufficiently sensitive to require a high degree of protection having regard to the nature of the personal information involved, the risk environment and the potential harm to individuals in the event of a breach. The OPC investigation concluded that the Defendants' safeguards relating to controlling access to the information, logging and monitoring, and technical controls were insufficient. It further determined that the Defendants failed to adequately investigate the June 2017 breach, and that the Defendants failed to adequately respond to customer complaints of a suspected privacy breach.

7. The Plaintiff, Christopher Purvis, is a victim of this breach of privacy. He brings this action on behalf of himself and members of the Class seeking redress for the Defendants' negligence and their highly offensive invasion of privacy.

III. THE PARTIES

a. The Plaintiff

8. The Plaintiff, Christopher Purvis, currently resides at 32 Carol Avenue, Fredericton, New Brunswick.

9. Mr. Purvis purchased a Dell computer in early 2016, using his work address and work contact information for the order.

10. Since his purchase, Mr. Purvis has contacted Dell technology support for assistance with his computer. As a result of these interactions, the Defendants created and stored Mr. Purvis' Private Customer Information including his customer service history, warranty information and model numbers, along with his Personal Information.

11. In January 2018, Mr. Purvis began to receive a number of harassing calls from individuals claiming to be Dell employees, reinforced by their having Personal Information and Private Customer Information only accessible to Dell employees, including his name, phone number, computer service tag number and precise details of previous service interactions with Dell.

12. Mr. Purvis is a computer tech and almost fell prey to the scam based on the extent of information the callers had about him. However, he contacted the Defendants to warn about a potential breach of private information leading to the Targeted Tech Support Scam. The Dell customer support

centre – the same centre from which the breach occurred – declined to address the issue, even when Mr. Purvis requested to escalate the matter.

13. Mr. Purvis then contacted Dell's Privacy Mailbox about the Targeted Tech Support Scam, where he was provided with a standard response. Mr. Purvis requested Dell to escalate this inquiry, but the Defendants again denied and ignored the requested investigation.

14. Mr. Purvis conducted research online, which indicated that many other individuals had complained about receiving similar fraudulent phone calls from purported Dell employees.

15. Without any action, investigation, or response from the Defendants, in February 2018, Mr. Purvis filed a complaint with the OPC. The OPC began an investigation into Mr. Purvis' allegations of a suspected Dell privacy breach, ultimately issuing a report on July 9, 2020, confirming the breach and finding the complaint well-founded. The report also described another victim's experience, who was convinced the Targeted Tech Support Scam was legitimate based on all the information the scammer had about her, and thus provided remote access to her computer and paid $100 to the scammer, who installed malicious software.

16. In April 2018, Mr. Purvis received an email from Dell, also sent to approximately 7,883 Class Members whose privacy was found in November 2017 to have been breached. The email stated that Dell "had determined that scammers claiming to work for Dell have some basic information related to your Dell service history (such as customer name, email address, Dell product information, Dell service tag or Dell support history)." There was no express mention of the privacy breaches that took place in June and November of 2017, known at that time to the Defendants.

17. The Defendants have confirmed that the Plaintiff's Personal Information and Private Customer Information were exfiltrated in the November 2017 Breach, described below.

18. From January 2018 to early 2020, Mr. Purvis received five to ten scam calls per day, seven days a week, at all hours. The calls came from numerous phone numbers, some were 1-800 numbers and others had personal names such as "John Peterson," preventing Mr. Purvis to block numbers and stop the calls. The harassing calls were constant and relentless. As the calls were made to his work phone number, Mr. Purvis could not simply ignore them. The calls would wake Mr. Purvis from sleep, and constantly interrupt his life. Mr. Purvis was eventually left with no option but to change his work phone number used by countless clients, work contacts and employers.

19. After changing his phone number, Mr. Purvis began to receive numerous Targeted Tech Scam emails per day, claiming to be from Dell and requesting him to urgently call a number to resolve a

Dell computer issue. Mr. Purvis has had this email account for over ten years, used for personal and family contacts, business matters, and records of online interactions. Mr. Purvis' personal email is now available to at least one group of scammers, increasing the risk of additional scams, his Personal Information being sold to other scammers, cybercrime or identity theft entities.

