CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

Nº: 500-06-001261-235

(Class Action)

SUPERIOR COURT

L C , residing and domiciled at

Plaintiff

v.

ESTÉE LAUDER COSMETICS LTD, legal person having its head office at 161 Commander Blvd., Agincourt, Province of Ontario, M1S 3K9, and having its principal establishment located at 3035 boulevard Carrefour Laval, Unit T-009, in the City and District of Laval, Province of Québec H7T 1C7;

Defendant

APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION
(Art. 574 C.C.P. and following)

TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT OF QUEBEC, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE PLAINTIFF STATES THE FOLLOWING:

INTRODUCTION

1. Plaintiff wishes to institute a class action on behalf of the following group, of which Plaintiff is a member, namely:

> All persons in Canada:
>
> (i) whose personal or financial information held by Estée Lauder was compromised in a data breach which occurred on or before July 12, 2023, or
>
> (ii) who received an email or letter from Estée Lauder, dated on or about September 5, 2023, informing them of such data breach;
>
> or any other Group(s) or Sub-Group(s) to be determined by the Court;
>
> (hereinafter Class Members are collectively referred to as "**Class Member(s)**", "**Group Member(s)**", the "**Group**", the "**Class**", "**Customer(s)**" or "**Client(s)**").

2. Defendant Estée Lauder Cosmetics Ltd, considers itself as "one of the world's leading manufacturers, marketers, and sellers of quality skin care, makeup, fragrance, and hair care products, and is a steward of outstanding luxury and prestige brands globally", doing business under the many well-known brand names including without limitation: AVEDA®, La Boutique de la compagnie des cosmétiques, MAC ®, ARAMIS PARFUMS DE DESIGNER. BANQUE BEAUTÉ, BOBBI BROWN, BUMBLE & BUMBLE PRODUCTS, JO MALONE, LA MER, LAB SERIES, LES COSMÉTIQUES PROFESSIONEL BOBBI BROWN, MAX HUBER, OJON, ORIGINS, TOM FORD, CLINIQUE, COSMETICS MAC, LES PRODUITS DE BEAUTÉ ESTÉE LAUDER LTÉE, MAC COSMÉTIQUES, COSMÉTIQUES MAC, LES COSMÉTIQUES MAKE-UP ART MAC, (hereinafter "**Estée Lauder**"), the whole as appears more fully from a copy of the *Registre des enterprises* report concerning Estée Lauder Cosmetics Ltd, communicated herewith as **Exhibit P-1**.

The Situation

3. On or about July 12, 2023, unauthorized third parties gained access to Estée Lauder's systems and obtained the personal information of its clients, including Plaintiff and the other Class Members (hereinafter the "**Data Breach**").

4. Plaintiff only received the following email from Estée Lauder on September 6, 2023, a copy of which is communicated herewith as **Exhibit P-2** (hereinafter the "**Notice**"), namely and excessive 56 days after the Data Breach had apparently occurred:

> **From:** The Estee Lauder Companies <notice@elcompanies.com>
> **Date:** September 5, 2023 at 2:27:39 PM EDT
> **To:** ...
> **Subject: Important Information About Data Security Incident / Renseignements importants sur un incident relatif à la sécurité des données**

ESTĒE LAUDER COMPANIES

Dear Valued Consumer,

We recently learned of a data security incident affecting our company. We determined through our ongoing investigation that an unauthorized third party gained access to some of our systems and obtained personal information of certain consumers of our brands on or around July 12, 2023.

The personal information obtained includes name, contact information (for example, email address), date of birth, gender and details about the individual's engagement with our brands (for example, products purchased or recommended, and the date and location of purchase or services). The impacted data varies for each affected individual.

After learning of the incident, we quickly launched an investigation and have been working with leading outside cybersecurity experts to determine

the nature and scope of the incident. We are also coordinating with law enforcement authorities. We take the security of our data and systems very seriously and have put in place additional monitoring measures to further protect our systems. Because the incident involved your email address, we recommend you remain alert for any unsolicited communications involving your personal information to help protect against phishing.

We deeply value you as our loyal consumer and regret any inconvenience this incident may have caused you. If you have any questions regarding this incident, please contact us at 1-866-779-7806 Monday through Friday, 8.00 AM – 5.30 PM Central Time.

Chères clientes et chers clients,

Nous avons récemment appris qu'un incident relatif à la sécurité des données touchait notre société. Nous avons établi, dans le cadre d'une enquête qui est toujours en cours, qu'une tierce partie non autorisée est parvenue, aux alentours du 12 juillet 2023, à accéder à certains de nos systèmes pour y recueillir des renseignements personnels au sujet de certains clients de nos marques.

