Electronically issued
Délivré par voie électronique : 08-Feb-2021
London

Court File No./N° du dossier du greffe: CV-21-00000241-00CP

Court File No.:

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

THERESA ORIET

Plaintiff

- and -

AGRONOMY COMPANY OF CANADA LTD. and SOLLIO AGRICULTURE L.P.

Defendants

PROCEEDING UNDER THE *CLASS PROCEEDINGS ACT, 1992*, SO 1992, c. 6

STATEMENT OF CLAIM

TO THE DEFENDANTS

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiff. The claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a statement of defence in Form 18A prescribed by the *Rules of Civil Procedure*, serve it on the Plaintiff' lawyer or, where the Plaintiff does not have a lawyer, serve it on the Plaintiff, and file it, with proof of service, in this court office, **WITHIN TWENTY DAYS** after this statement of claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your statement of defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a statement of defence, you may serve and file a notice of intent to defend in Form 18B prescribed by the *Rules of Civil Procedure*. This will entitle you to ten more days within which to serve and file your statement of defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU.

If you wish to defend this proceeding but are unable to pay legal fees, legal aid may be available to you by contacting a local legal aid office.

Date: Issued by: _____

Local Registrar

Superior Court of Justice
80 Dundas Street
London, Ontario

TO: **AGRONOMY COMPANY OF CANADA LTD.**
200-9001 Boulevard de l'Acadie
Montréal, Québec H4N 3H7
Canada

AND TO: **SOLLIO AGRICULTURE L.P.**
200-9001 Boulevard de l'Acadie
Montréal, Québec H4N 3H7
Canada

THE RELIEF CLAIMED

1. **THE PLAINTIFF CLAIMS** on her own behalf and on behalf of the Class:

   a. an order pursuant to the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 (the "*CPA*") certifying this action as a class proceeding and appointing the Plaintiff as the representative plaintiff;

   b. a declaration that the defendants owed a duty of care to the Plaintiff and the Class Members and breached the duty of care owed to them, and that, as a result, the Class Members incurred losses and/or damages;

   c. a declaration that the defendants intentionally or recklessly and without lawful justification intruded upon the seclusion of the Plaintiff and the Class Members in a way that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish, or alternatively, are jointly and severally liable for intruding upon the seclusion of the Plaintiff and the Class Members;

   d. with respect to the Class Members who are residents of the Province of Québec, a declaration that the defendants violated articles 3 and 35-37 of the *Civil Code of Québec,* CQLR c CCQ-1991 (the "*CCQ*"), section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12 (the "*Québec Charter*"), and section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1 (the "*PPIPS*"), each as amended;

   e. damages calculated on an aggregate basis or otherwise, in an amount sufficient to compensate the Plaintiff and the Class Members for the harm done to them as a result of the defendants' unlawful conduct, including breach of the *CCQ*, *Québec Charter*, *PPIPS,* negligence, and intrusion upon seclusion;

f. punitive and exemplary damages in an amount to be determined at trial;

g. an equitable rate of interest on all sums found due and owing to the Plaintiff and the Class Members or, in the alternative, pre- and post-judgment interest pursuant to the *Courts of Justice Act,* R.S.O. 1980, c. 43 (the "*CJA*");

h. costs of the notice to Class Members and administration pertaining to a plan of distribution;

i. costs of this action on a substantial indemnity basis; and

j. such further and other relief as this Honourable Court deems just.

THE NATURE OF THE CLAIM

2. This action concerns the excessive collection and unlawful disclosure by the defendants Sollio Agriculture L.P. ("Sollio AG") and their partner the Agronomy Company of Canada Ltd. ("Agromart") of sensitive personal and financial information from thousands of Canadian farmers and their farming operations.

3. The data collected included crucially sensitive personal data such as Social Insurance Numbers ("SIN"), personal net worth statements, driver's license numbers, dates of birth, specific banking and borrowing information including bank account numbers and credit card numbers, among other data. That same data was unlawfully and negligently retained, stored and managed by the defendants, leaving it ripe for exfiltration by fraudulent third parties.

4. The defendants collected and kept sensitive and valuable personal information from their customers. Having done so, they were responsible to safeguard it against unauthorized use, abuse or theft. As such, they are required to establish robust security policies,

procedures and practices to prevent, detect and diligently respond to cybersecurity incidents.

5. The defendants failed to comply with their duties. They employed no or wholly substandard security measures that were inappropriate relative to the importance and sensitivity of the class members' personal information. The defendants failed to act to address known or knowable vulnerabilities in their cyber security systems.

6. As a result of the defendants' failures, at some time on or about May 27, 2020 the class members' data was accessed and exploited by hackers. The hackers demanded undisclosed amounts of money from Agromart and/or Sollio AG as a ransom in exchange for the hackers refraining from posting or selling the data online. The defendants did not accede to the hacker's demands. Thereafter, the personal information of the class, including Mrs. Oriet, was auctioned off to bidders on the dark web.

7. Acquirers of the class members' data made prompt use of the information, conducting fraudulent transactions, accessing class members' bank accounts, or stealing their identities. The plaintiff's experience of multiple fraudulent transactions on her visa credit cards in the months following the data breach highlight the swift and effective actions of the purchasers of the data and the ongoing threat that class members will face for the foreseeable future.

8. As will be further detailed below, the failures of the defendants are shocking and raise grave privacy and security concerns, in that they:

    a. failed to obtain appreciable consent from the class members at the time of the collection of their sensitive personal information;

b. failed to have in place sufficient or any file encryption, backup storage, or other security infrastructure protections to prevent unauthorized access to or exfiltration of the class members' sensitive personal information;

c. failed to have in place sufficient or any firewall, antivirus, malware, or other ransomware detection systems that would detect the breach as it was attempted or as it occurred;

d. failed to adequately limit, contain and respond to the breach once known; and,

e. failed to give class members responsible, prompt, and generous notification of the breach and the risks to their personal information, identity, and the likelihood of fraud.

9. As a result of the defendants' actions, the personal information of thousands of Canadian farmers and their farming operations have been compromised, sold and disseminated on the dark web, from which they have suffered loss and damage.

THE PARTIES

The Plaintiff and the Class

10. The plaintiff, Theresa Oriet, (the "Plaintiff") is an individual resident in the town of St. Joachim, in the Province of Ontario. Mrs. Oriet is a farmer and a Director and the Chief Financial Officer of Oriet Farms Limited ("Oriet Farms"), a private farming corporation headquartered in St. Joachim, Ontario.

