UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DEBT CLEANSE GROUP LEGAL SERVICES LLC, individually and on behalf of all others similarly situated, Plaintiff, v. GOTO TECHNOLOGIES USA, INC., and LASTPASS US LP, Defendants.	Case No. **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiff Debt Cleanse Group Legal Services LLC ("Plaintiff") brings this class action complaint against Defendants GoTo Technologies USA, Inc. ("GoTo") and LastPass US LP ("LastPass") (collectively, "Defendants") to recover damages, restitution, and injunctive relief on behalf of a Class of persons whose information ("Customer Information") was accessed without authorization by criminals as a result of Defendants' unreasonable and deficient data security practices (the "Data Breach").

Plaintiff makes these allegations on personal information as to those allegations pertaining to itself, and upon information and belief, the investigation of counsel, and facts that are a matter of public record on all other matters.

NATURE OF THE ACTION

1. This class action lawsuit arises out of Defendants' notification to Plaintiff and Class members informing them about the Data Breach on November 30, 2022.

2. Because of Defendants' unreasonable data security practices, monitoring, and unreasonable aggregation and integration of Plaintiff's and Class members' Customer Information into their systems, in or around August 2022, unauthorized persons who are criminal actors gained

access to Defendants' systems and accessed and obtained Plaintiff's and Class members' Customer Information.

3. Defendants' deficient data security practices stand in stark contrast to their representations in advertisements and promotional materials to Plaintiff and Class members regarding their strong encryption, robust data security practices, and authentication procedures, which were false and misleading.

4. Plaintiff and Class members suffered injuries as a result of Defendants' unlawful and deceptive conduct in selling a password management service that was not as advertised and represented, and was unreasonable and deficient in ways that caused the Data Breach.

5. Plaintiff and Class members bring claims for negligence, negligent misrepresentation, breach of contract, and unjust enrichment against Defendants.

PARTIES, JURISDICTION AND VENUE

6. Plaintiff is a Delaware limited liability company with its principal place of business in Chicago, Illinois. In reasonable reliance on Defendants' misrepresentations regarding strong data security, Plaintiff purchased an enterprise license with LastPass and all of Plaintiff's employees used the program to store their passwords.

7. GoTo is a Delaware corporation with its principal place of business in Boston, Massachusetts.

8. LastPass is a limited partnership organized under the laws of Delaware with its principal place of business in Boston, Massachusetts.

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because at least one member of the Class, as defined below is a citizen of a different state

than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

10. The Court has personal jurisdiction over Defendants because Defendants' negligent acts or omissions, false and misleading misrepresentations, and violations of consumer protection statutes regarding the security of Plaintiff's and Class members' Customer Information alleged herein occurred in this state, and Defendants are organized under the laws of this state and are at home in this state.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the injury in this case substantially occurred in this District and Defendants reside in this District.

FACTUAL BACKGROUND

12. On August 25, 2022, LastPass issued the following notice:

> ***Original post from August 25, 2022***
>
> To All LastPass Customers,
>
> I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community.
>
> Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults.
>
> We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are

operating normally.

In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity.

Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve.

Thank you for your patience, understanding and support.

Karim Toubba

CEO LastPass

https://blog.lastpass.com/2022/11/notice-of-recent-security-incident/

13. Then, on September 15, 2022, LastPass released the following statement:

Update as of Thursday, September 15, 2022

To All LastPass Customers,

On August 25th, 2022, we notified you about a security incident that was limited to the LastPass Development environment in which some of our source code and technical information was taken. I wanted to update you on the conclusion of our investigation to provide transparency and peace-of-mind to our consumer and business communities.

We have completed the investigation and forensics process in partnership with Mandiant. Our investigation revealed that the threat actor's activity was limited to a four-day period in August 2022. During this timeframe, the LastPass security team detected the threat actor's activity and then contained the incident. There is no evidence of any threat actor activity beyond the established timeline. We can also confirm that there is no evidence that this incident involved any access to customer data or encrypted password vaults.