Les renseignements personnels recueillis comprennent le nom, les coordonnées (par exemple, l'adresse de courriel), la date de naissance, le genre ainsi que des renseignements détaillés sur l'engagement de la personne visée envers nos marques (par exemple, les produits qu'elle a achetés ou recommandés, ainsi que la date et le lieu d'achat ou l'emplacement des services). Les données touchées varient d'une personne à l'autre.

Après avoir été mis au fait de l'incident, nous avons rapidement lancé une enquête et avons travaillé avec des experts en cybersécurité externes de premier plan afin de déterminer la nature et la portée de l'incident. Nous collaborons également avec les autorités policières. Nous prenons la sécurité de nos données et de nos systèmes très au sérieux et avons mis en place des mesures de surveillance afin de mieux protéger nos

systèmes. Puisque l'incident touchait votre adresse de courriel, nous vous recommandons de demeurer à l'affût de toute communication non sollicitée qui vous demanderait de transmettre des renseignements personnels afin de vous protéger contre l'hameçonnage.

Votre fidélité nous tient à cœur et nous sommes sincèrement désolés des inconvénients que cet incident a pu vous causer. Si vous avez des questions au sujet de cet incident, veuillez communiquer avec nous au 1-866-779-7806 du lundi au vendredi, de 8 h 00 à 17 h 30, heure normale du Centre.

Estée Lauder Cosmetics Ltd, 161 Commander Blvd. Agincourt, ON. M1S 3K9, CANADA

ELN-19007

5. As appears from the Notice, Estée Lauder has confirmed and admitted that the Plaintiff and the Class Members will suffer inconvenience and that "because the incident involved your email address, we recommend you remain alert for any unsolicited communications involving your personal information to help protect against phishing.". Accordingly, Estée Lauder is confirming and admitting that the Plaintiff and Class Members are now at risk of such social engineering and phishing techniques used by fraudsters in order to committed identity theft and/or fraud.

6. As appears from the Notice, the database and information which was accessed and stollen by the unauthorized third parties includes the following:

- Name
- contact information (for example, email address)
- date of birth,
- gender
- details about the individual's engagement with our brands (for example, products purchased or recommended, and the date and location of purchase or services).

7. That being said, the Estée Lauder Canada Consumer Privacy Policy (available on its website), a copy of which is communicated herewith as **Exhibit P-3**, confirms that Estée Lauder indeed collects much more information from its customers, namely:

- Contact information and personal identifiers, such as your name, address, email address, telephone number, and username or social media handle.

- Device identifiers, such as information about your device like your MAC address, IP address, or other online identifiers.

- Demographic information, such as your age, or date of birth, sex, and gender.

- Physical characteristics, such as your hair type and color, skin type, and eye color.

- Biometric information, such as facial geometry, if you use certain of our virtual try-on applications or skin-care diagnostic tools.

- Commercial information, such as the products or services you have purchased, returned or considered, and your product preferences.

- Payment information, such as your method of payment and payment card information (including payment card number, delivery address and billing address).

- Identity verification information, such as photo identification for in-store pick-ups at one of our retail stores, loyalty member ID, and authentication information (like passwords).

- Online or network activity information, such as information regarding your interaction with our websites, mobile applications, digital properties, and advertisements, information about your browsing and search history on our websites or mobile applications, and log file information like your browser type and webpages you visit.

- Geolocation information, such as information that can help identify your physical location (like your GPS coordinates or the approximate location of your device).

- Audio and visual information, such as recordings of your voice when you call our customer service and images we record through video surveillance in our retail stores.

- Professional or employment-related information, such as professional licenses or certifications in connection with our professional programs.

- Health and medical information, such as skincare concerns, diagnoses, medical reports and history.

- User Content, such as your communications with us and any other content you provide (including photographs and images, videos, reviews, articles, survey responses, and comments).

- Inferences drawn from or created based on any of the information identified above.

8. Estée Lauder, who required the personal and financial information of its customers in the context of the marketing and sale of its products, had the obligation to protect that information and to ensure by all proper and required means that this information is safeguarded from compromise, theft or loss.

9. When a Data Breach affecting many thousands Consumers occurs, Estée Lauder had the obligation to immediately and accurately notify its Customers in order to help them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience.

