S-247342

NO.
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

[redacted]

PLAINTIFF

AND:

MONEYGRAM PAYMENT SYSTEMS, INC. and
MONEYGRAM PAYMENT SYSTEMS CANADA, INC.

DEFENDANTS

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c.50

NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff(s) for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

TIME FOR RESPONSE TO CIVIL CLAIM

A response to civil claim must be filed and served on the plaintiff(s),

(a) if you reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,

(b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,

(c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or

(d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF(S)

Part 1: STATEMENT OF FACTS

A. Nature of Action

1. The within proposed consumer protection multi-jurisdictional class proceeding involves the failure of the Defendants, MoneyGram Payment Systems, Inc. and MoneyGram Payment Systems Canada, Inc. (collectively hereinafter referred to as the "Defendant" or "MoneyGram"), to properly and adequately safeguard, secure, protect, store and/or maintain the personal identifiable information ("PII") and financial information of the Plaintiff and putative class members on its computer information systems, including, *inter alia*, their names, social insurance numbers, government identification information, transaction information, bank account information, MoneyGram Plus Rewards information, email addresses, postal addresses and phone numbers, which were accessed, compromised and/or stolen as a result of a cyber security data breach by unauthorized third parties (the "**Data Breach**").

2. The Defendant, MoneyGram, is a leading global money transfer, payment and financial services company which operates in more than 200 countries using both digital platforms

and retail locations. Consumers can send money domestically or internationally and pay bills using the Defendant's money transfer and payment services system.

3. As part of the Data Breach, cyber criminals gained access to the Defendant's information systems, performed reconnaissance measures, and stole a trove of consumer data before the Defendant even noticed such.

4. Specifically, the infiltration occurred between September 20 and 22, 2024, but the Defendant did not discovery the Data Breach until September 27, 2024.

5. The Data Breach occurred through a social engineering attack on the Defendant's IT helpdesk wherein the malicious actors impersonated an employee to gain access to that employee's account. The unauthorized actors then used the access given to it by IT helpdesk staff to remotely connect to the Defendant's information systems and target its Windows Active Directory systems directly.

6. The total number of individuals or entities who have had their data exposed due to the Defendant's failure to implement proper and appropriate security safeguards is unknown at this time, however, it is estimated to be in at least the hundreds of thousands, if not millions, based on the number of the Defendant's customers and the volume of money transfer transactions. The Defendant has not revealed the full extent of the Data Breach.

7. According to the Defendant's "**Consumer Data Notice**" regarding the Data Breach, it "proactively" took "certain systems offline, which temporarily impacted the availability of [its] services."

8. Given that the Defendant failed to identify the malicious activity until it was already concluded, the Defendant most likely lacked the appropriate logging, monitoring, and alerting systems necessary to enable it to identify such attacks. These tools are critical components of any reasonable cyber security program and are expected industry standards that the Defendant had a duty to implement and maintain but failed, refused and/or neglected to do so.

9. The Defendant did not initially recognize the cyber attack for what it was. Rather, it believed that it merely suffered a "network outage" rather than a data breach.

10. Notwithstanding its apparently lax cyber security measures, the Defendant purports to take cyber security seriously stating in part the following in its **"Global Privacy Notice"**:

> *"We use a variety of robust physical, technical, organizational, and administrative safeguards to protect your personal data from unauthorized access, loss or alteration."*

11. The Defendant disregarded the rights of the Plaintiff and putative class members by:

(a) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure it's computer data systems were protected;

(b) failing to disclose to it's customers the material fact that it did not have adequate computer data systems and security practices to safeguard customer PII and financial information;

(c) failing to take available steps to detect and prevent the Data Breach;

(d) failing to monitor and timely detect the Data Breach; and

(e) failing to provide the Plaintiff and putative class members prompt and accurate notice of the Data Breach.

12. As a result of the Data Breach, the Plaintiff and putative class members' PII and financial information have been exposed to unauthorized third parties or malicious actors for misuse. The injuries the Plaintiff and putative class members suffered as a direct result of the Data Breach include, but not limited to, the following:

(a) theft of PII and financial information;

(b) costs associated with the detection and prevention of identity theft and unauthorized use of PII and financial information;

(c) costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, lost money transfer and bill transfer payments, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts including, but not limited to, lost productivity and opportunities, time taken from the enjoyment of one's life and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

(d) the imminent and certainly impending injury resulting from the potential theft posed by the PII and financial information being exposed for sale on the "Dark Web";

(e) damages to and diminution in value of the PII and financial information entrusted to the Defendant for the sole purpose of acquiring or purchasing money transfer services from it; and

(f) the loss of privacy.

13. The injuries the Plaintiff and putative class members suffered were directly and proximately caused by the Defendant's failure to implement or maintain proper and adequate computer data security measures for the PII and financial information of the Plaintiff and putative class members.

14. The Plaintiff and putative class members retain a significant interest in ensuring that their PII and financial information, which remains in the Defendant's possession are protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose PII and financial information was accessed, compromised and/or stolen.

15. The Plaintiff and putative class members seek judgment requiring the Defendant to remedy the harm caused by it's misconduct, which includes, *inter alia*, compensating the Plaintiff and putative class members for the resulting theft arising from the Data Breach and for all reasonably necessary measures the Plaintiff and putative class members have had to take in order to identify, safeguard and protect their PII and financial information put at risk by the Defendant's inadequate and improper security of it's computer data systems .

B. The Parties

The Representative Plaintiff

16. [redacted]

17. In or about January 2022, the Plaintiff applied online for money transfer services from the Defendant and as a condition provided his PII and financial information to the Defendant.

18. Since the announcement of the Data Breach, the Plaintiff continues to monitor his money transfer services with the Defendant, bank and credit card accounts in an effort to detect and prevent any misuses of his personal and financial information. Further, the Plaintiff has incurred cost or expense in the form of having to purchase credit monitoring services.

19. The Plaintiff has, and continues to, spend his valuable time to protect the integrity of his finances and credit - time which he would not have had to expend but for the Data Breach.

20. The Plaintiff would not have applied for money transfer services with the Defendant and provided his PII and financial information to the Defendant had it disclosed that it lacked adequate computer systems and data security practices to safeguard consumers' PII and financial information from theft or misuse.

21. The Plaintiff suffered actual injury from having his PII and financial information accessed, compromised and/or stolen as a result of the Data Breach.

22. The Plaintiff suffered actual injury and damages in paying money transfer fees to, and

purchasing money transfer services through, the Defendant who failed to disclose that it lacked computer systems and data security practices adequate to safeguard consumers PII and financial information from theft or misuse.

23. The Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII and financial information--a form of intangible property that the Plaintiff entrusted to the Defendant for the purpose of applying for and using its money transfer services, which was accessed, compromised and/or stolen as a result of the Data Breach.

24. The Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has concerns for the loss of his privacy.

25. The Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his PII and financial information being placed in the hands of unauthorized third parties or malicious actors.

26. The Plaintiff has a continuing interest in ensuring his PII and financial information, which remains in the possession of the Defendant is protected and safeguarded from future data breaches.

The Defendants

27. The Defendant, MoneyGram Payment Systems, Inc. is a company duly incorporated pursuant to the laws of Delaware, one of the United States of America, and has a registered agent, The Corporation Trust Company, at Corporation Trust Center 1209 Orange Street, Wilmington, Delaware, 19801, United States of America.

28. The Defendant, MoneyGram Payment Systems, Inc., is one of the largest money transfer services company in the world and operates in more than 200 countries across 430,000 plus locations.