Our investigation determined that the threat actor gained access to the Development environment using a developer's compromised endpoint. While the method used for the initial endpoint compromise is inconclusive, the threat actor utilized their persistent access to impersonate the developer once the developer had successfully authenticated using multi-factor authentication.

Although the threat actor was able to access the Development environment, our system design and controls prevented the threat actor from accessing any customer data or encrypted password vaults.

Firstly, the LastPass Development environment is physically separated from, and has no direct connectivity to, our Production environment. Secondly the Development environment does not contain any customer data or encrypted vaults. Thirdly, LastPass does not have any access to the master passwords of our customers' vaults – without the master password, it is not possible for anyone other than the owner of a

vault to decrypt vault data as part of our Zero Knowledge security model.

In order to validate code integrity, we conducted an analysis of our source code and production builds and confirm that we see no evidence of attempts of code-poisoning or malicious code injection. Developers do not have the ability to push source code from the Development environment into Production. This capability is limited to a separate Build Release team and can only happen after the completion of rigorous code review, testing, and validation processes.

As part of our risk management program, we have also partnered with a leading cyber security firm to further enhance our existing source code safety practices which includes secure software development life cycle processes, threat modeling, vulnerability management and bug bounty programs.

Further, we have deployed enhanced security controls including additional endpoint security controls and monitoring. We have also deployed additional threat intelligence capabilities as well as enhanced detection and prevention technologies in both our Development and Production environments.

We recognize that security incidents of any sort are unsettling but want to assure you that your personal data and passwords are safe in our care.

Thank you for your continued trust and support.

Karim Toubba

CEO LastPass

https://blog.lastpass.com/2022/11/notice-of-recent-security-incident/

14. Then, on November 30, 2022, LastPass published the following statement:

Update as of Wednesday, November 30, 2022

To All LastPass Customers,

In keeping with our commitment to transparency, I wanted to inform you of a security incident that our team is currently investigating.

We recently detected unusual activity within a third-party cloud storage service, which is currently shared by both LastPass and its affiliate, GoTo. We immediately launched an investigation, engaged Mandiant, a leading security firm, and alerted law enforcement.

We have determined that an unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information. Our customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture.

We are working diligently to understand the scope of the incident and identify what specific information has been accessed. In the meantime, we can confirm that LastPass products and services remain fully functional. As always, we recommend that you follow our best practices around setup and configuration of LastPass, which can be found here.

As part of our efforts, we continue to deploy enhanced security measures and monitoring capabilities across our infrastructure to help detect and prevent further threat actor activity.

> We thank you for your patience while we work through our investigation. As is our practice, we will continue to provide updates as we learn more.
>
> Karim Toubba
>
> LastPass CEO
>
> https://blog.lastpass.com/2022/11/notice-of-recent-security-incident/

15. Plaintiff received notice of the Data Breach.

16. The full impact and scope of the Data Breach and Customer Information involved remains under investigation to this date.

17. On information and belief, Plaintiff's and Class members' Customer Information was copied multiple times by criminals and sold or used for criminal activity that threatens to cause harm to Plaintiff and Class members.

18. In addition to failing to secure the Customer Information with reasonable measures and preventing the Data Breach, Defendants delayed unreasonably to fulfill their obligations to provide notice of the Data Breach to Plaintiff and Class members. The Data Breach was discovered some time in August 2022, but prior statements in August and September disclaimed that any customer information was under threat. Those statements were false, and on November 30, 2022, Defendants finally notified Plaintiff and Class members that "certain elements" of Customer Information were accessed by the criminals.

19. Defendants are aware of the need to take reasonable measure to secure sensitive information in online environments. In fact, Defendants hold themselves out as experts in the area, as follows:

> Data breaches are on the rise, with more than 80% of breaches caused by

> weak, reused, or stolen passwords. Doing nothing could mean losing everything. That's why password security has never been more critical for individuals and businesses.
>
> As a pioneer in cloud security technology, LastPass provides award-winning password and identity management solutions that are convenient, effortless, and easy to manage. LastPass values users' privacy and security, so your sensitive information is always hidden – even from us.
>
> https://www.lastpass.com/company/about-us

20. Defendants made assurances, representations, and promises that were false, deceptive, and misleading to induce customers to purchase their products and services.