11. Mrs. Oriet completed an Agromart Credit Application and Agreement (the "Application") to purchase crop inputs from the defendant Agromart on November 1, 2018. The Application requested details of the Plaintiff's personal information, including: her address, phone

number, email address, SIN, driver's license number, birthdate, spouse's birthdate and spouse's driver's license number.

12. The Plaintiff seeks to represent a class consisting of all persons residing in Canada whose Personal Information was stored on the System in control of the defendants that was compromised or accessed in the Breach (the "Class", or "Class Members"), where:

    a. "Breach" means the events, culminating on or about May 27, 2020, whereby third-party hackers accessed, collected and exfiltrated information stored on the defendants' System;

    b. "Personal Information" means information about an identifiable individual and includes financial information; and,

    c. "System" means the centralized information technology database operated, maintained, monitored and secured by the defendants.

The Defendants

13. The defendant Agromart is an agricultural inputs supply company incorporated and registered pursuant to the laws of Nova Scotia. Agromart conducts business across Eastern Canada under the tradename "Agromart Group" and maintains corporate offices in Montréal, Québec and Belton, Ontario. The Agromart Group is comprised of over 20 franchised or partnership retailer entities (the "Retailers") that act as agents of Agromart and its partner Sollio AG to sell the defendants' crop input supplies to local farmers. Agromart is a consolidated subsidiary of the Sollio Cooperative Group, formerly known as La Coop Fédérée.

14. Sollio AG is a corporation incorporated pursuant to the laws of Québec with its primary office in Montréal, Québec. Sollio AG is the agri-business division of Sollio Cooperative

Group and its partner, as well as the partner of Agromart. Sollio AG operates in the industries of livestock production, crop production, and grain transportation and storage.

15. Agromart, Sollio AG and the Retailers collectively utilize standard form agreements to collect personal information from farmers. They also utilize a centralized information technology (IT) System, wherein the Retailers collect and input the Personal Information of the Class Members into the System, which is maintained, electronically stored, monitored and secured by the defendants.

16. The collection of Personal Information is a requirement for the provision of services with the defendants at the time the farmer enters into an agreement with the defendants directly or through one of their Retailer agents. The defendants further collect Personal Information during, in the course of or as a consequence of its relationship with their customers.

17. The Plaintiff pleads that by virtue of the acts and omissions described throughout this claim, the defendants are liable in damages to the Plaintiff and to the Class Members and that each defendant is responsible for the acts and omissions of the other defendant and its employees and/or agents for the following reasons, among others:

    a. each defendant was the agent of the other in sourcing and originating relationships and agreements with customers;

    b. each defendants' business was operated so that it was inextricably interwoven with the business of the other; and

    c. the defendants maintained common senior executive leadership personnel, common corporate headquarters, common physical premises and facilities

and a centralized IT System in which the Class Members' Personal Information was stored and disclosed.

Third-Party Hackers

18. REvil, or Sodinokibi (the "Hackers") are a group of fraudsters known for their tactics of employing their ransomware-as-a-service to extract large payouts from institutions that collect and store valuable, sensitive and/or personal information. They target vulnerable computer systems, encrypt and/or exfiltrate the data and hold it hostage to their ransom demand. In the event of a failed ransom attempt, they are frequently known to sell the ransomed data on the dark web.

19. The Hackers employ common ransomware tactics, focusing on vulnerable systems, utilizing phishing campaigns, and "malvertising". These attacks are frequently publicized and high-profile.

20. The Hackers' attacks are frequent, widespread, and resulted in self-reported annual revenues exceeding USD $100 million. In part due to this frequent and public exposure, their *modus operandi* and the methods institutions can employ to prevent against their attacks constitute widespread knowledge. Their targeted exploits pose a clear, foreseeable and legitimate risk to all institutional holders of sensitive, financial, and other personal information.

21. The Plaintiff pleads that the Breach occurred as the direct result of the defendants' reckless and cavalier attitude towards the security of the System and confidentiality for the Class Members' Personal Information, which they proceeded with in the face of the risks known to them. Therefore, the intentional acts of the Hackers are the result of the intentional, willful, and/or reckless actions of the defendants, as plead below.

FACTUAL BACKGROUND

Collection of Personal Information

22. Sollio AG and Agromart's business in the retail of crop inputs occurs through their network of agent Retailers.

23. The defendants utilized a standard form Application document to collect the Class Members' Personal Information.

24. The Application contains a record of the details of the farming operation and the individual farmer(s). Among other information, it includes the following Personal Information:

    a. the farmer's name, birthdate, driver's license number, phone number and address;

    b. the farmer's spouse or co-applicant's name, birthdate, and driver's license number;

    c. the legal description of the farming property; and,

    d. the farm's additional business principals or partners' names, birthdates, SINs, phone numbers and addresses.

25. Significantly, and without lawful authority or disclosure to guide the Class Members' consent, the defendants collected the SINs of all applicants, their spouses, and co-applicants on the Application.

26. The Application also requests the financial information of the person or corporation applying for credit and corresponding information from their spouse or co-applicant. This includes their banking institution's name and branch location, savings and chequing account numbers, loan manager, phone number, and a list of major credit references.

27. The highly sensitive and personal information in the form of SINs, financial information, and Application details were stored in the System alongside additional information the defendants collected from the Class Members, which included credit card information, credit scores, assets, outstanding loans, and personal net worth statements.

28. For example, the defendants' collection of the personal net worth statements of their customers included highly sensitive details of the Class Members' business and personal lives. Among other details, these forms detailed line-by-line the significant assets, liabilities, investments, account balances, loans, mortgages and hypothecs of the farmers, exposing the exact value of their business operations.

29. The Application does not contain any statement or other information concerning the purposes for which the Personal Information is being collected, the Class Members' consent to the purposes of the collection of the Personal Information, the uses that will be made of the Personal Information, or any information concerning the retention and protection of the Personal Information. The defendants do not otherwise have a publicly available privacy policy.