29. The Defendant, MoneyGram Payment Systems Canada, Inc., is a company duly incorporated pursuant to the laws of Canada, registered within the Province of British

Columbia under number C0866792, and has a registered and records office at 1800 - 510 West Georgia Street, Vancouver, British Columbia, V6B 0M3, Canada.

30. At all material times to the cause of action herein, the Defendant, MoneyGram Payment Systems Canada, Inc., was, and is, a wholly owned subsidiary of the Defendant, MoneyGram Payment Systems, Inc.

31. At all material times to the cause of action herein, the Defendant, MoneyGram Payment Services Canada, Inc. sold and provided money transfer services, and other financial services or products, throughout Canada, including the Province of British Columbia.

32. At all material times to the cause of action herein, the business and interests of each of the Defendants, MoneyGram Payment Systems, Inc. and MoneyGram Payment Systems Canada, Inc., is interwoven with that of the other and each is an agent of the other for the shared common purpose of offering money transfer services, and other financial services or products, to consumers in North America.

33. The Defendants, MoneyGram Payment Systems, Inc. and MoneyGram Payment Systems Canada, Inc., are collectively hereinafter referred to as the "Defendant" or "MoneyGram", unless referred to individually.

C. The Class and Class Period

34. This action is brought on behalf of members of a class consisting of the Plaintiff and all persons resident in Canada, except residents of Quebec, whose personal and financial information was accessed, compromised and/or stolen from the Defendant as a result of the Data Breach between September 22 and 24, 2024 (**"Class" or "Class Members"**), excluding employees, officers, directors , agents of the Defendant and their family members, class counsel, presiding judges, and any person who has commenced an individual proceeding against or delivered a release to the Defendant concerning the subject of this proceeding, or such other class definition as the Court may ultimately decide on the motion for certification.

D. Factual Allegations

i. The Defendant collected and stored Class Members' PII and financial information

35. The Defendant acquired, collected, stored and assured reasonable security over the Plaintiff's and Class Members' PII and financial information.

36. As a condition of its relationships with the Plaintiff and Class Members, the Defendant required that the Plaintiff and Class Members entrust the Defendant with highly sensitive and confidential PII and financial information.

37. The Defendant, in turn, stored that information in the Defendant's computer data system that was ultimately affected by the Data Breach.

38. By acquiring, collecting and storing the Plaintiff's and Class Members' PII and financial information, the Defendant assumed legal and equitable duties and further, knew or should have known, that it was thereafter responsible for protecting the Plaintiff's and Class Members' PII and financial information from unauthorized disclosure.

39. The Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and financial information.

40. The Plaintiff and Class Members relied on the Defendant to keep their PII and financial information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

41. The Defendant could have prevented the Data Breach by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as the Plaintiff's and Class Members' PII and financial information.

42. The Defendant's negligence in safeguarding the Plaintiff's and Class Members' PII and financial information is exacerbated by repeated warnings and alerts directed to protecting

and securing sensitive data, as evidenced by trending data breach attacks in recent years.

43. Yet, despite the prevalence of public announcements of data breach and data security compromises, the Defendant failed, neglected and /or refused to take appropriate steps to protect the Plaintiff's and Class Members' PII and financial information from being accessed, compromised and/or stolen.

ii. The Defendant had a duty to protect the stolen information

44. The Defendant's failure to adequately secure the Plaintiff's and Class Members' sensitive data violates duties it owes the Plaintiff and Class Members under common and statutory law, including the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 ("*PIPEDA*").

45. In addition to its obligations under *PIPEDA*, the Defendant owed a duty to the Plaintiff and Class Members to exercise reasonable care in acquiring, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in its possession from being accessed, compromised, stolen, lost and/or misused by unauthorized persons.

46. The Defendant owed a duty to the Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII and financial information of the Plaintiff and Class Members.

47. The Defendant owed a duty to the Plaintiff and Class Members to design, maintain and test its computer systems, servers, and networks to ensure that the PII and financial information of the Plaintiff and Class Members was adequately secured and protected.

48. The Defendant owed a duty to the Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained substandard data security systems.

49. The Defendant owed a duty to the Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

50. The Defendant owed a duty to the Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

51. The Defendant owed a duty to the Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII and/or financial information from theft as such an inadequacy would be a material fact in the decision to entrust this PII and/or financial information to the Defendant.

52. The Defendant owed a duty of care to the Plaintiff and Class Members as they were foreseeable and probable victims of any inadequate data security practices.

53. The Defendant owed a duty to the Plaintiff and Class Members to encrypt, and/or more reliably encrypt, the Plaintiff's and Class Members' PII and financial information and further, monitor user behavior and activity in order to identify possible threats.

iii. Defendant's Privacy Policy

54. As a condition of providing money transfer services, the Defendant required applicants to provide it with certain PII and financial information. In its ordinary course of business, the Defendant stored and maintained this PII and financial information.

55. By obtaining, collecting, using and deriving a benefit from the Plaintiff's and Class Members' PII and financial information, the Defendant assumed legal and equitable duties to those individuals or entities. The Defendant knew, or ought to have known, that it was responsible for protecting the Plaintiff's and Class Members' PII and financial information from disclosure. At all relevant times, the Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and financial information.

56. The Plaintiff and Class Members, as customers and/or consumers, relied on the Defendant to keep their PII and financial information confidential and securely stored, to use this

information for business purposes only and to make only authorized disclosures of this information.

57. In addition to its legal obligations under the law, the Defendant independently and routinely promised to safeguard PII and financial information. Pursuant to its "**Global Privacy Notice**" the Defendant represented in part the following:

> "*We use a variety of robust physical, technical, organizational, and administrative safeguards to protect your personal data from unauthorized access, loss or alteration.*"

iv. The Data Breach

58. On or about October 7, 2024 the Defendant notified Class Members by letter and/or on its website of the Data Breach entitled "**CONSUMER DATA NOTICE**", which represented in part the following:

> "*To Our Customers*
>
> *MoneyGram Payment Systems, Inc. recently learned of a cybersecurity issue affecting certain of our company's systems.*
>
> ***What Happened?***
>
> *On September 27, 2024, we determined that an unauthorized third party accessed and acquired personal information of certain consumers between September 20 and 22, 2024. Our investigation is ongoing.*
>
> ***What Information Was Involved?***
>
> *The impacted information included certain affected consumer names, contact information (such as phone numbers, email and postal addresses), dates of birth, a limited number of Social Security numbers, copies of*

government-issued identification (such as driver's licences), other identification documents (such as utility bills), bank account numbers, MoneyGram Plus Rewards numbers, transaction information (such as dates and amounts of transactions) and, for a limited number of consumers, criminal investigation information (such as fraud). The types of impacted information varied by affected individual."

59. The Data Breach occurred as a result of the Defendant's failure to adequately safeguard, protect and/or secure the PII and financial information of its customers.

60. At no point did the Defendant offer any concrete assistance or offer to remunerate the Plaintiff and Class Members for its negligence.

61. The PII and financial information accessed, compromised and/or stolen as a result of the Defendant's acts and/or omissions and its failure to properly safeguard and protect the PII, and financial information despite being aware of cyber security standards, industry best practices and the vulnerability of companies that offer money transfer services to attack.

62. In addition to its failure to prevent the Data Breach, the Defendant also failed to recognize, monitor and detect the Data Breach in a timely manner.

63. While timely action by the Defendant in identifying the Data Breach would likely have significantly reduced the harmful consequences, instead, its inaction and/or negligence contributed to the scale of the Data Breach and the resulting damages to the Plaintiff and Class Members.

v. Defendant's Data Breach was imminently foreseeable

64. The Defendant's data security obligations were particularly important given the substantial increase in cyber attacks and/or data breaches targeting institutions that collect and store PII and financial information, such as the Defendant, preceding the date of the Data Breach.