21. Defendants represented that: "as a password manager, our first priority is safeguarding your data. We've built LastPass so that we never have the key to your account." https://www.lastpass.com/how-lastpass-works.

22. Defendants claim to provide protection from data breaches:

> 80% of data breaches are caused by weak, reused or stolen passwords. Excellent business password hygiene and practices are necessary to avoid data breaches. However, traditional password management practices can be overwhelming for both employees and Admins.
>
> LastPass Business empowers your workforce by reducing friction for users and IT teams. Save time by simplifying employee password management while granting Admins actionable oversight, from advanced reporting to 100+ customizable security policies.
>
> https://www.lastpass.com/products/business

23. LastPass promises that customers using LastPass "set stronger security policies" and "decrease employee's password-related risks." https://www.lastpass.com/products/business

24. Plaintiff and Class members were exposed to these assurances and representations regarding the supposed superior data protection offered by Defendants' services, and reasonably relied on these representations in deciding to use or purchase accounts with Defendants' services.

25. Had Plaintiff and Class members known the true nature regarding Defendants' deficient and unreasonable data security practices that exposed their Customer Information to foreseeable threats of attack, they would not have used Defendants' services.

26. In addition, had Defendants not made the false representations in their notice letters claiming that no customer information was taken and that the investigation was concluded, Plaintiff and Class members would have taken proactive measures to safeguard their Customer Information before the Data Breach got worse.

27. Despite all of Defendants' assurances, representations, and promises regarding industry leading data security solutions, Defendants employed deficient and unreasonable data security practices.

28. Based on the notice, Plaintiff was warned that, based on an incomplete and ongoing investigation, certain details regarding Customer Information were compromised in an incident involving the unauthorize acquisition and use of an unidentified developer's credential over the course of four months. Each new notice revealed that the Data Breach was worse than before, while continuing to falsely allay reasonable concerns that Customer Information was taken or the Data Breach was serious.

29. Defendants collected, aggregated, digitized, and maintained significant financial and personal Customer Information pertaining to Plaintiff and Class members, including financial

account information, name, address, contact information, and passwords to accounts.

30. Defendants failed to provide Plaintiff with an outlook regarding how the investigation would be conducted or when the investigation would be completed.

31. Thus, although Defendants stated that passwords were still secure in the latest notice, Plaintiff reasonably expended time, costs, and energy to require Plaintiff's employees to change all of the passwords to their accounts to avoid the risk that additional updates would reveal Defendants' assurances were untrue.

32. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

33. Consumers place a high value not only on their personal and financial information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

34. The United States Government Accountability Office ("GAO") explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018). The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

35. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that

lasts for 7 years if someone steals their identity), reviewing their credit reports often, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

36. Identity thieves use stolen personal and financial information for "various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud." *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are ways for hackers to exploit information they already have to get even more personally identifying information through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

37. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

38. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber blackmarket" for years.

39. Thus, there is a strong probability that entire batches of stolen information have

been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiff and Class members may be at an increased risk of fraud and identity theft for many years into the future.

40. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."

41. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

42. Criminals can use the information to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendants to send fraudulent mail, emails, and other communications to Plaintiff and Class members that look authentic, but which are designed to lure them into paying money or providing other information that the criminals can use to steal money.

43. Criminals can use the payment and financial information that Defendants were entrusted with to perpetrate financial crimes that harm Plaintiff and Class members, or as appears to have happened to Defendants in this case, criminals can leverage pieces of information to gain access to additional information that they can use to exact significant damage on victims.

PLAINTIFF'S INJURIES

44. On or around June 9, 2018, Plaintiff was exposed to the misrepresentations from Defendants regarding their superior data security that were false, deceptive, and misleading. Reasonably relying on these misrepresentations, Plaintiff decided to purchase an enterprise subscription to LastPass and required all of Plaintiff's employees to implement LastPass. Had Plaintiff known the truth regarding Defendants' deficient and unreasonable data security practices, Plaintiff would not have purchased the services from Defendants. As a result, Plaintiff incurred damages in the amount of money paid for services and quality bargained for but not received.