30. All of the Personal Information collected, stored, and ultimately disclosed by the defendants was, and is, extremely sensitive financial and personal information of the Class Members. Due to the nature of the Personal Information collected and the defendants' complete lack of, or alternatively, sufficiency of, a privacy or retention policy, System encryption, and/or System security, this collection was objectively unreasonable and intruded on the reasonably expected privacy of the Class Members at the time it was collected.

31. This objectively unreasonable collection was colored by the defendants' complete lack of appreciable consent from the Class Members to the intrusive collection of highly sensitive Personal Information.

32. As a result, troves of the Class Members' Personal Information were stored together in a readily accessible System that afforded minimal, if any, protections over the Class Members' Personal Information, and was subsequently disclosed in the Breach, from which the Class Members suffered loss.

The Breach

33. Culminating on or about May 27, 2020, the Hackers accessed and exfiltrated data from the defendants' System.

34. At some point on or after May 27, 2020, the Hackers demanded a ransom from Agromart and/or Sollio AG to prevent the public listing and auctioning of the information encrypted and/or exfiltrated in the Breach. The defendants were given an undisclosed deadline to cooperate with the Hackers demands or have the significant, financial and Personal Information of the Class Members auctioned off on the dark web.

35. The defendants declined to cooperate with the Hacker's demands.

36. Between May 27 and June 2, 2020, the defendants made no attempt to inform the Class Members of the Breach, their decision not to cooperate with the ransom demand, that their highly sensitive Personal Information was at risk of disclosure and sale on the dark web, or that the Class Members should be taking active steps to protect and preserve their Personal Information.

37. On June 2, 2020, the Hackers notified a data breach blogger who disclosed that the Hackers would be posting the information exfiltrated in the Breach online because

Agromart refused to pay their ransom. The Hackers released a link to "auction" off the Breach data, which they described as:

> "all files of actual information from the last three months. Also in the archive you will get several databases that are no less interesting. Archive in zip format 1. Files pdf,docx,xlsx – 22328 2. Database – 3 When the auction is over, you will be provided with a download link from the cloud with the following deletion."

38. This statement of the Hackers suggests that the Breach disclosed, in addition to all transactional and other data from the preceding three months, an archive of 22,328 files, including sensitive Class Member account documents and financial information, and 3 databases listing the personal and sensitive financial information of Class Members and Agromart franchises (the "Data").

39. In the same posting, the Hackers announced that the Data would remain available for purchase via auction for seven (7) days. The Hackers announced a minimum deposit of $5,000 USD, a starting bid of $50,000 USD, and a $100,000 USD "blitz price" for the entire lot of Data (the "Auction").

40. The Hackers posted samples of the type of information available in the Data set. This included a number of Class Member Applications, the personal net worth statement of a Class Member, internal financial documents, and senior Agromart and Sollio AG employees' internal emails and notes detailing their response to the attack. Included in these internal email examples was an email to David Brand, general manager of Agromart and Sollio AG, the morning of June 2, 2020. Therefore, at the very least, the Hackers had control over and/or access to Agromart's electronic files in the System between May 27 and June 2, 2020.

41. As a result of Agromart's security failures and ineffectual handling of the Breach, the Personal Information of the Plaintiff and the Class Members was made available for

purchase in the Auction by ill-intentioned parties on or about June 2, 2020, and remained available until approximately June 9, 2020.

42. Further to the Hacker's threat, and in validation of their demands, the Data, including the Plaintiff and Class Members' Personal Information, was purchased and/or disclosed in the Auction.

The Aftermath

43. The Class Members did not receive timely notice of the Breach after it occurred.

44. In addition to the period between May 27 and June 2, 2020 during which the defendants were debating acceding to the Hackers' demands, in the approximately seven (7) days that the Data was available for purchase in the Auction by the highest criminal bidder on the dark web the defendants likewise made no attempts to notify the Class Members of the Breach.

45. Further, following the Breach the defendants issued no public statements or press releases to alert the public or their customers of the Breach.

46. Significantly, this lack of disclosure increased the foreseeable and ultimate harm suffered by the Class Members. The sale of their Personal Information, and the immediate steps Class Members needed to take to prevent significant harm, was preventable and/or could have been attenuated during the period between May 27 and approximately June 9, 2020.

47. Agromart, Sollio AG and the Retailers had in their possession, physically and/or electronically, all relevant contact information for the Class Members. It was well within the capacity of the defendants to contact the Class Members through their network of agents using the email addresses and/or telephone numbers collected in the Applications or otherwise. The defendants failed to mobilize any effective system to reach out to the

members of the Class during this critical period during and immediately following the Breach.

48. Agromart acknowledged the Breach publicly for the first and only time in an interview published June 23, 2020 in Farmtario, a farming periodical (the "Article"). The Article was not distributed directly to the Class Members.

49. David Brand was interviewed by Farmtario for the Article. Brand stated: "Agromart customers were contacted about the data breach and have been offered a year of monitoring of credit from Equifax at no cost," and further that "the investigation is well advanced, and we are confident that the scope of the event is minor".

50. Brand's statements were inaccurate. Class Members, including the Plaintiff, were unaware the Breach had occurred and had not been provided notice that the Breach had compromised their Personal Information. Further, Brand's own emails from June 2, 2020 were exposed by the Hackers, exemplifying the invasive scope, duration and severity of the Breach. Contrary to Brand's statements, the scope of the Breach and subsequent sale and disclosure of the Data was, and remains, significant.

51. Therefore, despite the defendants' knowledge by at least June 2 that they were dealing with professional hackers and that the Data would be sold to bidders on the dark web, they continued to act in the face of the risks to the Class Members, made no attempt to notify them despite having their contact information in their possession, and only provided minimal, and inaccurate, disclosure in the Article.

52. When the defendants finally did provide notice to Class Members including the Plaintiff, it was devoid of explanation for the delay and wholly deficient at explaining the severity of the Breach.

53. The defendants sent out standard-form notices (the "Notices") to members of the Class at staggered intervals throughout the summer of 2020. Rather than provide the affected farmers with timely and thorough disclosure of the relevant facts of the Breach, the defendants made no effort to notify the Class of the Breach until after their Personal Information was auctioned off on the dark web and/or disclosed by the Hackers.

54. Consistent with the defendants' tactic of downplaying the significance of the Breach, and regardless of being sent months apart, the Notices contained consistent language to the effect that the defendants "recently learned that, on or about May 27, 2020, an unauthorized individual accessed some parts of the Agromart Group's IT system." In fact, the defendants had known of the Breach since May, and its severe consequences since at least June 2, and made no attempt to explain this delay.