10. This lawsuit stems from Estée Lauder's failure to follow these obligations.

11. On July 18, 2023, Estée Lauder publicly announced the occurrence of the Data Breach by way of press release (although not notifying the Plaintiff and Class Members until early September of 2023, if at all, as mentioned above), a copy of the press release issued on the Estée Lauder US (.com) website is communicated herewith as **Exhibit P-4**:

The Estée Lauder Companies Inc. Provides Information on Cybersecurity Incident

PRESS RELEASE, JUL 18, 2023

NEW YORK--(BUSINESS WIRE)-- The Estée Lauder Companies Inc. (NYSE: EL) has identified a cybersecurity incident, which involves an unauthorized third party that has gained access to some of the Company's systems. After becoming aware of the incident, the Company proactively took down some of its systems and promptly began an investigation with the assistance of leading third-party cybersecurity experts. The Company is also coordinating with law enforcement. Based on the current status of the investigation, the Company believes the unauthorized party obtained some data from its systems, and the Company is working to understand the nature and scope of that data.

The Company is implementing measures to secure its business operations and will continue taking additional steps as appropriate. During this ongoing incident, the Company is focused on remediation, including efforts to restore impacted systems and services. The incident has caused, and is expected to continue to cause, disruption to parts of the Company's business operations.

During this period, we thank our employees for their resiliency. Together, we remain focused on our business, consumers and other stakeholders.

Cautionary Note Regarding Forward-Looking Statements
This press release contains forward-looking statements within the meaning of the federal securities laws, including statements regarding the cybersecurity incident and our related responsive actions. The forward-looking statements contained in this press release are based on management's current expectations and are subject to risks and uncertainties that could cause actual results to differ materially from those expressed or implied in the forward-looking statements, including: additional information regarding the extent of the cybersecurity incident that we may uncover during our ongoing investigation; our ability to assess and remedy the incident; and the length and scope of disruptions to the Company's business operations caused by the incident. Additional risks and uncertainties that may cause actual results to differ materially include the risks and uncertainties listed in the Company's filings with the Securities and Exchange Commission (the "SEC"), including the Company's Form 10-K filed with the SEC on August 24, 2022. The Company assumes no responsibility to update forward-looking statements made herein or otherwise.

About The Estée Lauder Companies Inc.
The Estée Lauder Companies Inc. is one of the world's leading manufacturers, marketers, and sellers of quality skin care, makeup, fragrance, and hair care

> products, and is a steward of outstanding luxury and prestige brands globally. The Company's products are sold in approximately 150 countries and territories under brand names including: Estée Lauder, Aramis, Clinique, Lab Series, Origins, M·A·C, La Mer, Bobbi Brown Cosmetics, Aveda, Jo Malone London, Bumble and bumble, Darphin Paris, TOM FORD, Smashbox, AERIN Beauty, Le Labo, Editions de Parfums Frédéric Malle, GLAMGLOW, KILIAN PARIS, Too Faced, Dr.Jart+, and the DECIEM family of brands, including The Ordinary and NIOD.
>
> ELC-C
>
> View source version on businesswire.com: https://www.businesswire.com/news/home/20230718384629/en/
> For inquiries, please visit www.elcompanies.com/en/news-and-media/contact-us.
> Source: The Estée Lauder Companies Inc.

12. The Data Breach was reported by multiple media outlets, as appears from the various articles reporting the issue communicated herewith as **Exhibit P-5**, *en liasse*.

13. The July 19, 2023 bleepingcomputer.com article entitled "Estée Lauder beauty giant breached by two ransomware gangs" (included in P-5), confirms *inter alia* the following:

> Two ransomware actors, ALPHV/BlackCat and Clop, have listed beauty company Estée Lauder on their data leak sites as a victim of separate attacks.
>
> In a disgruntled message to the company, the BlackCat gang mocked the security measures, saying that they were still present on the network.
>
> ...
>
> On their data leak site, Clop ransomware lists Estée Lauder with the simple message "The company doesn't care about its customers, it ignored their security!!!" and a note that they have more than 131GB of the company's data.
>
> BlackCat pressing for negotiation
>
> On Tuesday, BlackCat also added Estée Lauder to their list of victims but the entry is accompanied by a message showing the threat actor's dissatisfaction towards the company's silence to their extortion emails.

"We first wrote to the ELC leadership on 15 July 2023 to their corporate and personal emails. At 9:43 MSK (UTC +3).

"We sent further emails from the same address, but received no reply" - BlackCat ransomware

Referring to the security experts that Estée Lauder brought in to investigate, BlackCat said that despite the company using Microsoft's Detection and Response Team (DART) and Mandiant the network remained compromised and they still had access.

The attacker also said that they did not encrypt any of the company systems, adding that unless Estée Lauder engages in negotiations they will reveal more details about the stolen data.

14. The July 20, 2023 Securityweek.com article entitled "Cosmetics Giant Estée Lauder Targeted by Two Ransomware Groups" (included in P-5), confirms *inter alia* the following:

Two notorious cybercrime groups claim to have targeted the company. One of them is the Cl0p ransomware gang, which claims to have stolen more than 130 gigabytes of information through the MOVEit hack, which has impacted more than 300 organizations worldwide.