45. In addition, Plaintiff spent time, energy, and resources researching the Data Breach, investigating the facts and circumstances, conducting a risk assessment, and lost time to change all of its employees' passwords for the accounts using LastPass, which were considerable. Plaintiff lost time and spent money to pay employees to do these activities, and was diverted from performing money-making services while doing so.

CLASS ALLEGATIONS

46. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and a Class defined as follows:

> All persons who had their Customer Information accessed in the Data Breach.

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and its current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel

and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

47. **Numerosity**: The exact number of Class members is unknown to Plaintiff, but individual joinder is impracticable. LastPass boasts that 33+ million people and 100,000+ businesses use LastPass. *See* https://www.lastpass.com/company/about-us.

48. **Typicality**: Plaintiff's claims are typical of the claims of other members of the Class, in that Plaintiff and Class members sustained damages arising out of the same acts and omissions of Defendants relating to their failure to protect, oversee, monitor, and safeguard the Customer Information.

49. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiff's claims are made in a representative capacity on behalf of the other members of the Class. Plaintiff has no interests antagonistic to the interests of the other members of the Class and is subject to no unique defenses. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so.

50. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' practices challenged herein apply to and affect Class members uniformly, and Plaintiff's challenge to those practices hinge on

Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

51. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendants failed to maintain reasonable security procedures;

b. Whether Defendants' conduct constitutes negligence;

c. Whether Defendants' conduct constitutes negligent misrepresentation;

d. Whether Defendants' conduct constitutes a breach of contract;

e. Whether Plaintiffs are entitled to restitution on the basis of unjust enrichment; and

f. Whether Plaintiffs and Class members are entitled to damages and injunctive relief.

52. **Superiority**: This case is appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. Joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small in comparison to the burden and expense of individual prosecutions of litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties and the court systems of many states and federal districts. By

contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

CAUSES OF ACTION

COUNT I
Negligence

53. Plaintiff incorporates paragraphs 1–52 as if fully set forth herein.

54. Each of the Defendants owed a duty to Plaintiff and Class members to notify them that their Customer Information had been disclosed to and accessed by unauthorized criminal hackers.

55. Each of the Defendants owed a duty to Plaintiff and Class members to properly train, vet, and oversee employees and vendors who maintain, access, store, and manage Plaintiff's and Class members' Customer Information and to implement and maintain reasonable data security practices to protect the Customer Information from foreseeable cyberattacks and unauthorized access.

56. Defendants breached these duties and the applicable standards of care by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and Class members' Customer Information;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Customer Information;

d. Failing to adequately segregate and isolate Customer Information from publicly accessible or publicly adjacent environments;

e. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the other Class members' Customer Information;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiff's and the other Class members' Customer Information reasonably and appropriately in order to repel or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the Customer Information to ensure the Customer Information was being stored and maintained for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and the other Class members' Customer Information;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiff's and the other Class members' Customer Information, was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the other Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the other Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their Customer Information, and details regarding the disposition of Plaintiff's and the other Class members' Customer Information at all times during the Data Breach.

57. Defendants are both the actual and legal cause of Plaintiff's and the Class members' injuries. Had Defendants adopted and maintained reasonable data security procedures and provided timely notification of the Data Breach to those affected, including Plaintiff and the other Class members, Plaintiff and the other Class members would not have been damaged or would have been damaged to a lesser degree than they actually were.

58. Plaintiff and the other Class members have suffered damages as a result of Defendants' negligence. Plaintiff and Class members have suffered actual and concrete injuries

and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendants' warnings and following their instructions in the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of the benefit of the bargained for data security practices that were not provided as represented; and (i) and diminution of value of their Customer Information.

COUNT II
Negligent Misrepresentation

59. Plaintiff incorporates paragraphs 1–52 as if fully set forth herein.

60. Defendants supplied false information for the guidance of others in the course of their business. As alleged above, Defendants falsely represented that their products and services were superior data security practices that would protect Plaintiff and Class members from the Data Breach, when in actuality, Defendants employed deficient and unreasonable data security practices.

61. Defendants' representations were false and Defendants failed to exercise reasonable care in obtaining or communicating the information. Defendants' data security practices were unreasonable and deficient by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the

hackers' infiltration into the system(s) storing Plaintiff's and Class members' Customer Information;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Customer Information;

d. Failing to adequately segregate and isolate Customer Information from publicly accessible or publicly adjacent environments;

e. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the other Class members' Customer Information;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiff's and the other Class members' Customer Information reasonably and appropriately in order to repel or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the Customer Information to ensure the Customer Information was being stored and maintained for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and

unauthorized acquisition of Plaintiff's and the other Class members' Customer Information;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiff's and the other Class members' Customer Information, was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the other Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the other Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their Customer Information, and details regarding the disposition of Plaintiff's and the other Class members' Customer Information at all times during the Data Breach.

62. Plaintiff and Class members justifiably relied on Defendants' false information and were induced to obtain Defendants' products and services in reliance thereon.

63. Plaintiff and Class members have suffered damages as a result of Defendants' negligent misrepresentation. Plaintiff and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic

damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendants' warnings and following their instructions in the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of the benefit of the bargained for data security practices that were not provided as represented; and (i) and diminution of value of their Customer Information.

COUNT III
Breach of Contract

64. Plaintiff incorporates paragraphs 1–52 as if fully set forth herein.

65. LastPass promises in its Personal Terms of Service:

> 4.2.1. Information Security and Certifications
>
> We have implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure. We also maintain a compliance program that includes independent third-party audits and certifications. You can visit our Trust & Privacy Center (https://www.lastpass.com/trust-center) to review Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation), including, but not limited to, encryption use and standards, retention periods, and other helpful information.
>
> 4.2.2. Data Privacy
>
> We maintain a global data privacy program, designed to safeguard and responsibly handle your Content and any associated personal data we may collect

and/or process on your behalf. You understand that when using the Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. You can visit our Trust & Privacy Center (https://www.lastpass.com/trust-center/privacy) to review LastPass' comprehensive privacy program, third-party frameworks, privacy policies, and applicable data processing locations and Sub-Processor Disclosures, as well as the TOMs.

66. LastPass promises in its Business Terms of Service:

4.2.1. Information Security and Certifications

LastPass agrees to maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure, in accordance with industry standards. Additional information about LastPass' technical and organizational security measures ("TOMs"), including, but not limited to, encryption use and standards, retention periods, and other helpful information can be found in our Trust & Privacy Center (https://www.lastpass.com/trust-center), along with information regarding our independent third-party security audits and certifications.

4.2.2. Data Privacy

While providing the Services to you, LastPass agrees handle your Content and any associated personal data we may collect and/or process on your behalf in a responsible manner. You can visit our Trust & Privacy Center (https://www.lastpass.com/trust-center/privacy) to review additional information about LastPass' comprehensive privacy program, third-party privacy frameworks,

> privacy policies, and applicable data processing locations and Sub-Processor Disclosures. You understand that when using our Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. When providing our Services, LastPass acts as a data processor, service provider, or the equivalent construct. To review and execute LastPass' Data Processing Addendum ("DPA"), please visit https://www.lastpass.com/legal-center.

https://www.lastpass.com/legal-center/terms-of-service/business.

67. GoTo promises in its Terms of Service:

> 4.2. Your Privacy and Security.
>
> We maintain a global privacy and security program designed to protect your Content and any associated personal data we may collect and/or process on your behalf. You can visit our Trust & Privacy Center (https://www.goto.com/company/trust) to review applicable data processing locations and Sub-Processor Disclosures, as well as Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation). When providing our Services, we act as a data processor, service provider, or the equivalent construct. To review and execute our Data Processing Addendum ("DPA"), please visit https://www.goto.com/company/legal.

https://www.goto.com/company/legal/terms-and-conditions.

68. In addition, GoTo incorporates its security measure representations into its Terms of Service, as follows:

> GoTo is dedicated to monitoring and continuously improving our security, technical and organizational measures to better protect your sensitive Customer Content. We are always evaluating industry standard practices regarding technical data privacy and information security and strive to meet or exceed those standards. Our security programs are comprehensive and dedicated to all facets of security.
>
> Alongside our stringent internal security controls, we hold the following trusted third-party security certifications. As part of our commitment to our subscribers, we conduct SOC 2 (type II) audits, and share out a SOC 3 report, which is a shareable version of the SOC 2. The SOC 3 reports for each applicable product, can be found and downloaded on our product resources page here.

https://www.goto.com/company/trust/security-measures

69. Defendants breached the foregoing contractual terms resulting in the Data Breach, in one or more of the following ways:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and Class members' Customer Information;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were

the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Customer Information;

d. Failing to adequately segregate and isolate Customer Information from publicly accessible or publicly adjacent environments;

e. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the other Class members' Customer Information;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiff's and the other Class members' Customer Information reasonably and appropriately in order to repel or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the Customer Information to ensure the Customer Information was being stored and maintained for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and the other Class members' Customer Information;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiff's and the other Class members' Customer Information,

was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the other Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the other Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their Customer Information, and details regarding the disposition of Plaintiff's and the other Class members' Customer Information at all times during the Data Breach.

70. All conditions precedent were performed or have occurred.

71. As a proximate result of Defendants' breaches of contract described above, Plaintiff and Class members have incurred damages. Plaintiff and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendants' warnings and following their instructions in the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred

due to actual identity theft; (h) loss of the benefit of the bargained for data security practices that were not provided as represented; and (i) and diminution of value of their Customer Information.

COUNT IV
Unjust Enrichment

72. Plaintiff repeats and realleges paragraphs 1–52 as if fully set forth herein.

73. Defendants each knew that the data security of their systems was a material fact to consumers, including Plaintiff and Class members.

74. Because Defendants are responsible for, and control, their data security practices, Defendants knew and intended that their omissions and concealment thereof would mislead Plaintiff and Class members, and induce them to use, sign up for, and /or buy products and services that they would otherwise not have been willing to purchase.

75. Acting as reasonable consumers, had Plaintiff and Class members been aware of the true facts regarding Defendants' deficient and unreasonable data security practices, they would have declined to purchase Defendants' products and services and give them Customer Information.

76. Acting as reasonable consumers, Plaintiff and Class members could not have avoided the injuries suffered by Defendants' unlawful and unreasonable conduct.

77. As a direct and proximate result of Defendants' misrepresentations and omissions, Plaintiffs and members of the Class conferred a benefit on Defendants.

78. Defendants each acquired and retained money and other value consideration belonging to Plaintiff and the Class members as a result of their wrongful conduct. Defendants profited at the expense of Plaintiff and Class members because Plaintiffs and Class members paid money for products that were worthless due to the fact that they exposed rather than secured their Consumer Information and other data.

79. Defendants each have unjustly received and retained a benefit at the expense of

Plaintiff and Class members because Defendants unlawfully acquired their revenues by failing to employ reasonable data security practices contrary to their misrepresentations and omissions.

80. Defendants' retention of those benefits violates the fundamental principles of justice, equity, and good conscience. Under the principles of equity, Defendants should not be allowed to keep the money rightfully belonging to Plaintiff and Class members.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of the Class, requests that the Court:

A. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned counsel as Class counsel;

B. Award equitable relief as is necessary to protect the interests of Plaintiff and Class members;

C. Award damages to Plaintiff and Class members in an amount to be determined at trial;

D. Award Plaintiff and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

E. Award Plaintiff and Class members pre- and post-judgment interest, to the extent allowable; and

F. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Plaintiff Debt Cleanse Group Legal Services LLC, individually and on behalf of all others similarly situated,

By: */s/ Kenneth D. Quat*
Kenneth D. Quat, BBO #408640
Quat Law Offices
373 Winch St.
Framingham MA 01701
508-361-0207
kquat@quatlaw.com

Thomas A. Zimmerman, Jr. (to be admitted PHV)
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
firm@attorneyzim.com

Marc E. Dann (to be admitted PHV)
Brian D. Flick (to be admitted PHV)
DannLaw
15000 Madison Avenue
Cleveland, Ohio 44107
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Counsel for Plaintiff and the Putative Class

ClassAction.org