65. Data thieves regularly target institutions, such as the Defendant, due to the highly sensitive

information in their custody. The Defendant knew and understood that unprotected PII and financial information is valuable and highly sought after by criminal parties who seek to illegally monetize that PII and financial information through unauthorized access.

66. As a data custodian of PII and financial information, the Defendant knew, or should have known, the importance of safeguarding the PII and financial information entrusted to it by the Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on the Plaintiff and Class Members because of a breach.

67. Despite the prevalence of public announcements of data breach and data security compromises, the Defendant failed to take appropriate steps to protect the PII and financial information of the Plaintiff and Class Members from being accessed, compromised and/or stolen.

68. The Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed PII and financial information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

69. The injuries to the Plaintiff and Class Members were directly and proximately caused by the Defendant's failure to implement or maintain adequate data security measures for the PII and financial information of the Plaintiff and Class Members.

70. The ramifications of the Defendant's failure to keep secure the PII and financial information of the Plaintiff and Class Members are long lasting and severe. Once PII and financial information is stolen, fraudulent use of that information and damage to victims may continue for years.

vi. Value of PII

71. PII and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post for sale stolen credit or payment card numbers, social

insurance numbers, and other highly sensitive personal information, on several underground internet websites for such PII and financial information for both individuals and companies.

72. Identity thieves can use PII and financial information, such as that of the Plaintiff and Class Members, which the Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims - for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

73. According to the United States Government Accountability Office, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

74. As to the cause of action herein, the Defendant knew of the importance of safeguarding PII and financial information and of the foreseeable consequences that would occur if the Plaintiff's and Class Members' PII and financial information were accessed, compromised and/or stolen, including the significant costs that would be placed on the Plaintiff and Class Members as a result of a breach of this magnitude.

75. As averred to above, the Defendant is a sophisticated organization with the resources to deploy robust cyber security protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties owed to the Plaintiff and Class Members. As such, its failure to do so is intentional, willful, reckless and/or gross negligence.

76. The Defendant disregarded the rights of the Plaintiff and Class Members by, *inter alia*: (I) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard the Plaintiff's and Class Members' PII and

financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide the Plaintiff and Class Members prompt and accurate notice of the Data Breach.

vii. Failure to comply with industry standards

77. Experts studying cyber security routinely identify institutions that store PII and financial information, such as the Defendant, as being particularly vulnerable to cyber attacks because of the value of the PII and financial information, which they collect and maintain.

78. Certain industry best practices that should be implemented by institutions dealing with sensitive PII and financial information, such as the Defendant, include, but are not limited to: educating all employees, strong password requirements, multi-layer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, the Defendant failed to follow some or all these industry best practices.

79. Other best cyber security practices that are standard at large institutions that store PII and financial information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

80. Further, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cyber security programs.

81. The Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1. 1 (including without limitation PR.AC-I, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-I, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.C0-2), and the Center

for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cyber security readiness.

82. The Defendant failed to comply with these accepted standards, and those of *PIPEDA*, thereby permitting the Data Breach to occur.

viii. Common injuries & damages

83. As a result of the Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII and financial information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and the Plaintiff and Class Members have all sustained actual injuries and damages, including: (I) invasion of privacy; (ii) loss of time and productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) the loss of benefit of the bargain (price premium damages); (iv) diminution of value of their PII and financial information; and (e) the continued risk to their PII and financial information, which remains in the possession of the Defendant, and which is subject to further breaches, so long as the Defendant fails to undertake appropriate and adequate measures to protect the Plaintiff's and Class Members' PII and financial information.

ix. The Data Breach increases victims' risk of identity theft

84. The Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because the Defendant's failures resulted in the Plaintiff's and Class Members' social insurance numbers falling into the hands of identity thieves.

85. The unencrypted PII and financial information of Class Members has already, or will end up, for sale on the Dark Web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the Dark Web, it is usually at least sold on private telegram channels to even further identity thieves who purchase the PII and financial information for the express purpose of conducting fraud and identity theft operations.

86. Further, the standard operating procedure for cyber criminals is to use some data, like

social insurance numbers, to gain further access to a person's PII and financial information, which those cyber criminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.

87. Cyber criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

88. As such, the accessed, compromised and/or stolen PII and financial information from the Data Breach can easily be used to link and identify it to the Plaintiff and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create an identity package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

x. Loss of time to mitigate risk of identity theft and fraud

89. Due to the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII and/or financial information was accessed, compromised or stolen, as in this Data Breach, a reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and from a defendant asserting that the individual failed to mitigate his or her damages.

90. The need to spend time mitigating the risk of harm is especially important in the case at bar where Plaintiff's and Class Members' social insurance numbers or other government identification are affected.

91. The Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

92. These efforts are also consistent with the steps that government authorities recommend that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

xi. The future cost of credit and identity theft monitoring is reasonable and necessary

93. Based on the value of the information accessed, compromised and/or stolen, the data either has or will be sold to cyber criminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private telegram channels wherein thousands of cyber criminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

94. Such fraud may go undetected for years; consequently, the Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

95. The retail cost of credit and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a number of years that the Plaintiff and Class Members would not need to bare but for Defendant's failure to safeguard their PII and financial information.

xii. Plaintiff and Class Members suffered actual damages as a result of the Data Breach

96. The PII and financial information of the Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by the Defendant. The Defendant did not obtain the Plaintiff's and Class Members' consent to disclose their PII and financial information to any other third party as required by applicable law and industry standards.

97. The Data Breach was a direct and proximate result of the Defendant's failure to properly safeguard and protect the Plaintiff's and Class Members' PII and financial information from unauthorized access, use and disclosure, as required by government regulations and industry practices, including the Defendant's failure to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the Plaintiff's and Class Members' PII and financial information so as to protect against reasonably foreseeable threats to the security or integrity of such information.

98. The Defendant had the resources to prevent a data breach, but instead chose to put profit before consumers' privacy and protection of their PII and financial information.

99. Had the Defendant remedied the deficiencies in its computer data systems, followed government regulations and adopted the appropriate industry security measures, the Defendant would have prevented intrusion into its computer data systems and, ultimately, the theft of its consumers' confidential PII and financial information.

100. As a result of the Defendant's wrongful actions, inaction, negligent security practices and the resulting Data Breach, the Plaintiff and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity and filing police reports. This time has been lost forever and cannot

be recaptured.

101. The Defendant's, wrongful actions and/or inaction directly and proximately caused the theft and dissemination into the public domain of the Plaintiff's and Class Members' PII and financial information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

(a) theft of their personal and financial information;

(b) unauthorized charges on their debit and/or credit card accounts;

(c) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information and financial information being placed in the hands of unauthorized third parties and misused *via* the sale of the Plaintiff's and Class Members' information on the Dark Web;

(d) the untimely and inadequate notification of the Data Breach;

(e) the improper disclosure of their PII and financial information;

(f) loss of privacy;

(g) money transfer fees paid to the Defendant during the Data Breach, which the Plaintiff and Class Members would not have made with the Defendant had it disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII and financial information from theft;

(h) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

(I) ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established black market; and

(j) the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

102. While the Plaintiff's and Class Members' PII and financial information has been accessed, compromised and/or stolen, the Defendant continues to hold the PII and financial information of consumers, including the Plaintiff's and Class Members' PII and financial information. Given that the Defendant has demonstrated an inability to prevent a data breach, the Plaintiff and Class Members have an undeniable interest in ensuring that their PII and financial is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

Part 2: RELIEF SOUGHT

1. The Plaintiff, on his own behalf, and on behalf of Class Members, claims against the Defendant as follows:

(a) an order certifying this action as a class proceeding pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c.50 and appointing the Plaintiff as the named representative of the Class;