55. Further, the Notices provided limited and insufficient details of the Breach and the defendants' response to it. The defendants failed to disclose what steps they had taken to remediate the Breach and to update the security of their System to avoid any future privacy breaches, merely stating: "necessary measures were taken immediately to block the unauthorized access and to try to prevent such incidents in the future", and that they "acted quickly to secure the system."

56. In addition to being entirely inadequate and unresponsive to the flaws of the defendants' System, these statements were patently false and misleading. As set out above, the System was left vulnerable for an extended period during which time the Hackers were able to gain access and maintain control over the System. Between at least May 27 and June 2, 2020, the defendants knew of the Breach and failed to take any substantial steps to block the unauthorized access. Further, the defendants failed to provide any notice to the Class Members during this period and the seven (7) days thereafter during which time their Personal Information was available for auction on the dark web.

57. Mrs. Oriet did not receive direct notice of the Breach until provided with a letter sent by regular mail dated July 3 and postmarked July 7, 2020. Her spouse did not receive direct notice of the Breach until provided a letter also sent by regular mail dated August 27, 2020. The defendants therefore waited over one month to notify the Plaintiff, and over three months to notify her spouse that their Personal Information was compromised in the Breach.

58. The defendants' failure to provide timely notice of the Breach and the extensive amount of time they allowed to elapse before providing notice to the Class Members exacerbated the risks and dangers to the Class arising from them having been the victims of a privacy breach from known cyber criminals such as the Hackers.

59. The extent of the public disclosure of the Breach was contained in the June 23, 2020 Farmtario Article, and the only disclosure to members of the Class was made in the Notice, both of which were incomplete and inaccurate.

60. The defendants have reported the Breach to the Office of the Privacy Commissioner of Canada, which has not yet made public the results, if any, of their investigation.

61. The defendants' response to the Breach has been entirely inadequate and unresponsive to the risks, embarrassment, humiliation, distress, anxiety, financial damage and expenses to which it has exposed the Plaintiff and the Class Members.

The Harm

62. On or about July 13, 2020, approximately three weeks after the publication of the Article and seven weeks after the Breach occurred, Mrs. Oriet received the Notice, advising her that her Personal Information had been accessed in the Breach. In addition to the information set out in the preceding section, the Notice disclosed that her, "name, personal

address, name of co-applicant, SIN, birth date, driver's license number and e-mail address" were disclosed to unauthorized third parties.

63. Mrs. Oriet was shocked and distressed to learn that the Breach had occurred, and that, over a month after the fact, the defendants had not informed her that her Personal Information had been accessed, stolen and compromised.

64. Mrs. Oriet responded swiftly upon being notified of the Breach. Immediately upon receiving the Notice, she reviewed her banking statements for signs of fraudulent activity. As a result of her investigation, Mrs. Oriet discovered fraudulent activity on she and her husband's jointly held US Dollar Canadian credit card (the "Visa"). The activity discovered by Mrs. Oriet includes:

    a. an unknown transaction of $213.99 processed on July 7, 2020 to the Visa at BestBuy.com. Mrs. Oriet immediately reported the fraudulent transaction to her bank upon becoming aware of it on or about July 13, 2020. As a result of her proactive review and reporting, the charges were reversed by BestBuy.com on July 14, 2020; and,

    b. an unknown transaction of $213.99 processed on July 14, 2020 to the Visa at BestBuy.com. Due to her monitoring of her accounts, Mrs. Oriet caught the fraudulent charges and immediately reported them to her bank. The second set of charges were reversed by BestBuy.com on July 16, 2020;

(together, the "Fraudulent Activity").

65. Mrs. Oriet reported the Fraudulent Activity to the Ontario Provincial Police ("OPP"). The OPP advised that, since the Fraudulent Activity occurred in the USA on a US website, they were unable to assist with any investigation into the fraudulent charges.

66. Thereafter, Mrs. Oriet spent approximately one week responding to the Fraudulent Activity and changing as much of her Personal Information implicated in the Breach as possible. This included, *inter alia*:

    a. notifying all of her banks of the Breach and the Fraudulent Activity;

    b. notifying the Canada Revenue Agency of the Breach and the Fraudulent Activity;

    c. removing her name from joint accounts held with her husband;

    d. cancelling the Visa implicated in the Fraudulent Activity;

    e. applying for new identity documents, including a SIN and driver's license;

    f. changing passwords for her online and banking accounts;

    g. creating a new e-mail account for Oriet Farms;

    h. notifying credit monitoring entities of the Breach; and,

    i. signing up for credit monitoring services.

67. Further, and significantly, in order to protect the financial assets of Oriet Farms, Mrs. Oriet removed her name and authority as signing officer on Oriet Farm's banking accounts, despite her role as Chief Financial Officer and Director of the corporation.

68. In a letter dated August 27, 2020, approximately three months after the Breach, Mrs. Oriet's husband received a Notice. This is despite his Personal Information having already been accessed and compromised, as exemplified by the Fraudulent Activity. Dr. Oriet was advised by the defendants that his "name, birth date, personal address and driver's license number" was disclosed in the Breach.

69. The Notice ultimately given to the Class or some portion thereof was wholly deficient and failed to adequately disclose to the Class Members the extent of the Breach, and the risk to the Class Members arising therefrom. Instead, the defendants downplayed the extent of the Breach and the risks to which they exposed the Class because of their reckless behavior towards protecting the Class Members' Personal Information and wholly deficient response to the Breach.

70. In addition to failing to disclose the details of the Breach, neither Agromart nor Sollio AG have created or implemented a publicly accessible privacy policy to date. As a result, and in spite of the Breach having occurred over eight months ago, the Plaintiff and the Class Members remain fully unaware of how their Personal Information is being stored, disclosed and secured in the defendants' System.

71. Beyond the actual harm suffered by the Plaintiff and the Class to date, individuals affected by privacy breaches by known cybercriminals such as the Hackers must expect to find themselves the target of attempted or actual identity theft or other fraud in the future. Crucial personal identifiers such as SINs and driver's license numbers in concert with the other banking and financial information form the ideal foundation for repeated forms of identity theft. They may end up subject to an increased volume of "phishing" attacks, where criminals pose as trustworthy sources and attempt to obtain other or updated personal information that might lead to further cyber security breaches, identity theft or other fraud.