The second cybercrime group is the BlackCat/Alphv ransomware gang, which on July 18 claimed that they still had access to the company's systems, despite Microsoft and Mandiant being called in for incident response.

BlackCat hackers said they had not received any response from the company and threatened to reveal more information about the stolen files unless the cosmetics giant responds.

...

This is not the first time Estee Lauder has suffered a data breach. Back in 2020, a researcher discovered that the company had left 440 million records exposed to the internet in an unprotected database.

15. As reported in the P-5 articles, Estée Lauder therefore permitted at least two uncoordinated individual ransomware groups to manage to get into the Estée Lauder systems at the same time, which further evidences the fact that Estée Lauder's information security systems were grossly lacking and wholly inadequate, further demonstrating its faults and negligence.

16. Despite the fact that the Data Breach was announced in multiple media outlets, Estée Lauder never published the information on its Canadian website or social media accounts. This decreased the likelihood that the Class Members would read the press release and was surely intended to minimize the adverse effects of the Data Breach on Estée Lauder's sales.

17. Estée Lauder was negligent in choosing to wait before actually notifying the affected Customers (Class Members), leaving them at greater risk of fraud and identity theft, although Estée Lauder has and had the proper contact information and financial means in order to quickly reach the Class Members.

18. Moreover, Estée Lauder failed to confirm that it would indemnify and hold the Class Members harmless of any losses or damages suffered as a result of the Data Breach.

19. Estée Lauder did not even offer any insurance or credit monitoring services to the Class Members, which is the bare minimum it should have offered under the circumstances.

20. Estée Lauder failed to mandate (and pay for) TransUnion Canada and Equifax Canada to automatically activate credit monitoring services and fraud alerts for Class Members, putting these Class Members at greater risk of fraud.

21. Estée Lauder was negligent and committed faults in this regard since it failed to activate the TransUnion and Equifax services for their Canadian Customers, and many Class Members are not even aware of the Data Breach (in case of not receiving the Notice from Estée Lauder for whatever reason including change of address or bounce-back of emails).

22. By choosing not to automatically activate both credit agencies' credit monitoring services and by not posting the proper fraud alerts for all Class Members, Estée Lauder clearly chose to save money instead of helping protect the Class Members. Indeed, there is a fee payable to TransUnion and Equifax Canada for activating credit monitoring services and/or to post a fraud alert but Estée Lauder is not offering this and has not paid to automatically activate these services.

23. If one calls the 1-899-779-7806 number indicated at the bottom of the of Notice, the Estée Lauder representative is unable to confirm which information was actually stollen regarding the individual Class Members and the representative also confirms that Estée Lauder is not offering any credit monitoring services, insurance or other protections whatsoever to the Class Members.

24. As mentioned above, after becoming aware of the Data Breach, Estée Lauder waited over 56 days before starting to contact some but not all of the Class Members in order to inform them of Data Breach.

25. Accordingly, Defendants failed to promptly and quickly disclose the Data Breach to the Class Members/victims of the Data Breach, further fault committed.

26. Estée Lauder is hereby summoned to confirmed whether it communicated with the unauthorized third parties who perpetuated the Data Breach, to confirm whether it paid the ransoms being claimed by said third parties, and to produce copies of the said communications and/or details of payments made into the Court record.

27. Personal information is a valuable commodity. There is a "cyber black-market" available for criminals to openly post personal information on a number of Internet websites in what is known as the "dark web". This demand increases the likelihood of Class Members falling victim to identity theft.

28. As a result of Estée Lauder's inadequate data security, unauthorized third parties / cyber-criminals now possess the private information of Plaintiff and the Class Members.

29. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. By letting more than 56 days pass before starting to notify Class Members (with many not even informed yet), Estée Lauder failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class Members.

30. Estée Lauder Customers have been and/or will be exposed to fraud and/or identity theft and these Customers have been harmed as a result. Harm to victims of the Data Breach includes without limitation fraudulent charges on their accounts, disbursements incurred such as for purchasing extra insurance, placing a fraud alert on their credit file, loss time and expenses related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards or bank accounts; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; and (e) the general nuisance and annoyance of dealing with all these issues resulting from the Data Breach;

31. On top of actual monetary losses related to fraud and identity theft, Class Members have already and/or will continue to experience stress, anxiety, fear, inconvenience and/or loss of time due to the loss of their personal information, which has made the Class Members potential targets for fraud and/or identity theft.