20. During the period when Mr. Purvis received Tech Support Scam Calls on a daily basis, he visited family residing in Nova Scotia. He was in Nova Scotia over the thanksgiving holidays in 2018 and 2019, during which he continued to receive Targeted Tech Support Calls.

21. Mr. Purvis has suffered inconvenience, psychological distress, anguish, frustration, anxiety and stress that is serious and prolonged as a result of receiving years of harassing phone calls and emails due to the Defendants' negligence and breach of privacy.

22. Mr. Purvis continues to suffer anxiety and distress over the materially increased risk of identity theft, being the target of additional scams, and further cybercrime.

23. The Plaintiff, Christopher Purvis, seeks to certify this action as a class proceeding pursuant to the *Class Proceedings Act*, on his own behalf and on behalf of the Class. As the proposed representative plaintiff, Mr. Purvis has no adverse interest to those of the proposed Class. The Plaintiff states that he would fairly and adequately represent the interests of this identifiable Class, that the Plaintiff's claims raise common issues, and that a class proceeding is the preferable procedure for the resolution of such common issues.

b. The Defendants

24. Dell is one of the largest multinational technological corporations PC manufacturing companies in the world, also selling computer hardware products, laptops, monitors, and printers to both individual consumers and businesses. With these products, Dell offers warranties and customer support through third party providers.

25. The Defendant, Dell USA L.P., is a body corporate incorporated under the laws of Texas, with a registered office at 211 E. 7th Street, Suite 620, Austin, Texas, 78701.

26. Dell Canada Inc. is the Canadian subsidiary of Dell Technologies Inc. and is a body corporate incorporated under the laws of Ontario, with a registered office at 155 Gordon Baker Rd #501, North York, Ontario M2H 3N5.

27. Dell USA L.P. and Dell Canada Inc. (collectively, "Dell" or the "Defendants") represent Dell to be "a leader across PCs, Software, Servers, Security and Services." Furthermore, Dell claims to be the world leader in cybersecurity solutions with software to "respond smarter, and predict and prevent more threats altogether."

28. References to the Defendants are deemed to include all other predecessors, affiliates, subsidiaries, and parent companies. Dell is wholly responsible for all the acts and omissions of any predecessor, affiliate, subsidiary, or parent company, having acquired, authorized, supervised, or assumed the obligations of any such company. The Defendants' business, including business operated between and in connection with its subsidiaries, affiliates, and parent companies, is inextricably interwoven, and each corporate Defendant is the agent of the others for the purposes of selling and supporting technological devices in Canada.

29. The Plaintiff states that the Defendants are responsible, jointly and severally, for the harms and damages suffered by the Plaintiff and Class Members. The tortious and otherwise actionable conduct alleged in this claim by each corporate Defendant was authorized, ordered, and performed by each corporate Defendant's officers, directors, agents, employees, and/or representatives while engaged in the management, direction, control, or transaction of its unified business affairs.

30. The Plaintiff pleads that, by virtue of the impugned conduct described herein, each of the Defendants is vicariously liable for the acts and omissions of the others, including for the following reasons:

    (i) each corporate Defendant was the agent of the other corporate Defendant;

    (ii) each corporate Defendant's business was operated in an interconnected manner with the businesses of the other corporate Defendant;

    (iii) each corporate Defendant intended that the business of Dell would be operated, managed, and used to provide technology products and services as a singular, cohesive organization;

    (iv) each corporate Defendant operated in unison to operate, manage, and derive benefit from the sale of technological products and services; and

    (v) the Defendants are related, associated, and/or affiliated.

31. The Plaintiff pleads the doctrine of *respondeat superior* and states that the Defendants are vicariously liable for their employees', affiliates', agents', and representatives' actions, errors, and omissions, including privacy breaches and tortious conduct.

32. From 2009 to 2018, Dell contracted with the Provider to provide Dell customer technical support from its call centre in India. The contract provided that Dell would provide Personal Information and Private Customer Information to the Provider. The contract also included contractual obligations with the Provider regarding the provision by the Provider of physical, organizational and technical safeguards, which were foreseeably inadequate and insufficient to protect the sensitive information from the June and November 2017 breaches, described below.