72. Since the Data has been auctioned off on the dark web to fraudulent and/or criminal actors, and there is likely no way to prevent it from being re-sold or posted online at any time in the future, the risks associated with the Breach will continue on as credible threats for years. Further, the Data includes Personal Information such as SINs, which are assigned for life as fundamental personal identifiers. Because of their fundamental importance as a

personal identifier, SINs are not easily changed. The Plaintiff and the Class Members must therefore continuously monitor their accounts for fraudulent activity and will continue to suffer harm for the foreseeable future.

73. The defendants made a limited offer of one or two years of free credit protection services to individuals whose Personal Information was included in the Data (the "Offer"). The Offer provides no short-term or long-term protection or remedies to the Plaintiff and Class Members. Further, Class Members' associated businesses whose financial information was equally compromised in the Breach have not been offered any protection from the defendants, to the effect that they are completely exposed to criminal and fraudulent activity as a direct result of the Breach.

74. The Offer from the defendants is limited, in that it only provides some recourse for Class Members if damage has already been done during the limited timeframe.

75. Further, it is a well-established practice for hackers in data fraud cases such as the Breach to hold onto personal information for years, and to act on the fraud after the protections provided by limited credit protection plans, such as the Offer, have expired.

76. As a result, Class Members including the Plaintiff live with the risk that their Personal Information will be used by criminal actors, are broadly exposed to fraud and identity theft, and must actively monitor their financial and personal accounts for the foreseeable future. The Breach has therefore had an enormous and far reaching impact on the Class Members, the full extent of which is currently unknown.

CAUSES OF ACTION

Negligence

(i) The Duties of the Defendants

77. The defendants' duties were informed by its client agreements including the Application, its internal policies and procedures, privacy laws of Canada and industry practices.

78. The defendants owed the Plaintiff and the Class Members a duty at law to limit the collection of Personal Information, including highly sensitive financial and irreplaceable identifying information. Once collected, the defendants owed the Class Members a further duty to protect the Personal Information against unauthorized use, disclosure or theft commensurate with the sensitivity of the information. Upon becoming aware of the unauthorized use, disclosure or theft of the Personal Information, the defendants had a further duty to provide responsible, prompt, and generous notification to the Class.

79. To the extent that the defendants, or any of them, delegated any responsibility for collecting, storing, using, retaining, and/or disclosing the Class Members' Personal Information to any other party or parties, including the Retailers, the defendants are jointly and severally liable for resultant damages, because each party individually and as agent for the other held a non-delegable duty to secure the Class Members' Personal Information.

80. The defendants wholly failed in their duties to the Class as set out by the applicable standards below.

(ii) The Applicable Standards

81. The defendants' duties were included expressly or impliedly in its Applications and other agreements with the Class Members, and also informed by the defendants' duties at common law, which required that the defendants:

a. collect, store and manage the Class Members' Personal Information in accordance with all legislation and regulations governing the collection and disclosure of personal information;

b. store and manage the Class Members' Personal Information diligently and in accordance with established standards for the implementation of protocols, policies and procedures;

c. safeguard the Class Members' Personal Information in a manner commensurate with its sensitivity against unauthorized use, disclosure or theft; and

d. not disclose the Class Members' Personal Information to anyone without or in excess of their knowledge and informed consent, except in the limited and defined circumstances provided under the contracts between the parties.

82. Moreover, as an entity that collects, uses or discloses Personal Information in the course of commercial activities carried on in Canada, the defendants are subject to the *PIPEDA*, including Schedule 1 thereof which required, *inter alia*, the following:

a. section 4.1 of Schedule 1 required that the defendants be responsible and accountable for Personal Information and required the defendants to implement policies and practices to give effect to the principles concerning the protection of Personal Information;

b. section 4.2 of Schedule 1 required that the defendants identify the purposes for which that information was collected at the time or before Personal Information was collected;

c. section 4.3 of Schedule 1 required that the knowledge and consent of the Class Members were required for the collection, use or disclosure of Personal Information and that the defendants were required to make a reasonable

effort to ensure that the Class Members were advised of the purposes for which Personal Information was collected;

d. section 4.3.2 of Schedule 1 required that the Class Members' consent be "meaningful," requiring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed";

e. section 4.3.3 of Schedule 1 required that the defendants not require an individual to “consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes” of the collection;

f. sections 4.3.5 and 4.3.8 of Schedule 1 specified that Class Members' reasonable expectations were relevant to obtaining consent, and that the Class Members ought to have been afforded the opportunity, subject to legal or contractual restrictions and reasonable notice, to withdraw consent;

g. section 4.4 of Schedule 1 required that the defendants “not collect personal information indiscriminately”, and both the amount and type of information collected shall be limited to that which is necessary;

h. section 4.5 of Schedule 1 required that the defendants were not permitted to use or disclose the Class Members' Personal Information for any purposes other than those for which it was collected, except with the Class Members' consent;

i. section 4.7 of Schedule 1 required the defendants to protect the Class Members' Personal Information by security safeguards appropriate to the sensitivity of the Personal Information from unauthorized access, disclosure, copying or use;

j. section 4.7.2 required more sensitive information to be safeguarded by a higher level of protection by the defendants;

k. section 4.7.3 of Schedule 1 required the methods of protection of the Personal Information to include physical, organizational and technological measures, including the use of passwords and encryption; and,

l. section 4.8 of Schedule 1 required the defendants make readily available information about its policies and practices relating to the management of the Class Members' Personal Information.

83. Further, as corporations carrying on enterprises in Québec, the standard of care applicable to the defendants' collection, storage, use, retention, and/or disclosure of the Personal Information is informed by the requirements set out in the *PPIPS,* which required, *inter alia*, the following:

a. section 5 required the defendants to collect only the Personal Information necessary for the object of the collection;

b. section 6 required the defendants to collect the Personal Information directly from the individual concerned;

c. section 8 required the defendants to inform the Class Members of the object of the collection, the use to which it will be made, the categories of persons who will have access to it, and the place(s) where the Personal Information will be kept;

d. section 10 required the defendants to take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored;

e. section 13 prohibited the defendants from communicating, without consent, Personal Information to third parties for use inconsistent with the object of the collection;

f. section 14 required the defendants to obtain manifest, free, and enlightened consent to any disclosure of their Personal Information to third parties and/or unauthorized persons; and,

g. section 17 required that the defendants take all reasonable steps to ensure that the Personal Information would not be used for purposes irrelevant to the object of the file or communicated to third parties without consent.