32. The Class Members have suffered or will suffer certain additional inconveniences and damages including but not limited to the following:

a) Delays in the processing of any future requests or applications for credit in the future;

b) To closely monitor their accounts for possible fraud for all periods subsequent to the loss of information, for many months or years;

c) To be even more attentive than normally necessary concerning the communication of their personal information since they are at threat of social engineering and phishing, due to the higher possibility of fraudulent activity caused by Defendant' loss of the information (as confirmed in the Notice);

d) To inform their financial institutions of the loss of the information by the Defendant and to deal with said financial institutions in order to reduce risk of fraud as much as possible. In this regard, certain Class Members have and/or will close their accounts and open new accounts in order to protect themselves, which will cause further loss of time, inconvenience and costs;

e) Obtaining and reviewing their credit reports, regularly, in order to look for unauthorized transactions or fraud;

f) A negative effect on their credit score.

33. Many Class Members have also paid or will pay certain fees or costs in order to further protect themselves, such as in order to activate a credit monitoring service or in order to purchase fraud insurance or alerts, title or other insurance, to change their personal information such as requesting new driver's licence numbers or Social Insurance Numbers, for credit protection consulting services, etc. Estée Lauder is solely responsible for these costs or fees paid by the Class Members and for the inconvenience caused to Class Members in this regard.

34. Plaintiff invokes *inter alia* the following sections of provincial and federal legislation which apply under the circumstances and Plaintiff respectfully submits that the mere fact that the personal information was entrusted to the Defendant and subsequently lost by Defendant as detailed above constitutes an unlawful violation of the Class Members' fundamental rights, which makes Defendant liable to pay compensatory, moral and punitive damages:

a) Sections 3, 35, 36, 37 and 1621 of the *Civil Code of Quebec*, S.Q. 1991, c. 64;

b) Sections 5 and 49 of the *Charter of Human Rights and Freedoms*, CQRL, c. C-12;

c) Sections 1, 2, 3.1 and following, 10, 13 and 17 of the *Act Respecting the Protection of Personal Information in the Private Sector*, CQRL, c. P-39.1;

d) Sections 2, 3, 5 and 11 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5, as well as its sections 4.1, 4.3, 4.4, 4.7 of its Schedule 1;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF

35. Plaintiff reiterates the above allegations in the present section, as though recited at length.

36. As mentioned above, Plaintiff only received the Notice email (P-2) on September 6, 2023, informing her for the first time that the Data Breach had occurred and that Estée Lauder had permitted unauthorized third party individuals to gain access to her personal information.

37. Very worried about protecting her credit file and assets after learning of the Data Breach, and in order to help protect herself from fraud and identity theft (since Estée Lauder was not offering any protection at all), Plaintiff subscribed to the Equifax Complete Premier credit monitoring service, offered by Equifax Canada, at a monthly price of $24.95 per month (plus taxes), payable on an automatic recurring basis, which amounts she claims from Estée Lauder as damages stemming directly from the Data Breach and the receipt of the Notice, the whole as more fully appears from her Equifax Canada email confirmation, communicated herewith as **Exhibit P-6**.

38. Indeed, and as alleged above, Estée Lauder should have offered such credit monitoring services to the Plaintiff and the Class Members (for multiple years of coverage) when

sending the Notice, but Estée Lauder has refused to offer such protection in order to save money, therefore transferring the burden, cost, loss of time and inconvenience onto the Plaintiff and the Class Members, further faults committed by the Defendant.

39. The Plaintiff and the Class Members, in good faith, were reasonably justified in assuming that Estée Lauder would properly safeguard their personal and financial information, which Estée Lauder clearly did not.

40. As a result of learning that her personal information was lost by Estée Lauder, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and fear due to the loss of personal information.

41. In order to save money, Estée Lauder has failed or refused to mandate and pay for TransUnion and Equifax Canada to immediately and automatically activate credit monitoring and fraud alerts for all affected Class Members such as Plaintiff.

42. All fees payable to TransUnion or Equifax Canada in order to activate these alerts are hereby claimed by Plaintiff and the Class Members from Estée Lauder as damages.

43. TransUnion and Equifax Canada are the two (2) only credit agencies in Canada, both of which Estée Lauder failed to contact immediately about the Data Breach affecting Plaintiff and other Class Members.

44. Estée Lauder had the obligation to ensure, by the most technologically sophisticated means possible and available, that said information was protected and could not be accessed. Estée Lauder failed in this regard and failed to secure this private and highly sensitive information and their negligence and carelessness facilitated the Data Breach, making Estée Lauder liable to pay compensatory, moral and punitive damages.

45. Indeed, the P-5 news articles confirm further faults committed by Estée Lauder, namely that it failed to even encrypt the personal information of its clients and that it had failed to identify and remedy (or shut down) the vulnerabilities in its inadequate systems even after being made aware of the Data Breach.