33. The Defendants transferred the Personal Information and Private Customer Information to the Provider, and thus the Provider and its employees had unmonitored access to this sensitive information to carry out technical support services on behalf of the Defendants. With respect to the Personal Information and Private Customer Information, Dell controlled the activities of the Provider, was in a position to reduce or completely avoid the loss, and Dell benefited from the activities of the Provider, who was furthering its business enterprise. The breaches of privacy were inextricably connected with Dell's authorization to the Provider to collect and use the Personal Information and Private Customer Information on its behalf. At all material times, the Defendants were responsible for protecting the Plaintiff's and Class' Personal Information and Private Customer Information while being transferred to and processed by the Provider. The Defendants were obligated to ensure the information was protected with sufficient safeguards, including physical, organizational, and technological safeguards to protect the against loss or theft, unauthorized access, disclosure, copying, or use. These obligations arise under the *Personal Information and Protection of Electronic Documents Act*, SC 2000, c 5, (PIPEDA) and pursuant to their common law duties, as described below.

IV. THE BREACH OF PRIVACY

(i.) Targeted Tech Support Scams

34. Technical support scams involve telephone or email fraud activities where a scammer poses as support from a legitimate company they claim to represent. The scammer then tries to gain an individual's trust to provide the scammer with remote access to their computer or paying for fraudulent technical support services. Once the scammer has remote access to the individual's computer, they can steal credit card or banking information, or install malicious software.

35. Targeted Tech Support Scams occur when the fraudster has access to both Personal Information and Private Customer Information, allowing them to trick targets into believing the calls come from authorized personnel of the trusted company, thereby increasing the effectiveness of the scam and likelihood that the victim will fall prey to it.

36. Targeted Tech Support Scams have been reported since 2008 and have steadily increased since. It is estimated that the great majority of this illegal activity originates from call centres in India.

37. Online reports of Targeted Tech Support Scams with callers having Dell customer information have been reported since 2015 on Dell's Community Message Board, and by the media in January 2016 and July 2018.

38. Targets of these scams suffer inconvenience, psychological distress and financial loss. Once targeted by these scams, individuals are more likely to be targeted by other scams and identity theft. Not only do victims falling prey to these scams pay scammers for what they believe to be legitimate tech support, but malicious software installation results in loss of data and the need for remediation, costing money for those unexperienced in computers. Furthermore, targets may require costly third-party credit protection and anti-fraud monitoring as they anxiously wait for further fraud.

(ii.) Dell Privacy Breaches

39. At the end of November 2017, the Defendants were informed by the Provider of detected privacy breaches containing Personal Information and Private Customer Information ("November 2017 Breach"). On November 4, 2017, the Provider had detected a suspicious email with a large attachment sent to an external email address by a managerial employee with rights to create reports with Dell customer information. The Provider advised that while this email had been intercepted, previous emails with smaller attachments had not been detected and Dell customers' privacy had been breached multiple times. The smaller emails contained Personal Information and Private Customer Information of approximately 7,883 Canadian Dell customers, which the Provider's employee had sold to a third party.

40. During the November 2017 Breach investigation, another of the Provider's managerial employees admitted to selling customers' Personal Information and Private Customer Information to a third party in June 2017 ("June 2017 Breach"). This employee used a USB drive to physically remove the information outside the organization, and this went entirely undetected by the Provider. Having had no safeguards to detect or prevent against physical removal of customer information, and then due to their inadequate investigation of the breach, the Defendants' own negligence means they are unaware of the number of Canadian Dell customers affected by the June 2017 Breach, or the scope of the information involved.

41. The employees had unmonitored access to the breached information through a customer management system portal, and it was accessed in the course of their employment, and connected with the acts Dell authorized the Provider to carry out on its behalf.

42. The Defendants received hundreds of customer complaints of the 2017 breaches, including many complaints after the June 2017 Breach, but before the November 2017 Breach. Since 2015, the Defendants have received over a thousand scam call reports from Canadians. Yet, the Defendants chose not to take investigative or remedial action, which could have prevented further breaches, or warn customers of the privacy breaches. In April of 2018, the Defendants sent an email to only the customers affected by the November 2017 Breach, making no express mention of the June 2017 Breach or the November 2017 Breach.