84. The defendants' duties and responsibilities were also informed by industry practices. These industry practices are guided by the Government of Canada's *Social Insurance Number Code of Practice*, which sets out the private sector's responsibilities to the public, including the obligation to:

a. never ask for a customer's SIN unless legally required to collect it for income reporting purposes;

b. fully comply with *PIPEDA* in disclosing the purpose of collecting a SIN and obtaining consent, including stating clearly at the time of the request why the SIN is being requested and how it will be used;

c. advise clients they do not have to provide their SIN if they do not want to, and thereby cannot make clients provide their SIN as a condition for receiving a product or service;

d. protect their clients' personal information, including SINs, from theft and inappropriate use or disclosure;

e. take immediate steps to minimize the potential damage if customers' SINs are stolen or inappropriately used or disclosed; and,

f. only use the SIN for the disclosed purposes.

85. Further, the *Social Insurance Number Code of Practice* states that the practice of collecting SINs for "identification or client account number reasons, or to increase accuracy in credit bureau matching" is "strongly discouraged" in the private sector.

86. All of the above standards and statutory obligations are informed by the common-law principles for the collection, retention, use and disclosure of Personal Information as laid out by the Canadian Standards Association in the *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 (the "*Model Code*"). Specifically, the *Model Code* imposed the following minimum standards on the defendants at common law:

> "1. Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles;
>
> 2. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected;
>
> 3. Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate;
>
> 4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means;
>
> 5. Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes;
>
> 6. Accuracy: Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used;
>
> 7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information;
>
> 8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information; …"

87. At all times, the defendants were obliged to have effective, current and robust cyber security protective measures in place to secure all of the Personal Information which they

collected, stored, used, retained, and/or disclosed, consistent with the quasi-constitutional nature of the right to privacy and applicable industry standards.

88. The standard of care expected of the defendants is heightened by the volume and sensitivity of the Personal Information collected, stored, used, retained, and/or disclosed by the defendants. The Personal Information of the Class Members lies at the core of individual privacy, and therefore demands enhanced and special protections, including protection from attack by malicious third parties intent on exfiltrating Personal Information for improper purposes.

89. The defendants were, and are, obliged to safeguard the Personal Information of the Class Members in their custody or control and which is stored electronically on their System. They were, and are, obliged to take reasonable steps commensurate with the sensitivity of the Personal Information to ensure that the Personal Information in their custody or control was, and is, not accessed or disclosed without authority, including being protected against theft or loss, and to ensure that records containing Personal Information are protected against unauthorized copying, modification, exfiltration or disposal.

(iii) Breach of the Duties Owed to the Class

90. The defendants violated the foregoing duties imposed upon by way of Canada's privacy laws and industry standards to prevent the unlawful and excessive collection of the Class Members' Personal Information, to prevent access, theft or exfiltration by unauthorized third parties, and to detect and diligently respond to the Breach. Specifically, the defendants breached their duties to the Class Members when they failed to:

a. take all reasonable steps to ensure that they identified, prior to collection, the purposes, objectives or use for the collection of the Personal Information;

b. limit the collection, use or disclosure of any Personal Information unaffiliated with said purpose or objective;

c. establish, maintain, enforce or make readily available information about their policies and practices relating to the management of the Personal Information, including individuals' rights to keep the Personal Information confidential;

d. establish, maintain and enforce proper security measures, procedures, policies and/or practices to protect the Class Members' Personal Information appropriate to the sensitivity of that information, the purposes or objectives for which it was to be used, the quantity and/or the medium on which it was stored;

e. establish, maintain and enforce appropriate security measures, procedures, policies and/or practices sufficient to safeguard the Class Members' Personal Information in the System and ensure it would not be lost, disclosed, accessed, or used by unauthorized persons, including in a cyber attack;

f. regularly audit their measures, procedures, policies and/or practices to ensure they were effective or appropriate;

g. diligently act on and address known or knowable vulnerabilities, improper or ineffective security measures, procedures, policies and/or practices involving the System and its security;

h. limit the exposure of the Class Members' Personal Information in the Breach;

i. supervise their employees properly, or provide their employees with proper training with regard to the collection, storage, use, retention, or disclosure of Personal Information;

j. supervise their employees properly, or provide their employees with proper training with regard to management of the System's security;

k. take reasonable steps to ascertain whether their third party provider of cyber security, if any, took security measures adequate to safeguard the Class Members' Personal Information on the System or were compliant with industry standards;

l. exercise reasonable care to securely collect, store, use, retain and disclose the Class Members' Personal Information;

m. otherwise failing to collect, store, use, retain, and/or disclose the Class Members' Personal Information only in accordance with appropriate legislative, regulatory and industry standards, including the *Model Code, PIPEDA,* the *CCQ* and the *PPIPS*; and/or,

n. failing to offer sufficient identity theft insurance services to the Class Members.

91. On the knowledge of the sensitivity of the Personal Information collected, stored, used, retained, and/or disclosed by the defendants, the defendants had a further duty to the Plaintiff and the Class Members to warn of any unauthorized purposes to which their Personal Information could reasonably be made, including the duty to:

a. provide responsible, prompt, and generous notification of any breach of security safeguards involving Class Members' Personal Information as soon as feasible after the defendants determined that a breach had occurred; and,

b. provide sufficient information to allow the Class Members to understand the significance of a breach of security safeguards involving Class Members' Personal Information and to take steps to reduce or mitigate the risk of harm that could result.

92. The defendants wholly failed in their obligations to the Plaintiff and the Class Members. Their cyber security protective measures, if any, were antiquated, inadequate, unreasonable, and readily penetrable by third parties. The defendants failed to meet the relevant standards of care that they were obliged to meet to protect the Class Members' privacy and breached their duties to the Plaintiff and the Class Members.

(iv) Causation

93. By and as a result of its actions and omissions, the defendants amassed a trove of highly sensitive Personal Information of the Class, enabled the Breach, disclosed the Class Members' Personal Information to unauthorized persons, and/or recklessly caused it to be disclosed to unauthorized persons, without the Class Members' knowledge or consent.

94. The Breach would not have happened but for the defendants' breaches of its duties owed to the Class Members to securely and responsibly collect, store and manage their Personal Information; to prevent and timely detect the Breach; and to properly respond to the Breach and warn the Class Members of its implications.

95. At all material times, the defendants knew or ought to have known that their routine collection, storage, use, and/or retention of sensitive financial and personal information from the Class Members made them a valuable target for hackers including both those who would employ ransomware and those who would attempt to sell or use the stolen Data for gain. The defendants also knew or ought to have known that their cyber security was grossly inadequate and vulnerable to hackers, rendering the Class Members' Personal Information vulnerable to theft or compromise. Therefore, they knew that they were a target of significant cyberattacks that, if not prevented, detected in a timely fashion or properly responded to, would have far reaching implications on their customers.

96. Despite their knowledge of those risks, the defendants failed to act diligently in accordance with their duties and the standards required of them to prevent, timely detect and properly respond to the Breach, which caused the loss to the Plaintiff and the Class Members.

97. As a result of the defendants' negligence, the Hackers took and sold and/or disseminated the Plaintiff's and the Class Members' Personal Information, causing proximate loss to the Plaintiff and the Class. In particular, and without limitation, but for the defendants' actions and/or omissions, the Personal Information of the Plaintiff and the Class Members would not have been excessively collected, stored in a readily accessible, vulnerable database such as the System, disseminated on the dark web, and/or been subjected to fraud.

(v) Injury to the Plaintiff and the Class Members

98. The Plaintiff states that, by virtue of their collection, storage, use, retention, and/or disclosure of the Personal Information of the Class Members, including but not limited to that obtained in the Applications, the defendants are in a relationship of sufficient proximity with the Plaintiff and the Class Members such that they could be, and were, foreseeably harmed by the defendants' wrongful actions and/or omissions.

99. As a result of the defendants' actions and/or omissions, the Plaintiff and the Class Members have suffered harm. Particulars of such harm include:

a. theft of assets or the infliction of debt by fraudsters;

b. damage to personal and credit reputation;

c. appropriation of personality or identity theft;

d. serious and prolonged mental distress;

e. costs incurred in rectifying or preventing identity theft or fraud; and,

f. special damages caused by unlawful conduct by third parties, including identity theft or fraud, occasioned by or attributable to the defendants' breaches as alleged herein.

Intrusion Upon Seclusion

100. The defendants are liable for the tort of intrusion upon seclusion because their willful, intentional or reckless conduct facilitated the deliberate intrusion of the Hackers in a manner highly offensive to a reasonable person.

101. Specifically, the defendants' behavior enabled the Breach by willfully, intentionally or recklessly failing to comply with appropriate legislative, regulatory and industry standards as specifically articulated in the preceding section, including the *Model Code, Social Insurance Number Code of Practice, PIPEDA, CCQ* and the *PPIPS*, such that the defendants intruded on the reasonably expected privacy of the Class Members through the excessive collection of unnecessary Personal Information without a proper security System in place. Further, the System was riddled with vulnerabilities sufficiently serious to result in the same consequences as intentional disclosure by the defendants themselves.

102. The defendants unreasonably and excessively collected the Personal Information of the Class Members without any, or alternatively sufficient, privacy or retention policy, System encryption, or System security. The defendants failed to obtain consent to the intrusive collection of the Class Members' highly sensitive Personal Information, merely stating that the applicant "consents to the obtaining of such credit and or personal information as Creditor deems necessary at any time."

103. This attempt at consent was, and is, insufficient and non-commensurate with the invasive and intrusive volume and significance of the data collected. Further, the lack of consent is

consistent with and reflective of that fact that the defendants had no plan for the secure and secluded storage of the highly sensitive Personal Information. This information was stored together in a readily accessible System that afforded no, if any, seclusion or protection over the Class Members' Personal Information. The defendants thereby intentionally and willfully intruded on the reasonable expectation of privacy of the Plaintiff and the Class Members in a manner that was objectively unreasonable at the time of the collection.

104. The defendants' conduct thereby created the environment and opportunity for the Breach. The defendants created and maintained the insecure System containing the Personal Information and intentionally or recklessly by their conduct permitted the Hacker's access to and exfiltration of the Data, which was unauthorized and inconsistent with the Plaintiff's and the Class Members' rights of possession.

105. Further, the defendants failed to provide responsible, prompt, and generous notification of the Breach to the Class Members with sufficient information to allow them to understand the significance of the Breach or for preventative actions to be taken against future intrusions. This failure exacerbated the risks and dangers to the Class arising from them having been the victims of a privacy breach.

106. The Plaintiff states that the defendants were aware that there was a danger that their conduct could bring about the result of a security event such as the Breach and subsequent sale of the Data on the dark web, but nevertheless persisted, despite the risk.

107. The defendants' intrusion upon the Plaintiff's and the Class Members' privacy was objectively highly offensive due to the nature and sensitivity of the Personal Information collected, stored, disclosed, disseminated and/or sold on the dark web in, following, or

resulting from the Breach. Specifically, the actions of the defendants are uniformly and objectively highly offensive, due to their:

a. collection of vast amounts of sensitive Personal Information from members of the Class without taking steps to safeguard said Personal Information in a manner commensurate with its sensitivity, thereby demonstrating disregard for the Class Members' interest in preserving their Personal Information and right to privacy;

b. failure to adopt, maintain and/or enforce proper policies, practices and/or procedures to securely collect, store and manage the Class Members' Personal Information, thereby demonstrating a disregard for cyber security and the confidentiality of the Class Members' Personal Information despite the risks known or knowable to the defendants;

c. failure to securely store the Class Members' Personal Information in a manner commensurate with its sensitivity, thereby demonstrating disregard for the Class Members' interest in safeguarding their Personal Information and right to privacy;

d. failure to promptly and diligently act on known or knowable vulnerabilities or deficiencies in the security of the System, including but not limited to in the aftermath of the Breach, thereby demonstrating disregard for the Class Members' interest in safeguarding their Personal Information and right to privacy; and

e. failure to promptly respond to the Breach and notify members of the Class in a thorough, candid and comprehensive manner, thereby demonstrating

disregard for the disclosure of the Class Members' sensitive Personal Information.

108. Collectively, the defendants' reckless attitude towards the collection, retention, storage and security of Personal Information on the System facilitated the Hackers' ability to invade the Class Members' privacy and led directly to the unlawful invasion of the Class Members' privacy. Their actions were highly offensive, causing distress and anguish to Class Members, for which the defendants are liable.

Québec Class Members

109. On behalf of the Class Members, if any, resident in the province of Québec, the Plaintiff pleads that the defendants violated articles 3 and 35-37 of *CCQ*, section 5 of the *Québec Charter*, and section 10 of the *PPIPS*, each as amended.

110. The defendants violated these Class Members' right to respect for their private lives and their right to privacy without their consent and without being authorized by law.

111. As a result of the breaches of the *CCQ*, the Plaintiff and the Class are entitled to moral and material damages pursuant to articles 1457b and 1463-1464 of the *CCQ*.

REMEDIES

Damages

112. As a result of the defendants' actions and/or omissions the Plaintiff and the Class Members have suffered losses and damages.

113. The Plaintiff and the Class Members are owed damages to compensate for the defendants' negligence including, but not limited to injuries suffered for:

a. theft of assets or the infliction of debt by fraudsters;

b. damages to personal and credit reputation;

c. costs incurred in rectifying identity theft or fraud or, in the alternative, costs incurred in preventing identity theft or fraud;

d. lost or wasted time and inconvenience in responding to the Breach;

e. general damages to be assessed in the aggregate; and

f. special damages caused by unlawful conduct by third parties, including identity theft or fraud, occasioned by or attributable to the defendants' breaches as alleged herein.

114. Additionally, for and on behalf of each Class Member who as a result of the Breach has been the subject of unauthorized withdrawal of funds from his, her or its accounts, wherever held, the Plaintiff claims compensatory damages in the sum that equals the amount of the funds withdrawn from, or charged to, the account without authorization, plus interest calculated at an annual rate to be determined at trial.

115. In addition to the damages set out above, the Class Members are entitled to symbolic and moral damages for the reprehensible conduct of the defendants and corresponding violation of their rights to privacy at common law.

116. The Plaintiff states that the defendants' Offer to provide a credit monitoring service is neither reasonable, adequate, nor timely because the Class Members remain exposed to the risks of fraudulent activity stemming from the Breach well beyond the expiry of the proposed one or two year package.

Punitive and Exemplary Damages

117. By virtue of the defendants' high-handed conduct and its disregard for the privacy rights of the Plaintiff and the Class Members, the Plaintiff asks this Court to award exemplary and punitive damages against the defendants, in an amount deemed appropriate by this Court at trial.

118. The defendants' deliberate disregard for the confidentiality and security of the Class Members' Personal Information constitutes a flagrant betrayal of their trust. Their actions were high-handed, arrogant, and display a reckless disregard for the Class Members' privacy and property rights. As a result, the Class Members have suffered damage to, among other things, their pride, self-respect and reputation.

119. Moreover, subsequent to learning of the existence of the Breach, the defendants failed to implement a timely, comprehensive notice program to inform the Class Members about the Breach. This conduct was further high-handed, reckless, without care, deliberate, and offensive to moral standards of the community.

120. The Plaintiff relies on equity which entitles the Court to order exemplary or punitive damages or other relief the Court considers proper.

THE RELEVANT STATUTES

121. The Plaintiff relies upon the *CPA, PIPEDA, CCQ, PPIPS,* the *CJA,* and the *Negligence Act*, R.S.O. 1991, c. N.1, each as amended.

REAL AND SUBSTANTIAL CONNECTION WITH ONTARIO

122. This action has a real and substantial connection with Ontario because, among other things:

a. many of the proposed Class Members reside in Ontario;

b. the defendants carry on business in Ontario;

c. contracts relating to the subject matter of this action were made in Ontario;

d. the tort of intrusion upon seclusion was committed in Ontario;

e. the Class Members' Personal Information was collected, stored and/or transmitted in and through Ontario; and,

f. a substantial portion of the damages sustained by the Class were sustained by persons and entities domiciled in Ontario.

SERVICE OUTSIDE ONTARIO

123. This originating process may be served without Court order outside of Ontario in that the claim is:

a. in respect of real or personal property in Ontario (Rule 17.02(a));

b. in respect of a contract where, the contract was made in Ontario (Rule 17.02(f)(i));

c. in respect of a tort committed in Ontario (Rule 17.02 (g)); and,

d. against a person ordinarily resident or carrying on business in Ontario (Rule 17.02 (p)).

THE PLAINTIFF proposes that this action be tried in the City of London, in the Province of Ontario.

February 8, 2021

FOREMAN & COMPANY
PROFESSIONAL CORPORATION
4 Covent Market Place
London, ON N6A 1E2

Jonathan J. Foreman (LSO# 45087H)
Anne E. Legate-Wolfe (LSO# 76832J)
Tel: (519) 914-1175
Fax: (226) 884-5340
E-mail: jforeman@foremancompany.com
alegatewolfe@foremancompany.com

WADDELL PHILLIPS
PROFESSIONAL CORPORATION
36 Toronto St., Suite 1120
Toronto, ON M5C 2C5

Margaret L. Waddell (LSO #29860U)
Tina Q. Yang (LSO #60010N)
Tel: (416) 477-6979
Fax: (416) 477-1657
Email: marg@waddellphillips.ca
tina@waddellphillips.ca

Lawyers for the Plaintiff

THERESA ORIET Plaintiff	v.	AGRONOMY COMPANY OF CANADA et al. Defendants	Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

PROCEEDING COMMENCED AT LONDON

Proceeding Under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

FOREMAN & COMPANY
PROFESSIONAL CORPORATION
4 Covent Market Place
London, ON N6A 1E2

Jonathan J. Foreman (LSO# 45087H)
Anne E. Legate-Wolfe (LSO# 76832J)
Tel: (519) 914-1175
Fax: (226) 884-5340
Email: jforeman@foremancompany.com
alegatewolfe@foremancompany.com

WADDELL PHILLIPS
PROFESSIONAL CORPORATION
36 Toronto St., Suite 1120
Toronto, ON M5C 2C5

Margaret L. Waddell (LSO 29860U)
Tina Q. Yang (LSO 60010N)
Tel: (416) 477-6979
Fax: (416) 477-1657
Email: marg@waddellphillips.ca
tina@waddellphillips.ca

Lawyers for the Plaintiff