Punitive Damages:

46. For all of the reasons more fully detailed above, which are reiterated as though recited at length in the present section, Plaintiff respectfully submits that Estée Lauder were grossly and/or intentionally negligent and are liable to pay punitive damages to the Class Members.

47. In fact, without limiting the generality of the forgoing, Estée Lauder was grossly negligent and/or intentionally negligent when it:

a. did not follow or properly implement an effective data security industry standard to protect the Class Members' highly sensitive personal and financial information, which information Estée Lauder allowed to be accessed and/or downloaded/stollen by unauthorized third parties;

b. failed to promptly and clearly notify the Plaintiff and the Class Members of the Data Breach and failed to keep them informed;

c. failed to properly ensure that Plaintiff and Class Members are protected by credit monitoring services by both Equifax Canada and TransUnion and failing to post fraud alerts on the Class Members' credit files immediately after the Data Breach;

d. failed to timely detect and prevent the Data Breach itself;

e. failed to encrypt and protect the Class Members' personal information;

f. failed to close off and/or remedy the vulnerabilities in its systems after being made aware of the Data Breach (leaving the Class Members' information at risk and unsecured);

g. failed to offer indemnification for losses suffered by Class Members; and

h. as mentioned in the P-5 news article: "This is not the first time Estee Lauder has suffered a data breach. Back in 2020, a researcher discovered that the company had left 440 million records exposed to the internet in an unprotected database." Accordingly, Estée Lauder has repeatedly committed such faults putting its clients' information at great risk and such past faults and conduct further warrant the award of punitive damages.

48. Considering the above and considering the fact that Estée Lauder has violated various laws which have been enacted in order to protect the Class Members' personal and/or financial information, Estée Lauder is liable to pay punitive damages to all of the Class Members due to the loss of private information itself, aside from any other compensatory and moral damages suffered by the Class Members.

49. Estée Lauder's above detailed actions qualify the fault as intentional which is a result of wild and foolhardy recklessness in disregard for the rights of the Class Members, with full knowledge of the immediate and natural or at least extremely probable consequences that its action would cause to the Class Members.

50. Estée Lauder's negligence has shown a malicious, oppressive and high-handed conduct that represents a marked departure from ordinary standards of decency. In that event, punitive damages should be awarded to Class Members.

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE CLASS MEMBERS

51. Plaintiff reiterates the above allegations in the present section, as though recited at length.

52. Class Member had their personal information lost by Estée Lauder as described hereinabove, and/or received the Notice from Estée Lauder.

53. Class Members have or will experience stress, anxiety, inconvenience, loss of time, and/or fear due to the loss of personal information and/or the receipt of the Notice. Estée Lauder has already admitted and confirmed that the Plaintiff and the Class Members will suffer inconvenience as a result of the Data Breach (as confirmed in the P-2 Notice).

54. Class Members have to closely monitor their accounts and emails looking for possible fraud and phishing, from now on and for all periods subsequent to the loss of information.

55. Class Members will be inconvenienced by any safety measures that may become necessary in order to prevent further fraud exposure, such as signing up for credit monitoring service, posting an alert on their accounts or credit files, changing their personal information or account numbers, transferring money from one account to another, closing and opening accounts, paying for and dealing with NSF or other bank charges or interest, etc.

56. Furthermore, every Class Member may be required to pay costs or fees in order to sign up for such credit monitoring, to post an alert on their accounts or credit files, to change their personal information, to purchase insurance, or in order to otherwise protect themselves from further fraud exposure.

57. The Class Members' credit score may also be negatively affected as a result of the Data Breach.

58. Moreover, as mentioned above, it is likely that many Class Members have not been notified of the loss of their information, making them still at great risk of fraud or identity theft.

59. Every Class Member can still fall victim to fraud or identity theft, in the future, due to Estée Lauder's negligence in the safekeeping of their personal information and negligence in the way it handled itself after being made aware of this Data Breach.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

60. The composition of the Group makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings (Article 575 (3) C.C.P.) for the following reasons.

61. Plaintiff is unaware of the specific number of persons included in the Class but Plaintiff estimates that hundreds of thousands of Canadian Class Members have been impacted by the Data Breach, considering the very significant success and market share of Estée Lauder's various brands offered in Canada. Estée Lauder is hereby summoned to confirm the total number of affect Class Members in Canada in general, and in Quebec particularly.

62. Class Members are numerous and are scattered across the entire province and country since Estée Lauder offers its products across the country, including Quebec.