43. The OPC's investigation concluded in July of 2020 and confirmed the breaches, finding that Dell did not adequately safeguard the personal information under its control from inappropriate disclosure and breach. The OPC found that the information is particularly sensitive considering the nature of the information involved, the known risk environment and the potential harm to individuals in the event of a breach. It found that Dell's safeguards were lacking in the following areas:

(i) Access controls: Too many employees had the ability to access, re-access and build detailed customer reports containing numerous un-masked data elements, including Personal Information and Private Customer Information.

(ii) Monitoring and logging: There was no evidence of a logging and monitoring process - either by Dell to its Provider, or by the Provider to its system - to detect employee requests for Personal Information and Private Customer Information.

(iii) Technical measures: Notwithstanding Dell's knowledge of the risk of theft of Personal Information and Private Customer Information, email safeguards were easily circumvented using multiple smaller attachments, and Dell had not restricted the use of USB drives at employee workstations, allowing for undetected physical removal of the information.

(iv) Breach investigation: Dell's investigation into complaints of the breaches was not prompt nor thorough. Dell did not investigate complaints arising after the June 2017 Breach that could have prevented the November 2017 Breach. Dell did not ensure remedial measures were taken, but instead ignored and dismissed complaints, including that of the Plaintiff, allowing the issue to persist, and further breaches to occur. Dell blamed victims of the scams, claiming that customers should have recognized the scam. Dell chose not to investigate or take all reasonable steps to determine the scope of the June 2017 Breach, or those impacted.

44. The Defendants' safeguards were inadequate to protect the information. While the Provider scanned outgoing emails for attachment size and certain types of Personal Information (such as Social Insurance Numbers and credit card numbers), the scan did not detect smaller email

attachments containing Personal Information and Private Customer Information, enabling the breaches to go undetected. Personal Information and Private Customer Information could also easily be removed physically, without detection.

45. The Defendants' behaviour in ignoring customer indications of privacy breaches was particularly reckless and negligent, given the known risk of Targeted Tech Support Scams originating from India. The privacy breaches were simply a materialization of a foreseeable risk.

46. While the Defendants modified some of their safeguards following the November 2017 Breach, they have not offered any credit or fraud monitoring to customers whose information was breached. Nor did the Defendants take all reasonable measures to investigate and identify the customers and the scope of information breached in the June 2017 Breach. The Defendants have done nothing to mitigate or rectify the constant, prolonged, harassing, anxiety-inducing occurrences of these continuing Targeted Tech Support Scams for the Plaintiff and Class.

V. CAUSES OF ACTION

(i.) Dell's Negligence

47. At all material times, the breaches of the Plaintiff's and Class Members' privacy were within the Defendants' knowledge and control.

48. At all material times hereto, by virtue of selling PC products, collecting, creating and storing Personal Information and Private Customer Information, and providing related technical services, the Defendants owed legal duties to the Plaintiff and Class Members, including, *inter alia*, the duties to:

(i) be aware of, implement adequate safeguards, and properly respond to the heightened risk environment in which their customers' Personal Information and Private Customer Information was transferred, collected, created and stored;

(ii) ensure that their affiliates and third-party service providers protect the Personal Information and Private Customer Information with adequate and stringent security controls to safeguard the information in light of the known risk environment;

(iii) only disclose and permit the transfer, collection, creation and storage of Personal Information and Private Customer Information to affiliates and third-parties who agree to implement adequate measures to protect that information and use it solely for the purposes for which they are contracted, and to otherwise fulfill Dell's legal and regulatory requirements;

(iv) perform audits, assessments, examinations and reviews in relation to the data processed by the Provider at regular intervals and in light of the known risk environment;

(v) adequately protect and safeguard Personal Information obtained from customers and Private Customer Information created in the course of providing services to customers by implementing, and ensuring the Provider's implementation of, suitable technical, physical, and administrative information security safeguards in light of the known risk environment;

(vi) implement and require stringent access controls to limit the number of employees able to access, re-access and create reports containing Personal Information and Private Customer Information;

(vii) protect the Personal Information and Private Customer Information against breach, unauthorized use, theft and Targeted Tech Support Scams by ensuring that the least amount of information is made accessible to employees as is required to carry out their job functions, and by prohibiting the creation of detailed customer reports containing numerous data elements;

(viii) implement an active logging and monitoring process to oversee, manage, review and detect suspicious employee access to Personal Information and Private Customer Information;

(ix) take reasonable measures to inform customers of a known privacy breach implicating their Personal Information and Private Customer Information;

(x) promptly and thoroughly investigate a potential privacy breach and take all reasonable efforts to ascertain whether a breach occurred, its causes, potential vulnerabilities that remain unaddressed, the information breached and customers impacted, and ensure remedial measures are taken; and

(xi) comply with the minimum legal and regulatory standards set out by PIPEDA to ensure that private information in the Defendants' custody or control was adequately protected against theft, loss, use, copying and disclosure.

49. The Defendants breached the duties enumerated above, as set out in the following paragraphs.

50. The Plaintiff pleads that the conduct of the Defendants constitutes negligence, by their not having in place appropriate physical, organizational, and technical safeguards that would reasonably have prevented the June and November 2017 privacy breaches. The privacy breaches were reasonably foreseeable in light of the risk environment and known concerns of Targeted Tech Support Scams.

51. At all material times, the Defendants owed legal duties to the Plaintiff and Class Members to take reasonable care in protecting their Personal Information and Private Customer Information. The Defendants breached the requisite standard of care. The Defendants were negligent in that they:

(i) chose not to implement reasonable precautions and adequate safeguards considering the heightened risk environment in which their customers' Personal Information and Private Customer Information was transferred, collected, created and stored;

(ii) chose not to ensure that the Provider would protect the Personal Information and Private Customer Information with reasonably stringent security controls in light of the known risk environment;

(iii) chose not to perform regular, or any, audits, assessments, examinations and reviews in relation to the data processed by the Provider;

(iv) chose not to protect and safeguard Personal Information and Private Customer Information by implementing, and ensuring the Provider's implementation of, reasonably suitable technical, physical, and administrative information security safeguards;

(v) chose not to reasonably control access to the Personal Information and Private Customer Information, including by ensuring that the least amount of information is made accessible as is required to carry out job functions, and by prohibiting the creation of detailed customer reports containing numerous data elements;

(vi) chose not to actively log and monitor employee access to Personal Information and Private Customer Information;

(vii) chose not to ensure that the Provider's implemented safeguards could adequately detect privacy breaches;

(viii) chose to ignore and disregard customer complaints of potential privacy breaches;

(ix) chose not to exercise reasonable care in investigating customer complaints of potential privacy breaches, or carrying out thorough internal investigations of known privacy breaches in a timely manner or at all;

(x) chose not to take prompt and reasonable remedial measures upon becoming aware of potential breaches, including following the June 2017 Breach, but before the November 2017 Breach;

(xi) chose not to comply, or require the Provider's compliance with, with the minimum standards as set out in PIPEDA to ensure that private information in the Defendants' custody or control was adequately protected against theft, loss, use, copying and disclosure;

(xii) did not detect the June 2017 Breach in a timely manner;

(xiii) did not take all reasonable measures to thoroughly investigate the June 2017 Breach, once it was known or ought to have been known, including the scope of the information breached and customers impacted;

(xiv) chose not to take reasonably appropriate, or any, steps to prevent further breaches once privacy breaches ought to have been known;

(xv) chose not to inform their customers of the privacy breaches; and

(xvi) such further and other particulars as may be provided prior to the trial of this action.

52. The Defendants' negligence as set out above created a substantial likelihood of foreseeable harm for the Plaintiff and Class Members. The Plaintiff states that, as a result of the Defendants' negligence, the Plaintiff and Class have suffered inconvenience, distress, anguish, frustration, anxiety, stress and psychological damages of a serious and prolonged nature, and financial loss. The harms and damages of the Plaintiff and Class Members were caused by the negligent acts and omissions of Dell, for which Dell is fully liable.

(ii.) Intrusion Upon Seclusion by Dell

53. The acts and omissions of the Defendants constitute reckless intrusions upon seclusion that would be highly offensive to a reasonable person, for which the Defendants are liable. The Defendants' intrusion upon seclusion arises from the following:

(i) the Defendants were reckless in that they chose not to take reasonable and adequate steps to protect Personal Information and Private Customer Information against theft, unauthorized access, disclosure, copying, or use despite the Defendants' knowledge of the obvious and serious risk of theft of Personal Information and Private Customer Information;

(ii) combined Personal Information and Private Customer Information with inadequate privacy controls in a known risk environment for Targeted Tech Support Scams;

(iii) the information breached is particularly sensitive as it includes both Personal Information and Private Customer Information involving private correspondence and records regarding the Plaintiff's and Class Members' private communications with Dell;

(iv) the intrusions are highly offensive to a reasonable person given the combination of Personal Information with Private Customer Information that was breached and sold, which increases the risk of successful fraud, Targeted Tech Support Scams and identity theft;

(v) the intrusions are highly offensive to a reasonable person given the Defendants' portrayal as a leader in technological privacy;

(vi) the Defendants knew or ought to have known that a privacy breach of Personal Information and Private Customer Information would have significant and foreseeable adverse effects on Class Members; and

(vii) the intrusions and resultant Targeted Tech Support Scams caused serious and prolonged inconvenience, frustration, psychological distress and anxiety, as well as financial loss.

(iii.) Vicarious Liability for Intrusion Upon Seclusion by Agent

54. The Plaintiff pleads the doctrine of *respondeat superior* and states that the Defendants are vicariously liable for their agent's errors and omissions. The Defendants are liable for the acts and omissions of the Provider, given:

(i) the Provider was an agent of the Defendants;

(ii) the Provider's business was operated in an interconnected manner with the business of the Defendants;

(iii) the Defendants intended that the Provider would operate, manage and provide customer services to their customers as part of Dell's singular, cohesive organization;

(iv) the Provider operated in unison with the Defendants, and on their behalf, to provide customer services to Dell's customers; and

(v) the Provider and Defendants are related, associated, and/or affiliated.

55. The acts and omissions of the Provider's employees constitute intentional intrusions upon seclusion that would be highly offensive to a reasonable person, for which the Defendants are vicariously liable. The Defendants' vicarious liability arises from the fact that the Provider was providing technical support services on the Defendants' behalf, as its agent, in furtherance of the Defendants' enterprise, and the Provider was expected to protect the Plaintiff's and Class Members' Personal Information.

56. The relationship between the Defendants and the Provider is sufficiently close to warrant the imposition of vicarious liability. Dell used the Provider to provide Dell customer support, provided Personal Information and Private Customer Information to the Provider, and directed the Provider's provisions of physical, organizational and technical safeguards over such information, which were unreasonable and inadequate and which created conditions conducive to the intrusion upon seclusion.

57. With respect to the Personal Information and Private Customer Information, Dell controlled the activities of the Provider, was in a position to reduce or completely avoid the loss, and the Provider furthered Dell's corporate interests and business enterprise and lightened Dell's workload in terms of providing customer support on Dell's behalf.

58. The Provider's intentional intrusion upon seclusion is sufficiently connected to the Provider's assigned tasks of collecting and storing Personal Information and Private Customer Information, and providing Dell customer support, and thereby constitutes a materialization of the risks created by the Defendants' enterprise.

59. The Defendants knew or ought to have known of the serious risks of employee privacy breaches of Personal Information and Private Customer Information for use in Targeted Tech Support Scams in India. Nonetheless, at all material times, the Defendants authorized the Provider's employees unmonitored access to both Personal Information and Private Customer Information without adequate safeguards or monitoring controls in a known high-risk environment for the purpose of conducting business on behalf of the Defendants.

VI. DAMAGES

60. As a result of the Defendants' negligence and intrusion upon seclusion, the Plaintiff and Class Members have suffered and continue to suffer damages. The Plaintiff states that the Defendants knew, or ought to have known, that their common law and privacy breaches would cause the Plaintiff and Class Members damages, which include but are not limited to the following:

a. serious and prolonged emotional and psychological distress, harm and suffering arising from the Targeted Tech Support Scams and the increased future risk of identity theft, cybercrime and further scams;

b. inconvenience, expenditure of time and frustration;

c. out of pocket costs; and

d. financial loss.

VII. PUNITIVE DAMAGES

61. The Defendants have acted in a high-handed, wanton, reckless and/or deliberate manner, without due regard for the Plaintiff's and Class Members' privacy, so as to warrant an award of punitive damages, in accordance with the goals of retribution, denunciation and deterrence.

62. The Defendants failed to provide for sufficient safeguards to protect the Plaintiff's and Class Members' Personal Information and Private Customer Information from theft and/or disclosure and use. In so doing, they knowingly exposed the Plaintiff and Class Members to these risks, which in fact materialized.

63. The Defendants' disregard for the Plaintiff's and Class Members' privacy meant that Dell did not prevent or detect privacy breaches. Upon becoming aware, through customer complaints, that privacy breaches may have occurred, the Defendants failed to take the information seriously and failed to investigate in a timely fashion, or fully, thereby exposing the Plaintiff and Class Members to increased consequences of the breaches. Upon finally investigating, Dell's notification to the Plaintiff and Class Members about the privacy breaches, and its responses to their complaints, displayed disregard of their entitlement to know what had taken place and a continued disregard for their privacy.

64. The Defendants' conduct was callous and arrogant and offends the ordinary community standards of moral and decent conduct. The actions and omissions of the Defendants involved such want of

care that it could only have resulted from actual conscious indifference to the interests and welfare of the Plaintiff and Class Members.

65. Punitive damages are appropriate in the circumstances for the following reasons, *inter alia*:

Blameworthiness of Conduct

(i) The high-handed, wanton, reckless and/or deliberate conduct of the Defendants has persisted for a lengthy period of time;

(ii) The Defendants have concealed or attempted to cover up their misconduct;

(iii) The Defendants are, and have been, aware that their conduct is wrong;

(iv) The Defendants failed to address the effects of their misconduct; and

(v) The actions of the Defendants are deeply intrusive of the privacy rights of the Plaintiff and Class, causing harm.

Vulnerability of Class

(i) The Plaintiff and Class Members rely on the Defendants as leaders in the technology and security industry, and therefore rely on the Defendants to safeguard their information to the highest standard in the industry, particularly as the Class Members have no realistic choice but to provide their information to the Defendants if they are to receive necessary technological support for their purchases.

Proportionate to Need for Deterrence

(i) The misconduct of a leader in the technology and security industry must not be repeated by other technology and security companies, or condoned; and

(ii) The message needs to be sent to the Defendants and others in the industry that the Court is not indifferent to the serious issue of protecting privacy.

Proportionate to Other Penalties

(i) There are no other adequate penalties at law.

VIII. RELIEF SOUGHT

66. The Plaintiff, on behalf of the Class Members, claims:

(i) an Order certifying this action as a class proceeding and appointing the Plaintiff, Christopher Purvis, as Representative Plaintiff for the Class;

(ii) general and special damages for the breach of privacy and negligence;

(iii) punitive damages;

(iv) costs of preventing and rectifying identity theft and/or fraud;

(v) active identity theft and credit monitoring services;

(vi) interest pursuant to the *Judicature Act,* R.S.N.S. 1989, c. 240;

(vii) costs;

(viii) the costs of notice and of administering the plan of distribution of the recovery in this action, plus applicable taxes; and

(ix) such further and other relief as this Honourable Court deems just.

IX. LEGISLATION AND RULES

68. The Plaintiff pleads and relies upon the following:

a. *Class Proceedings Act,* S.N.S. 2007, c. 28;

b. *Judicature Act,* R.S.N.S. 1989, c. 240;

c. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

PLACE OF TRIAL: Halifax, Nova Scotia.

DATED at Halifax, Nova Scotia this 6th day of October, 2021.

RAYMOND F. WAGNER, Q.C.
MADDY CARTER
KATE BOYLE
Wagners
1869 Upper Water Street
Suite PH301, Historic Properties
Halifax, NS B3J 1S9
Tel: 902-425-7330
Email: raywagner@wagners.co
Email: mcarter@wagners.co
Email: kboyle@wagners.co
Solicitors for the Plaintiff