(b) a declaration that the Defendant owed a duty of care to the Plaintiff and Class Members and was negligent in failing to adequately safeguard, protect, store and/or maintain the PII and financial information of the Plaintiff and Class Members;

(c) a declaration that the Defendant breached its duty to adequately safeguard, protect, store and/or maintain the PII and financial information of the Plaintiff and Class Members;

(d) a declaration that the Defendant breached its contractual duties owed to the Plaintiff and Class Members by permitting or failing to prevent the compromise and/or theft of the PII and financial information of the Plaintiff and Class Members as a result of the Data Breach;

(e) a declaration that the Defendant violated the Plaintiff's and Class Members' statutory right to privacy under the *Privacy Act*, R.S.B.C. 1996, c.373, *The Privacy Act*, R.S.S. 1978, c. P-24, *The Privacy Act*, C.C.S.M. c. P125, *Privacy Act*, R.S. N.L. 1990, c-P-22 by failing to adequately safeguard, protect, store and/or maintain their personal and/or financial information;

(f) a declaration that the Defendants violated the *Business Practices and Consumer Protection Act*, S.B.C. 2004, *Fair Trading Act*, R.S.A. 2000, c. F2, *Consumer Protection and Business Practices Act*, S.S. 2014, c.C-30.2, *Business Practices Act, C.C.S.M.* c. B1230, *Consumer* Protection and Business Practices Act, S.N.L. 2009, c. C-31.1 and *Business Practices* Act, R.S.P.E.I. 1988, c.B-7 by engaging in deceptive acts and/or business practices which misrepresented the safety and security of the Plaintiff's and Class Members' PII and financial information on its computer data system;

(g) a declaration that the Defendant violated *PIPEDA* by failing to adequately safeguard, protect, store and/or maintain the PII and financial information of the Plaintiff and Class Members;

(h) a declaration that the Defendant is vicariously liable for the acts and/or omissions of its officers, directors, agents, employees and representatives;

(i) damages;

(j) punitive, aggravated or exemplary damages;

(k) interim, interlocutory and permanent Orders as are necessary to protect the interests of the Plaintiff and Class Members as result of the Data Breach including,

inter alia, that the Defendant provide appropriate credit monitoring services;

(l) costs on a solicitor/client basis;

(m) pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996, c. 79; and

(n) such further and other relief as to this Honourable Court may seem just.

Part 3: LEGAL BASIS

A. Jurisdiction

1. There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act,* R.S.B.C. 2003, c.28 (the *"CJPTA"*) in respect of these Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to sections 10(e)(I), (g) and (h) of the *CJPTA* because this proceeding:

(e)(i) concerns contractual obligations, which to a substantial extent, were to be performed in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia.

B. Causes of Action

Negligence

2. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

3. The Defendant acquired and took possession of Plaintiff's and the Class Members' PII and financial information, and as such, it had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Further, the Defendant had a duty to destroy the Plaintiff's and Class Members' PII and financial information within an appropriate amount of time after it was no longer required by it, in order to mitigate the risk of such non-essential PII and financial information being accessed, compromised and/or stolen in a data breach.

4. Upon accepting and storing the Plaintiff's and Class Members' PII and financial information in its computer data systems and on its networks, the Defendant undertook and owed a duty of care to the Plaintiff and Class Members to exercise reasonable care to secure and safeguard the Plaintiff's and Class Members' PII and financial information and to use commercially-reasonable methods to do so. The Defendant knew that the PII and financial information was private and confidential, and should be protected as private and confidential.

5. The Defendant owed a duty of care not to subject the Plaintiff and Class Members, along with their PII and financial information, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate computer data system security practices.

6. The Defendant owed a duty of care to the Plaintiff and Class Members to quickly detect a data breach and to timely act on warnings about data breaches.

7. The Defendant's duties arose from its relationship to the Plaintiff and Class Members and from industry standards.

8. The Defendant through its actions and/or failures to act, unlawfully breached duties owed to the Plaintiff and Class Members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the PII and financial information entrusted to it.

9. The Defendant through its actions and/or failures to act, allowed unmonitored and

unrestricted access to unsecured PII and financial information.

10. The Defendant through its actions and/or failures to act, failed to provide adequate supervision and oversight of the PII and financial information with which it was entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather the Plaintiff's and Class Members' PII and financial information, misuse that PII and financial information and intentionally disclose it to unauthorized third parties without consent.

11. The Defendant knew, or ought to have known, the risks inherent in collecting and storing PII and financial information, the importance of adequate security and the well-publicized data breaches within the money transfer and/or financial services industries.

12. The Defendant knew, or ought to have known, that its computer data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII and financial information.

13. Due to the Defendant's knowledge that a breach of its computer data systems would damage hundreds of thousands or more of its customers including the Plaintiff and Class Members, it had a duty to adequately protect its computer data systems and the PII and financial information contained thereon.

14. The Defendant had a special relationship with the Plaintiff and Class Members. The Plaintiff's and Class Members' willingness to entrust the Defendant with their PII and financial information was predicated on the understanding that it would take adequate security precautions to safeguard that information. Moreover, only the Defendant had the ability to protect its computer data systems and the PII and financial information stored on those computer data systems from cyber attack.

15. The Defendant's own conduct also created a foreseeable risk of harm to the Plaintiff and Class Members and their PII and financial information. The Defendant's misconduct included, *inter alia*, failing to:

(a) secure its computer data systems, despite knowing their vulnerabilities;

(b) comply with industry standard security practices;

(c) implement adequate system and event monitoring; and

(d) implement the systems, policies, and procedures necessary to prevent this type of Data Breach.

16. The Defendant also had independent duties under government regulations that required it to reasonably safeguard the Plaintiff's and Class Members' PII and financial information, and promptly notify them about the Data Breach.

17. The Defendant breached it's duties owed to the Plaintiff and Class Members, the particulars of which, *inter alia*, are:

(a) failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard the Plaintiff's and Class Members' PII and financial information;

(b) failing to timely and accurately disclose that the Plaintiff's and Class Members' PII and financial information had been improperly accessed, compromised and/or stolen.

(c) by creating a foreseeable risk of harm through the misconduct as alleged herein;

(d) failing to implement adequate security systems, protocols and practices sufficient to protect the Plaintiff's and Class Members' PII and financial information before and after learning of the Data Breach;

(e) failing to comply with industry data security standards during the period of the Data Breach;

(f) failing to adequately protect and safeguard the PII and financial information by knowingly disregarding standard information security principles, despite obvious

risks, and by allowing unmonitored and unrestricted access to unsecured PII and financial information;

(g) failing to provide adequate supervision and oversight of the PII and financial information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and financial information of the Plaintiff and Class Members, misuse the PII and financial information and intentionally disclose it to others without consent;

(h) failing to adequately train its employees not to store PII and financial information longer than absolutely necessary;

(I) failing to consistently enforce security policies aimed at protecting the Plaintiff and Class Members' PII and financial information;

(j) failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

(k) failing to encrypt the Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

18. The Defendant's wilful failure to abide by these duties was wrongful, reckless and gross negligence in light of the foreseeable risks and known threats.

19. Through the Defendant's acts and/or omissions, as alleged herein, including it's failure to provide adequate security and to protect the Plaintiff's and Class Members' PII and financial information from being foreseeably captured, accessed, disseminated, stolen and misused, the Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Plaintiff's and Class Members' PII and financial information while it was within its possession or control.

20. The Defendant had an affirmative duty to timely disclose the unauthorized access and theft

of the Plaintiff's and Class Members' PII and financial information so that the Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII and financial information.

21. The Defendant breached its duty to notify the Plaintiff and Class Members of the unauthorized access to their PII and financial information by waiting to notify them and then by failing to provide the Plaintiff and Class Members complete and sufficient information regarding the Data Breach.

22. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, the Defendant prevented the Plaintiff and Class Members from taking meaningful proactive steps to secure their financial data, bank accounts and/or credit cards

23. The Defendant improperly and inadequately safeguarded the Plaintiff's and Class Members' PII and financial information in deviation of standard industry rules, regulations and practices at the time of the unauthorized access. The Defendant's failure to take proper security measures to protect sensitive PII and financial information, as described herein, created conditions conducive to a foreseeable, intentional criminal act namely, the unauthorized access and theft of Plaintiff's and Class Members' PII and financial information.

24. The Defendant's conduct was grossly negligent and departed from all reasonable standards of care including, but not limited to, failing to adequately protect the PII and financial information, failing to conduct regular security audits, failing to provide adequate and appropriate supervision of persons having access to the Plaintiff's and Class Members' PII and financial information, and failing to provide the Plaintiff and Class Members with timely and sufficient notice that their sensitive PII and financial information had been accessed, compromised and/or stolen.

25. Neither the Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their PII and financial information, as described herein.

26. The Defendant's failure to exercise reasonable care in safeguarding PII and financial

information by adopting appropriate security measures including proper encryption storage techniques, was the direct and proximate cause of the Plaintiff's and Class Members' PII and financial information being accessed, compromised and/or stolen through the Data Breach.

27. The Defendant breached its duties to the Plaintiff and Class Members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard the Plaintiff's and Class Members' PII and financial information.

28. As a result of the Defendant's breach of duties, the Plaintiff and Class Members suffered damages including, but not limited to, damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia,* by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft, as described herein.

Breach of Contract

29. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

30. The Defendant solicited and invited the Plaintiff and Class Members to apply for money transfer services by providing their PII and financial information. The Plaintiff and Class Members accepted the Defendant's offers and provided their PII and financial information to the Defendant to apply for its money transfer services.

31. When the Plaintiff and Class Members applied for the Defendant's money transfer services, they provided their PII and financial information to the Defendant. In so doing, the Plaintiff

and Class Members on the one hand, and the Defendant, on the other, entered into mutually agreed-upon contract, express and/or implied, pursuant to which the Plaintiff and Class Members agreed that their PII and financial information was valid, while the Defendant agreed that it would use the Plaintiff's and Class Members' PII and financial information in its possession for only the agreed-upon purpose of processing money transfer services, and no other purpose.

32. Implicit in the agreement to use the PII and financial information in its possession for only the agreed-upon money transfer services, and no other purpose, was the obligation that the Defendant would use reasonable measures to safeguard and protect the PII and financial information of the Plaintiff and Class Members in its possession. The relevant provisions of the agreement are as follows:

(a) *"The MoneyGram online money transfer services ("**Services**") are provided by MoneyGram Payment Systems Canada, Inc. ("**we**", "**us**", "**our**", or "**MoneyGram**") through our website (moneygram.ca) and mobile site (collectively, the **"Website"**) and our network of agents., authorized delegates and other permitted entities (each an "**Agent**"). These terms and conditions, along with any forms, receipts, acknowledgments, or other documentation completed or used in connection with your use of the Services, including any pre-transaction or post-transaction disclosures, constitute the entire agreement ("Agreement") between you, the individual purchaser of the Services ("**you**", "**your**" or "**Sender**") and MoneyGram."*

(b) *Acceptance of Terms of Use*

These terms of use are entered into by and between you and MoneyGram Payment Systems Canada, Inc. ("Company", "we" or "us"). The following terms and conditions, together with any documents incorporated by reference (collectively, these "Terms of Use"), govern your access to and use of moneygram.com, including any content, functionality and services offered on or through the

moneygram.com domains, subdomains or sub-directories, regardless of your means of access and use (whether on line or mobile, including by way of mobile application) (collectively the "Sites"), whether as a guest or a registered user.

Please read the Terms of Use carefully before you start to use the Sites. By using the Sites, you accept and agree to be bound and abide by these Terms of Use and our Privacy Statement, which are located at each homepage of our Sites and are incorporated herein by reference.

To access the Sites or some of the resources it offers, you may be asked to provide certain registration details or other information. It is a condition of your use of the Sites that all the information you provide on the Sites is correct, current and complete. You agree that all information you provide to us through the Sites or otherwise, including but not limited to the use of any interactive features on the Sites, is governed by our Privacy Statement, and you consent to all actions we take with respect to your information consistent with our Privacy Statement

(c) *Privacy Notice*

By using the Services you consent to the collection, use, disclosure and transfer (including cross-border transfer) of your personal information, please see our ***Privacy Notice****.*

(d) *Global Privacy Notice*

This notice explains how we use your personal data: what information we collect about you, why collect it, what we do with it, and what your rights are related to the use of your data. Below you will find information on:

i *Who is the data controller*

Ii. *Who is the data protection officer*

iii *What categories of your personal data we process*

iv. *Why we collect, use and store your personal data*

v. *How we share your personal data*

vi. *How we transfer your personal data to third countries*

vii. *How long we retain your personal data*

viii. *What are our information security standards*

What categories of your personal data we process?

The categories of personal data we process will vary based on your relationship or interaction with us. This may include the following:

• Personal identification information, such as your name, residential and/or business address, e-mail address, telephone number, date of birth, gender, images, marital status, country of citizenship, and identification numbers (e.g., national identification number(s) and /or national ID details);

•Transaction and financial details, such as money transfer data relating to the sender and the receiver, bill paying details, as well as bank and credit information,

• Business-related information that helps us provide Services to you, such as membership in our loyalty programs, how you Services, employer information, communication preferences, or your marketing choices;

•Technological information, such as IP address, browser, device information, including device identifiers and device's advertising ID, mobile application usage data, information collected through cookies, pixel tags, browser analysis tools, server logs, web

beacons, SDK and other similar technologies (collectively, cookies), your current location from your mobile device, demographic information and closed-circuit television ("CCTV") data. Some of the information is collected via cookies. For details on how we use cookies, please see our Cookie Notice; and

•Compliance information, such as may be requested by law enforcement or pursuant to our compliance procedures to comply with legal obligations and internal policies such as concerning fraud prevention, anti-money laundering and sanctions. We collect personal data directly from you, for example, when you contact our call center, complete online forms, register for our loyalty programs, apply to become an agent, or use the Services. In some situations, we also collect your personal data from other people or organizations such as: money transfer senders, our third-party vendors, public record sources (federal, state or local government sources), MoneyGram affiliates and subsidiaries, social media platforms, MoneyGram partners or agents, depending on our relationship with them.

33. By accepting the PII and financial information for money transfer services the Defendant assented to and confirmed its agreement to reasonably safeguard and protect the Plaintiff's and Class Members' PII and financial information from unauthorized disclosure or uses and to timely and accurately notify the Plaintiff and Class Members if their data had been breached, accessed, compromised and/or stolen by unauthorized third parties.

34. The Plaintiff and Class Members would not have provided and entrusted their PII and financial information to the Defendant to apply for its money transfer services in the absence of the contracts, express and/or implied, between them and the Defendant.

35. The Plaintiff and Class Members fully performed their obligations under the contracts, express and/or implied, with the Defendant.

36. The Defendant breached the contracts, express and/or implied, it made with the Plaintiff and Class Members by failing to safeguard and protect the Plaintiff's and Class Members' PII and financial information and by failing to provide timely and accurate notice to them that their PII and financial information was accessed, compromised and/or stolen as a result of the Data Breach.

37. The Defendant breached the contracts, express and/or implied, it made with the Plaintiff and Class Members by failing to ensure that the Plaintiff's and Class Members' PII and financial information in its possession was used only for the agreed-upon purpose and no other purpose.

38. The Plaintiff and Class Members conferred a monetary benefit on the Defendant, which has accepted or retained that benefit. Specifically, the Defendant charges a transaction fee for money transfer services. In exchange, the Plaintiff and Class Members should have received the money transfer services that were the subject of the transaction and should have been entitled to have the Defendant protect their PII and financial information with adequate computer data security measures in the performance of its money transfer services obligations.

39. The Defendant failed to secure the Plaintiff's and Class Members' PII and financial information and therefore, did not provide full compensation for the benefit the Plaintiff and Class Members provided.

40. The Defendant acquired the PII and financial information through inequitable means when it failed to disclose the inadequate computer data security practices, as alleged herein.

41. Had the Plaintiff and Class Members known that the Defendant would employ inadequate computer data security measures to safeguard their PII and financial information, they would not have applied for the Defendant's money transfer services.

42. As a direct and proximate result of the Defendant's breaches of the contracts, express and/or implied, between it on the one hand, and the Plaintiff and Class Members on the other, the Plaintiff and Class Members suffered actual losses and damages, as described

herein.

43. The Plaintiff and Class Members were harmed as the result of the Defendant's breach of the contracts, express and/or implied, because their PII and financial information was accessed, compromised and/or stolen, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and financial information was disclosed to third parties without their consent. The Plaintiff and Class Members also suffered diminution in value of their PII and financial information in that it is now easily available to hackers on the Dark Web. The Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees and other expenses relating to identity theft losses or protective measures. The Plaintiff and Class Members are further damaged as their PII and financial information remains in the hands of those who obtained it without their consent.

Breach of Privacy

44. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

45. The Plaintiff and Class Members had a legitimate expectation of privacy to their PII and financial information and were entitled to the protection of this information against disclosure to unauthorized third parties.

46. The Defendant owed a duty to its customers, including the Plaintiff and Class Members, to keep their PII and financial information confidential.

47. The Defendant failed to protect and released to unknown and unauthorized third parties computer databases containing the PII and financial information of the Plaintiff and Class Members.

48. The Defendant allowed unauthorized and unknown third parties access to and examination of the PII and financial information of the Plaintiff and Class Members by way of the Defendant's failure to protect the PII and financial information in its computer databases.

49. The unauthorized release to, custody of and examination by unauthorized third parties of the PII and financial information of the Plaintiff and Class Members, especially where the information includes social insurance numbers, dates of birth, government identification information, transaction information and bank account information, is highly offensive to a reasonable person.

50. The intrusion was into a place or thing which was private and is entitled to be private. The Plaintiff and Class Members disclosed their PII and financial to the Defendant as part of their use of the Defendant's money transfer services, but privately with an intention that the PII and financial information would be kept confidential and would be protected from unauthorized disclosure. The Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

51. The Data Breach at the hands of Defendant constitutes an intentional and wilful interference with the Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person causing them distress, humiliation and/or anguish.

52. The Defendant acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its computer data security practices were inadequate and insufficient. As such, the Defendant intentionally violated and wilfully invaded the privacy of the Plaintiff and Class Members.

53. By permitting unauthorized third parties to access to the Plaintiff's and Class Members' PII, and financial information the Defendant breached the Plaintiff's and Class Members' statutory right to privacy under the *Privacy Act,* R.S.B.C. 1996, c.373, *The Privacy Act*, R.S.S. 1978, c. P-24, *The Privacy Act*, C.C.S.M. c. P125, *Privacy Act*, R.S. N.L. 1990, c-P-22 and *PIPEDA,* which the Plaintiff and Class Members plead and rely upon.

54. As a proximate result of the above acts and/or omissions of the Defendant, the PII and financial information of Plaintiff and Class Members was disclosed to third parties without authorization, causing the Plaintiff and Class Members to suffer damages.

55. Unless and until enjoined and restrained by order of this Court, the Defendant's wrongful conduct will continue to cause great and irreparable injury to the Plaintiff and Class Members in that the PII and financial information maintained by Defendant can be viewed, distributed and/or used by unauthorized persons. The Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for the Plaintiff and Class Members.

Breach of Consumer Protection Legislation

56. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

57. The Plaintiff and Class Members purchased money transfer services from the Defendant pursuant to a contract and/or agreement. These services were exclusively for personal, family or household reasons.

58. The contract and/or agreement is a "consumer contract" with the Defendant pursuant to applicable consumer protection legislation in their respective provinces, including the: Business *Practices and Consumer Protection Act*, S.B.C. 2004, *Fair Trading Act*, R.S.A. 2000, c. F2, *Consumer Protection and Business Practices Act*, S.S. 2014, c. C-30.2, *Business Practices Act,* C.C.S.M. c. B1230*, Consumer Protection and Business Practices* Act, S.N.L. 2009, c. C-31.1 and *Business Practices* Act, R.S.P.E.I. 1988, c.B-7 ("Applicable Consumer Protection Legislation") . These contracts created contractual privity between the Class Members and the Defendant.

59. The Applicable Consumer Protection Legislation was enacted to protect consumers against unfair and/or deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale of goods or services to consumers. The Defendant's acts, omissions, representations and/or practices, as described herein, as to its computer data system for the purposes of providing money transfer services falls with within the Applicable Consumer Protection Legislation.

60. The Plaintiff and Class Members are "consumers" within the meaning of the Applicable

Consumer Protection Legislation.

61. The Defendant's acts, omissions, misrepresentations and/or practices were and are likely to deceive consumers. By misrepresenting the safety and security of its computer data system, the Defendant breached the Applicable Consumer Protection Legislation. The Defendant had exclusive knowledge of undisclosed material facts, namely, that its computer data system was defective and/or unsecured, and withheld that knowledge from the Plaintiff and Class Members.

62. The Defendant made, approved and/or authorized a number of common representations in relation to its data security practices and measures. At the time that the Plaintiff and Class Members entered into their money transfer services contracts or agreements, the Defendant made the following representations in its in Global Privacy Notice (the "Representations") in breach of the Applicable Consumer Protection Legislation:

(a) representing that it uses a variety of robust, physical, technical organizational and administrative safeguards to protect its customers data from unauthorized access, loss or alteration;

(b) representing that it uses industry-accepted database and network technologies to encrypt and protect consumer data stored on its database system, transmitted within its network, to partner networks or third party providers;

(c) representing that it maintains a robust information security program that drives compliance with data protection standards;

(d) representing that customers can move, copy and/or transfer personal data from its data base to another IT environment in a safe and secure way without affecting its usability;

(e) representing that its personal data transfers are compliant with applicable data protection laws of third countries; and

(f) representing that its third party vendors who process personal data on its behalf have adequate computer systems and data security practices to safeguard the Plaintiff's and Class Members' PII and financial information.

63. The Defendant stored the Plaintiff's and Class Members' PII and financial information in its computer data system. The Defendant represented to the Plaintiff and Class Members that its computer data system was secure and their PII and financial information would remain private and protected.

64. The Defendant knew, or ought to have known, that it did not employ reasonable measures to keep the Plaintiff's' and Class Members' PII and financial information secure and prevent the loss or misuse of that information.

65. The Defendant's deceptive acts and/or business practices induced the Plaintiff and Class Members to provide their PII and financial information for the purpose of acquiring money transfer services from the Defendant. But for these deceptive acts and/or business practices, the Plaintiff and Class Members would not have provided their PII and financial information to the Defendant.

66. The Defendant's Representations that it would safeguard and protect the Plaintiff's and Class Members' PII and financial information in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to acquire the Defendant's money transfer services.

67. The Plaintiff and Class Members were harmed as the result of Defendant's breaches of the Applicable Consumer Protection Legislation because their PII and financial information was accessed, compromised and/or stolen, placing them at a greater risk of identity theft and their PII and financial information was disclosed to unauthorized third parties without their consent.

68. The Plaintiff and Class Members have suffered loss or damage as a result of the Defendant's failure to adequately safeguard, protect, secure and/or maintain the Plaintiff's and Class Members' PII and financial information.

i. British Columbia

69. The Defendant's provision of money transfer services were "consumer transactions" within the meaning of the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2 ("*BPCPA*").

70. With respect to those transactions, the Plaintiff and Class Members who purchased and/or used money transfer services are "consumers" and the Defendants were "suppliers" within the meaning of the *BPCPA*. The Defendant is considered to be a "supplier" as defined in section 1 of the *BPCPA* because in the course of business, the Defendant supplied a service to the Class and solicited, offered, advertised and promoted with respect to the consumer transaction between the Class Members and the Defendant.

71. By misrepresenting to the Plaintiff and the Class Members that their PII and financial information would be safe, secure and adequately protected, the Defendant breached s. 5(1) of the *BPCPA*.

72. The Defendant's conduct had the effect of deceiving or misleading consumers as to the safety and security of their PII and financial information.

73. As a result of the Defendant's conduct, the Plaintiff and the Class Members have suffered loss of their PII and financial information and damages related to that loss. The Plaintiff seeks injunctive relief, declaratory relief, damages and statutory compensation pursuant to ss. 171 and 172 of the *BPCPA* on his own behalf and on behalf of Class Members who purchased the Defendant's money transfer services in Canada. Such relief includes the disgorgement of the profits or revenues received by the Defendant from the sale of its money transfer services in Canada and a refund of the transaction fees paid by the Class Members.

74. The Class Members suffered damage and/or loss due to the deceptive acts or practices and unconscionable acts or practices of the Defendant, and as such are entitled to damages pursuant to section 171 of the *BPCPA*, including disgorgement.

75. The Class Members are entitled to a declaration that the Defendant's acts or practices contravened the *BPCPA*, and that the Defendant restore the monies paid by the Class Members to the Defendant as a result of its contravention of the *BPCPA,* pursuant to section 172 of the *BPCPA.*

76. The Class Members are entitled, to the extent necessary and pursuant to section 173(3) of the *BPCPA*, to a waiver of any notice requirements under the *BPCPA*, or alternatively, that the within action should proceed irrespective of any notice being served pursuant to the *BPCPA*.

ii. Alberta

77. The Class Members in Alberta who contracted for money transfer services for personal, family, or household purposes are "consumers", as defined in section 1(1) of the *Consumer Protection Act*, R.S.A. 2000 c. C-26.3 (*"ACPA"*).

78. The Defendant is a "supplier" as defined in section 1(1) of the *ACPA*. In the course of business, the Defendant sold or otherwise provided money transfer services to the Class Members.

79. The Representations made by the Defendant were unfair practices and deceived or misled, or might reasonably have deceived or misled, the Class Members, pursuant to section 6 of the *ACPA*.

80. The Representations were made on or before the Class Members entered into the contracts or agreements to purchase the money transfer services, for the purposes of section 7 of the *ACPA*.

81. The Class Members suffered damage and/or loss due to the unfair business practices of the Defendant, and as such are entitled to damages pursuant to sections 7(1),(3), and 13 of the *ACPA*, including disgorgement.

82. The Class Members are entitled to repayment by the Defendant of transfer fees paid for the

money transfer services, pursuant to sections 7(1),(3), and 13 of the *ACPA*.

83. The Class Members are further entitled to exemplary or punitive damages because the Defendant engaged in a policy or practice of distributing, marketing, and selling the money transfer services while aware of the deficiencies in its privacy protections, as pleaded above, pursuant to sections 7.2(1) and 13 of the *ACPA*.

84. The Class Members are entitled, to the extent necessary and pursuant to section 7.2(3) of the *ACPA*, to a waiver of any notice requirements under the *ACPA*.

iii. Saskatchewan

85. The Class Members in Saskatchewan who contracted for money transfer services for personal, family, or household purposes are "consumers", as defined in section 2 of the *Consumer Protection and Business Practices Act*, SS 2014, c C-30.2 ("*CPBPA*").

86. The Defendant is a "supplier" as defined in section 2 the *CPBPA*. In the course of business, the Defendant sold or otherwise provided money transfer services to the Class Members.

87. The Representations made by the Defendant were deceiving or misleading or false claims, pursuant to sections 6 and 7 the *CPBPA*.

88. The Representations were made on or before the Class Members entered into the contracts agreements to purchase money transfer services, for the purposes of section 9 of the *CPBPA*.

89. The Class Members suffered damage and/or loss due to the unfair business practices of the Defendant, and as such are entitled to damages pursuant to section 93(1)(b) of the *CPBPA*, including disgorgement.

90. The Class Members are entitled to a repayment by the Defendant of the transfer fees paid by the Class Members for the money transfer services, pursuant to section 93(1)(a) of the *CPBPA*.

91. The Class Members are further entitled to exemplary or punitive damages, pursuant to sections 93(1(b) and (2) of the *CPBPA*, because the Defendant engaged in a policy or practice of distributing, marketing, and selling its money transfer services while aware of the deficiencies in the protection of private information, as pleaded above, and as such did not take reasonable precautions or exercise due diligence.

iv. Manitoba

92. The Class Members in Manitoba who contracted for money transfer services for personal, family, or household purposes are "consumers" as defined in section 1 of the *Business Practices Act,* C.C.S.M. c. B120 ("*BPA*").

93. The Defendant is a "supplier" as defined in section 1 of the *BPA*. In the course of business, the Defendant sold or otherwise provided money transfer services to the Class Members.

94. The Representations made by the Defendant were deceiving or misleading, pursuant to section 2 of the *BPA*.

95. The Representations were made on or before the Class Members entered into the contracts agreements to purchase the money transfer services, for the purposes of section 7 of the *BPA*.

96. The Class Members suffered damage and/or loss due to the unfair business practices of the Defendant, and as such are entitled to damages pursuant to section 23(2) of the *BPA*, including disgorgement.

97. The Class Members are entitled to a repayment by the Defendant of the transfer fees paid by the Class Members for the money transfer services, pursuant to section 23(2) of the *BPA*.

98. The Class Members are further entitled to exemplary or punitive damages because the Defendant engaged in a policy or practice of distributing, marketing, and selling the money transfer services while aware of the deficiencies in its privacy protections, as pleaded

above, pursuant to section 23(4) of the *BPA*.

v. Ontario

99. The Class Members in Ontario who contracted for money transfer services for personal, family, or household purposes are "consumers", as defined in section 1 of the *Consumer Protection Act*, 2002, S.O. 2002, c.30 ("*CPA*").

100. The Defendant is a "supplier" as defined in section 1 of the *CPA*. In the course of business, the Defendant sold or otherwise provided money transfer services to the Class Members.

101. The Representations were false, misleading or deceptive and constituted an unfair practice under section 14 of the *CPA*.

102. The Representations were made on or before the Plaintiff and other Class Members entered into the agreements to purchase the money transfer services, for the purposes of section 18 of the *CPA*.

103. The Class Members suffered damage and/or loss due to the unfair business practices of the Defendant, and as such are entitled to damages pursuant to section 18 of the *CPA*, including disgorgement.

104. The Class Members are entitled to a repayment by the Defendant of the transfer fees paid by the Class Members for the money transfer services, pursuant to section 18 of the *CPA*.

105. The Class Members are further entitled to exemplary or punitive damages because the Defendant engaged in a policy or practice of distributing, marketing, and selling the money transfer services while aware of the deficiencies in its privacy protections, as pleaded above, pursuant to section 18 of the *CPA*.

106. The Class Members are entitled, to the extent necessary and pursuant to section 18(15) of *CPA,* to a waiver of any notice requirements under the *CPA* particularly as the Defendant concealed the actual state of affairs from Class Members.

vi. Newfoundland and Labrador

107. The Class Members in Newfoundland and Labrador who contracted for money transfer services for personal, family, or household purposes are "consumers", as defined in section 2 of the *Consumer Protection and Business Practices Act*, SNL 2009, C-31.1 ("*NFLD CPBPA*").

108. The Defendant is a "supplier", as defined in section 2 of the *NFLD CPBPA*. In the course of business, the Defendant provided money transfer services to the Class Members. The Defendant engaged in a consumer transaction with the Class Members for the provision of those services.

109. The Representations made by the Defendant were deceiving or misleading, pursuant to section 7 of the *NFLD CPBPA* and constitute unconscionable acts or practices, as defined in section 8 of the *NFLD CPBPA*.

110. The Representations were made on or before the Class Members entered into the agreements to receive the money transfer services, for the purposes of section 7(2) of the *NFLD CPBPA*.

111. The Class Members suffered damage and/or loss due to the unfair business practices of the Defendant, and as such are entitled to damages, including disgorgement, and repayment by the Defendant of the transfer fees paid by the Class Members for the money transfer services pursuant to section 10 of the *NFLD CPBPA.*

112. The Class Members are further entitled to exemplary or punitive damages because the Defendant engaged in a policy or practice of distributing, marketing, and selling the money transfer services while aware of the deficiencies in its privacy protections, as pleaded above, pursuant to section 10, pursuant to section 10 of the *NFLD CPBPA*.

vii. Prince Edward Island

113. The Class Members in Prince Edward Island who purchased the money transfer services

for personal, family, or household purposes, and not acting in the course of carrying on business, are "consumers", as defined in section 1 of the *Business Practices Act*, R.S.P.E.I. 1988, c B-7 ("*PEI BPA*").

114. The Representations made by the Defendant were false, misleading, or deceptive consumer representations, pursuant to section 2(a) of the *PEI BPA* and constituted unconscionable consumer representations, as defined in section 2(b) the *PEI BPA.*

115. The Representations were consumer representations, as defined in section 1 of the *PEI BPA*, because they were made by the Defendant in the course of business with a respect to supplying money transfer services to the Class Members, or made for the purpose of or with a view to receiving consideration for the money transfer services.

116. The Representations were made before the Class Members entered into the agreements to obtain the money transfer services, for the purposes of section 4 of the *PEI BPA.*

117. The Class Members suffered damage and/or loss due to the unfair business practices of the Defendant.

118. Since rescission is no longer possible, Class Members are entitled to damages, including disgorgement, and/or recovery of the transaction fees which Class Members paid under the money transfer services agreement in excess of the fair value of the services, pursuant to section 4(1) of the *PEI BPA*.

119. The Class Members are further entitled to exemplary or punitive damages because the Defendant's unfair practices constituted unconscionable consumer representations, as pleaded above, pursuant to section 4(2) of the *PEI BPA*.

Violation of *PIPEDA*

120. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

121. The Defendant provided financial services to the public through electronic communications, namely, the use of wire, electromagnetic, photo-optical or photo-electric facilities for the transmission of wire or electronic communications received from and on behalf of customers.

122. *PIPEDA* contains provisions that provide customers of entities providing electronic communication services to the public with redress if a company mishandles their electronically stored information.

123. The Data Breach was the result of the Defendant's failure to implement safeguards appropriate to the extreme sensitivity of customers PII and financial information in breach of *PIPEDA*.

124. The Defendant failed to designate the appropriate individuals who were responsible and accountable for its computer data system security management, including compliance with its internal policies and reasonable industry standards in its collection, storage, protection and destruction of customer PII and financial information, contrary to section 4.1 of Schedule 1 of *PIPEDA*.

125. The Defendant allowed the PII and financial information of the Plaintiff and Class Members to be used and disclosed for purposes other than those for which it was collected contrary to section 4.5 of Schedule 1 of *PIPEDA*.

126. The Defendant failed to implement appropriate organizational and technological safeguards to protect the PII and financial information of the Plaintiff and Class Members against loss, theft, unauthorized access, disclosure, copying, use and/or notification contrary to section 4.7 of Schedule 1 of *PIPEDA*.

127. As a result of the Defendant's conduct and violations of sections 4.1, 4.5 and 4.7 of Schedule 1 of *PIPEDA*, the Plaintiff and Class Members have suffered injuries, including various forms of identity theft, lost money and the costs associated with the need for credit monitoring to protect against additional identity theft. The Plaintiff and Class Members seek the maximum statutory damages available under *PIPEDA* in addition to the cost for credit

monitoring services.

Plaintiff's(s') address for service:

Dusevic & Garcha
Barristers & Solicitors
#210 - 4603 Kingsway
Burnaby, BC V5H 4M4
Canada

Fax number address for service (if any):

604-436-3302

E-mail address for service (if any):

ksgarcha@dusevicgarchalaw.ca

Place of trial:

Vancouver, BC
Canada

The address of the registry is:

800 Smithe Street
Vancouver, BC V6Z 2E1
Canada

Dated: October 28, 2024.

Signature of K.S. Garcha
lawyer for Plaintiff(s)

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act* R.S.B.C. 2003 c.28 (the *"CJPTA"*) in respect of the Defendant. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to sections 10 (e)(I), (g) and (h) of the *CJPTA* because this proceeding:

(e)(I) concerns contractual obligations, which to a substantial extent, were to be performed in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia.

APPENDIX

[The following information is provided for data collection purposes only and is of no legal effect.]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a proposed multi-jurisdictional class proceeding brought on behalf of the Plaintiff and all persons resident in Canada, except the Province of Quebec, whose personal and financial information was accessed, compromised and/or stolen from the Defendant's computer data system following a data breach by unauthorized third persons.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:
[ ] motor vehicle accident
[ ] medical malpractice
[ ] another cause

A dispute concerning:
[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] personal property
[ ] the provision of goods or services or other general commercial matters
[ ] investment losses
[ ] the lending of money
[ ] an employment relationship
[ ] a will or other issues concerning the probate of an estate
[x] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[x] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws
[ ] none of the above
[ ] do not know
x] a matter not listed here

Part 4:

1. *Class Proceedings Act*, R.S.B.C. 1996, c.50;
2. *Court Jurisdiction and Proceedings Transfer Act* R.S.B.C. 2003 c.28;
3. *Privacy Act*, R.S.B.C. 1996, c.373, *The Privacy Act*, R.S.S. 1978, c. P-24, *The Privacy Act*, C.C.S.M. c. P125, *Privacy Act*, R.S. N.L. 1990, c-P-22;
4. *Business Practices and Consumer Protection Act*, S.B.C. 2004, *Fair Trading Act*, R.S.A. 2000, c. F2, *Consumer Protection and Business Practices Act*, S.S. 2014, c.C-30.2, *Business Practices Act, C.C.S.M.* c. B1230, *Consumer* Protection and Business Practices Act, S.N.L. 2009, c. C-31.1 and *Business Practices* Act, R.S.P.E.I. 1988, c.B-7;
5. *Negligence Act,* R.S.B.C. 1996, c.333;
6. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5;
7. *Court Order Interest Act*, R.S.B.C., c. 79;