63. In addition, given the costs and risks inherent in an action before the Courts, many people will hesitate to institute an individual action against the Estée Lauder. Even if the Class Members themselves could afford such individual litigation, the Court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues raised by Estée Lauder's conduct would increase delay and expense to all parties and to the Court system;

64. Moreover, a multitude of actions instituted risks leading to contradictory judgments on issues of fact and law that are similar or related to all Class Members;

65. These facts demonstrate that it would be impractical, if not impossible, to contact each and every Class Member to obtain mandates and to join them in one action;

66. In these circumstances, a class action is the only appropriate procedure for all of the Class Members to effectively pursue their respective rights and have access to justice;

67. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely Estée Lauder's negligence and fault;

68. The claims of the Class Members raise identical, similar or related issues of law and fact (Article 575 (1) C.C.P.), namely:

(a) Did Defendant commit a fault regarding the storage and the safe-keeping of the personal information of the Class Members?

(b) Did Defendant commit a fault by delaying the notification to Class Members that a Data Breach had occurred?

(c) Did Defendant commit a fault due to the deficiencies of the notices and information given to Class Members about the Data Breach?

(d) Is Defendant liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

69. The interests of justice favour that this application be granted in accordance with its conclusions.

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

70. The action that Plaintiff wishes to institute for the benefit of the Class Members is an action in damages.

71. The facts alleged herein appear to justify the conclusions sought by the Plaintiff (Article 575 (2) C.C.P.), namely the following conclusions that Plaintiff wishes to introduce by way of an originating application:

> **GRANT** the Class Action of Plaintiff on behalf of all the Class Members against Defendant;
>
> **CONDEMN** Defendant to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendant's loss of Class Members' information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendant to pay to the Class Members punitive damages for the unlawful and intentional interference with their right to privacy and **ORDER** collective recovery of these sums;
>
> **THE WHOLE** with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees and publication fees to advise Class Members;

72. Plaintiff suggests that this class action be exercised before the Superior Court in the District of Montreal for the following reasons:

a) Plaintiff resides in the District of Montreal;

b) A great number of Class Members reside in the judicial District of Montreal and/or provided their personal and financial information to Defendant in the District of Montreal;

c) Defendant carries on business in the District of Montreal;

d) Defendant has establishments in the District of Montreal;

e) The undersigned attorneys representing the Plaintiff and the proposed Class practice in the District of Montreal;

73. Plaintiff, who is requesting to be appointed as Representative Plaintiff, is in a position to properly represent the Class Members (Article 575 (4) C.C.P.), since:

a) Her personal information was lost by Defendant as described hereinabove;

b) She has already and will continue to suffer anxiety, inconvenience, stress, loss of time, and fear, as well as out of pocket expense, as a result of said loss of information;

c) She may in the future fall, victim to fraud and/or identity theft because of Defendant's loss of her personal information;

d) She understands the nature of the action and has the capacity and interest to fairly and adequately protect and represent the interest of the Class Members;

e) She is available to dedicate the time necessary for the present action before the Courts of Quebec and to collaborate with Class Counsel in this regard and Plaintiff is ready and available to manage and direct the present action in the interest of the Class Members that Plaintiff wishes to represent;

f) Plaintiff is determined to lead the present file until a final resolution of the matter, the whole for the benefit of the Class Members;

g) Her interests are not antagonistic to those of other Class Members;

h) She has given the mandate to the undersigned attorneys to obtain all relevant information to the present action and intends to keep informed of all developments;

i) She has given the mandate to the undersigned attorneys to post the present matter on their firm website in order to keep the Class Members informed of the progress of these proceedings and in order to more easily be contacted or consulted by said Class Members.

j) She, with the assistance of the undersigned attorneys, is ready and available to dedicate the time necessary for this action and to collaborate with other Class Members and to keep them informed;

74. The present application is well founded in fact and in law;

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present Application;

AUTHORIZE the bringing of a class action in the form of an Application to institute proceedings in damages in the District of Montreal;

APPOINT the Plaintiff as the Representative Plaintiff representing all persons included in the Class herein described as:

All persons in Canada:

(i) whose personal or financial information held by Estée Lauder was compromised in a data breach which occurred on or before July 12, 2023, or

(ii) who received an email or letter from Estée Lauder, dated on or about September 5, 2023, informing them of such data breach;

or any other Group(s) or Sub-Group(s) to be determined by the Court;

IDENTIFY the principle issues of law and fact to be treated collectively as the following:

(a) Did Defendant commit a fault regarding the storage and the safe-keeping of the personal information of the Class Members?

(b) Did Defendant commit a fault by delaying the notification to Class Members that a Data Breach had occurred?

(c) Did Defendant commit a fault due to the deficiencies of the notices and information given to Class Members about the Data Breach?

(d) Is Defendant liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

> **GRANT** the Class Action of Plaintiff on behalf of all the Class Members against Defendant;
>
> **CONDEMN** Defendant to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendant's loss of Class Members' information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendant to pay to the Class Members punitive damages for the unlawful and intentional interference with their right to privacy and **ORDER** collective recovery of these sums;
>
> **THE WHOLE** with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees and publication fees to advise Class Members;

DECLARE that all Class Members who have not requested their exclusion from the Class in the prescribed delay to be bound by any Judgment to be rendered on the class action to be instituted;

FIX the delay of exclusion at 30 days from the date of the publication of the notice to the Class Members;

ORDER the publication or notification of a notice to the Class Members in accordance with Article 579 C.C.P., pursuant to a further order of this Honorable Court;

ORDER that said notice be posted and available on the home page of Defendant's various brand and corporate websites, Facebook account(s), Instagram account(s) and X (formerly Twitter) account(s), and **ORDER** Defendant to send the notice by email with proof of receipt and by direct mail to all Class Members;

ORDER Defendant to pay for all said publication/notification costs;

THE WHOLE with costs including without limitation the Court filing fees herein, expert fees, stenography fees, bailiff and/or process server fees, and all costs related to preparation and publication of the notices to Class Members.

MONTREAL, September 7, 2023

(s) *Lex Group Inc.*

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7
Telephone: 514.451.5500 ext. 101
Fax: 514.940.1605

SUMMONS

(Articles 145 and following C.C.P.)

Filing of a judicial application

Take notice that the Plaintiff(s) has filed this application in the office of the Superior Court of Quebec in the judicial district of Montreal.

Defendant's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal, situated at 1, Notre-Dame Est, Montréal, Québec within 15 days of service of the application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the Plaintiff's lawyer or, if the Plaintiff is not represented, to the Plaintiff.

Failure to answer

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgment may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

Content of answer

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the cases required by the Code, cooperate with the Plaintiff in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of the summons or, in family matters or if you have no domicile, residence or establishment in Québec, within 3 months after service;
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Change of judicial district

You may ask the court to refer the originating application to the district of your domicile or residence, or of your elected domicile or the district designated by an agreement with the Plaintiff.

If the application pertains to an employment contract, consumer contract or insurance contract, or to the exercise of a hypothecary right on an immovable serving as your main residence, and if you are the employee, consumer, insured person, beneficiary of the insurance contract or hypothecary debtor, you may ask for a referral to the district of your domicile or residence or the district where the immovable is situated or the loss occurred. The request must be filed with the special clerk of the district of territorial jurisdiction after it has been notified to the other parties and to the office of the court already seized of the originating application.

Transfer of application to Small Claims Division

If you qualify to act as a Plaintiff under the rules governing the recovery of small claims, you may also contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the Plaintiff's legal costs will not exceed those prescribed for the recovery of small claims.

Calling to a case management conference

Within 20 days after the case protocol mentioned above is filed, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing this, the protocol is presumed to be accepted.

Exhibits supporting the application

In support of the application, the Plaintiff intends to use the following exhibits:

Exhibit P-1: Copy of the *Registre des enterprises* report concerning ESTÉE LAUDER COSMETICS LTD,

Exhibit P-2: September 6, 2023 email from Defendant to Plaintiff;

Exhibit P-3: Estée Lauder Canada Consumer Privacy Policy;

Exhibit P-4: "The Estée Lauder Companies Inc. Provides Information on Cybersecurity Incident" Press release dated July 18, 2023;

Exhibit P-5: Various news articles, *en liasse*;

Exhibit P-6: Equifax Canada confirmation email to the Plaintiff.

These exhibits are available on request.

Notice of presentation of an application

If the application is an application in the course of a proceeding or an application under Book III, V, excepting an application in family matters mentioned in article 409, or VI of the Code, the establishment of a case protocol is not required; however, the application must be accompanied by a notice stating the date and time it is to be presented.

DO GOVERN YOURSELF ACCORDINGLY.

MONTREAL, September 7, 2023

(s) *Lex Group Inc.*

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff

NOTICE OF PRESENTATION

(Article 223 of the Superior Court's Directives for the Montreal District)

TO: ESTÉE LAUDER COSMETICS LTD, legal person having its head office at 161 Commander Blvd., Agincourt, Province of Ontario, M1S 3K9, and having its principal establishment located at 3035 boulevard Carrefour Laval, Unit T-009, in the City and District of Laval, Province of Québec H7T 1C7;

Defendant

TAKE NOTICE that the present Application for Authorization to Institute a Class Action will be presented before the Superior Court, at the Montreal Courthouse located at 1 Notre-Dame Street East, in the city and district of Montreal, at a date to be determined by the coordinating Judge of the class actions division.

MONTREAL, September 7, 2023

(s) *Lex Group Inc.*

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff