C A N A D A

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

№ : 500-06-

(Class Action)

SUPERIOR COURT

A., having elected domicile for the purposes of the present lawsuit at the offices of her attorneys, namely at Lex Group Inc., 4101 Sherbrooke Street West, Westmount, Quebec, H3Z 1A7;

Plaintiff

vs.

LVMH FRAGRANCE BRANDS CANADA LTD., legal person having its head office at 1002-180 Bloor Street West, Toronto, Province of Ontario, M5S 2V6, and having its elected domicile and *fondé de pouvoir* at 2000-630 boul. René-Lévesque Ouest, in the City and District of Montreal, Province of Quebec, H3B 1S6;

-and-

LVMH WATCH & JEWELRY CANADA LTD., legal person having its head office at 30 East Beaver Creek Road, Suite 212 Richmond Hill, Province of Ontario, L4B 1J2, and having its elected domicile at 26E-1501 avenue McGill College, in the City and District of Montreal, Province of Quebec, H3A 3M8;

-and-

LOUIS VUITTON CANADA, INC., legal person having its head office at 4999-199 ST Bay, Toronto, Province of Ontario, M5L 1A9, and having its *fondé de* pouvoir at

3000-1 Place Ville Marie, in the City and District of Montreal, Province of Quebec, H3B 4N8;

-and-

PARFUMS CHRISTIAN DIOR CANADA INC., legal person domiciled at 2000-630 boul. René-Lévesque Ouest, in the City and District of Montreal, Province of Quebec, H3B 1S6;

-and-

CHRISTIAN DIOR COUTURE CANADA INC., legal person domiciled at 2002-365 ST Bloor East, Toronto, Province of Ontario, M5W 3L4, and having its elected domicile at 2000-630 boul. René-Lévesque Ouest, in the City and District of Montreal, Province of Quebec, H3B 1S6;

-and-

TIFFANY & CO. CANADA, legal person having its head office at M108-150 Bloor Street West, Toronto, Province of Ontario, M5S 2X9, and having its principal establishment located at 1290 rue Sherbrooke Ouest, in the City and District of Montreal, Province of Quebec, H3G 1H5.

Defendants

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:

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

The LVMH Group: All persons in Canada: (i) whose personal or financial information was held by Defendants (or another member of the LVMH Moët Hennessy Louis Vuitton SE group of companies) and was compromised in the data breach which occurred between on or around January 26, 2025 and on or around June 7, 2025, or (ii) who received an email or letter from Defendants (or another member of the LVMH Moët Hennessy Louis Vuitton SE group of companies), as of May 13, 2025, informing them of such data breach;
The Louis Vuitton Subgroup: All persons in Canada: (i) whose personal or financial information held by Louis Vuitton was compromised in a data breach which occurred on or around June 7, 2025, or (ii) who received an email or letter from Louis Vuitton, dated on or about July 23, 2025, informing them of such data breach;
The Dior Subgroup: All persons in Canada: (i) whose personal or financial information held by Dior was compromised in a data breach which occurred on or around January 26, 2025, or

(ii) who received an email or letter from Dior, dated between on or about May 13 and on or about July 18, 2025, informing them of such data breach;
The Tiffany & Co. Subgroup: All persons in Canada: (i) whose personal or financial information held by Tiffany & Co. was compromised in a data breach which occurred on or around April 8, 2025, or (ii) who received an email or letter from Tiffany & Co., dated on or about May 26, 2025, 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)**").

LVMH and the Defendants

2. **LVMH Moët Hennessy Louis Vuitton SE** is a French multinational holding company, commonly known as LVMH, (hereinafter "**LVMH**"), led by billionaire **Bernard Arnault**.

3. As appears from the LVMH global website's history page (https://www.lvmh.com/en/our-group/history), a copy of which is communicated herewith, as **Exhibit P-1**:

   a) "LVMH was created in 1987 through the merger of Moët Hennessy and Louis Vuitton, ushering in a new era for the luxury industry.";

   b) "Bernard Arnault has led the Group since 1989 and is the majority shareholder, pursuing a clearly focused vision: make LVMH the world leader in luxury. An unprecedented portfolio of iconic brands makes LVMH unique in the world, a Group that has continued to grow and thrive since its founding."

4. Indeed, and as appears from said Exhibit P-1 and from the full list of *Maisons* (houses or brands) included in the LVMH group as listed on the https://www.LVMH.com/en/press webpage, a copy of which is communicated herewith as **Exhibit P-2**, LVMH operates in many sectors, including without limitation in wines & spirits, fashion & leather goods, perfumes & cosmetics, watches & jewelry, selective retailing and other activities. As

appears from P-2, the LVMH groups owns and operate many of the world's most iconic and well-known luxury brands, including without limitation: Celine, Christian Dior, Fendi, Givenchy, Kenzo, Loewe, Louis Vuitton; Marc Jacobs, Bulgari, Hublot, Tag Huere, Tiffany & Co, Zenith, and Sephora.

5. **Defendant LVMH Fragrance Brands Canada Ltd.** is part of LVMH and, itself and through its affiliated companies which are all linked to LVMH, is one of the world's leading manufacturers, marketers, and sellers of quality fragrances and beauty products. It does business in Quebec under *inter alia* the following names: LVMH FRAGRANCE BRANDS CANADA LTD., PARFUMS GIVENCHY CANADA, LTD., LVMH MARQUES DE PARFUMS and PARFUMS GIVENCHY CANADA, LTÉE (hereinafter "**LVMH Fragrance Brands Canada**"), the whole as appears more fully from a copy of the *Registre des enterprises du Québec* report concerning LVMH Fragrance Brands Canada Ltd., communicated herewith as **Exhibit P-3**.

6. As appears from Exhibit P-3, LVMH Fragrance Brands Canada has an elected domicile and *fondé de pouvoir* in Montreal (Quebec) and is owned by LVMH member **LVMH Fragrance Brands S.A.S.** in France.

7. **Defendant LVMH Watch & Jewelry Canada Ltd.** is part of LVMH and, itself and through its affiliated companies which are all linked to LVMH, is one of the world's leading manufacturers, marketers, and sellers of quality watches and jewelry. It does business in Quebec under *inter alia* the following names: LVMH MONTRES ET JOAILLERIE CANADA LTÉE, and LVMH WATCH & JEWELRY CANADA LTD. (hereinafter "**LVMH Watch & Jewelry Canada**"), the whole as appears more fully from a copy of the *Registre des enterprises du Québec* report concerning LVMH Watch & Jewelry Canada Ltd., communicated herewith as **Exhibit P-4**.

8. As appears from Exhibit P-4, LVMH Watch & Jewelry Canada has an elected domicile in Montreal (Quebec).

9. **Defendant Louis Vuitton Canada, Inc.** is part of LVMH and, itself and through its affiliated companies which are all linked to LVMH, is one of the world's leading manufacturers, marketers, and sellers of quality luxury bags, leather goods, shoes, fragrance, watches, jewellery, clothing, and accessories. It does business under *inter alia* the following names: LOUIS VUITTON CANADA, INC., LOUIS VUITTON @OGILVY, and LOUIS VUITTON (together with its worldwide affiliated Louis Vuitton entities hereinafter referred to collectively as "**Louis Vuitton**"), the whole as appears more fully from a copy of the *Registre des enterprises du Québec* report concerning Louis Vuitton Canada, Inc., communicated herewith as **Exhibit P-5**.

10. **Defendant Parfums Christian Dior Canada Inc.** is part of LVMH and declares on its website that: "Parfums Christian Dior Canada Inc. (hereinafter **"Parfums Christian Dior"**) and its affiliates create, design and distribute worldwide luxury beauty products for both men and women including but not limited to fragrances, makeup, and skincare, in particular those bearing Parfums Christian Dior labels, such as: Christian Dior Paris, Dior, and CD", the whole as more fully appears from the Parfums Christian Dior Canada Inc. Legal terms document on its Canadian dior.com website, communicated herewith as **Exhibit P-6**.

11. The Exhibit P-6 Parfums Christian Dior Canada Inc. Legal terms document links to a Christian Dior Privacy Policy document entitled Privacy Statement- Parfums Christian Dior (last updated in July 2025, namely after the data breach, Defendants having apparently replaced the version posted immediately prior to the Dior Data Breach), a copy of which is communicated herewith as **Exhibit P-7**, which confirms the following:

> "This Privacy Statement ("Statement") is provided by The Maison Christian Dior Couture and The Maison Parfums Christian Dior (together, "Christian Dior," "Dior," "Maisons," "we" or "us"), a luxury retail and wholesale brand with its global headquarters in Paris, France and its United States and Canada headquarters in New York, New York.".

12. In addition, the dior.com Canadian website has another Christian Dior Privacy Policy document, this time entitled Privacy Statement – Christian Dior Couture (also last updated in July 2025, namely after the data breach, Defendants having apparently replaced the version posted immediately prior to the Dior Data Breach), a copy of which is communicated herewith as **Exhibit P-8**. It also states the following:

> "This Privacy Statement ("Statement") is provided by The Maison Christian Dior Couture and The Maison Parfums Christian Dior (together, "Christian Dior," "Dior," "Maisons," "we" or "us"), a luxury retail and wholesale brand with its global headquarters in Paris, France and its United States and Canada headquarters in New York, New York.".

13. As appears from a copy of the *Registre des enterprises du Québec* report concerning Defendants Parfums Christian Dior Canada Inc., communicated herewith as **Exhibit P-9**, it does business under a long list of other names as well.

14. As appears from Exhibit P-9, Parfums Christian Dior Canada Inc. is domiciled in Montreal (Quebec) and declares that its ultimate beneficial owners (*Liste des bénéficiaires ultimes*) are LVMH itself (namely **LVMH Moët Hennessy Louis Vuitton S.E.**, in Franch) with over 75% of the voting rights, and billionaire **Bernard Arnault** (in France) who is listed as having the *contrôle de fait*.

15. **Defendant Christian Dior Couture Canada Inc.** is part of the LVMH and, itself and

through its affiliated companies which are all linked to LVMH, is one of the world's leading manufacturers, marketers, and sellers of quality luxury bags, leather goods, shoes, fragrance, watches, jewellery, clothing, and accessories. It does business under *inter alia* the following names: BABY DIOR, CD, CD DE CHRISTIAN DIOR, CHRISTIAN DIOR, CHRISTIAN DIOR BOUTIQUE, CHRISTIAN DIOR MONSIEUR, DIOR, DIOR 2, D's, and MISS DIOR. Plaintiff communicates a copy of the *Registre des enterprises du Québec* report concerning Christian Dior Couture Canada Inc. as **Exhibit P-10**.

16. As appears from Exhibit P-10, Christian Dior Couture Canada Inc. has an elected domiciled in Montreal (Quebec) and declares that its ultimate beneficial owners (*Liste des bénéficiaires ultimes*) are LVMH itself (namely **LVMH Moët Hennessy Louis Vuitton S.E.**, in Franch) with over 75% of the voting rights, and billionaire **Bernard Arnault** (in France) who is listed as having the *contrôle de fait*.

17. Defendants **Parfums Christian Dior Canada Inc.** and **Christian Dior Couture Canada Inc.**, together with their worldwide affiliated entities and LVMH are hereinafter referred to collectively as "**Dior**".

18. **Defendant Tiffany & Co. Canada** is part of the LVMH and, itself and through its affiliated companies which are all linked to LVMH, is one of the world's leading manufacturers, marketers, and sellers of quality luxury jewellery and accessories. It does business under *inter alia* the following names: TIFFANY & CO. CANADA and TIFFANY & CO. ® (together with its worldwide affiliated Tiffany & Co. entities hereinafter referred to collectively as "**Tiffany**"), the whole as appears more fully from a copy of the *Registre des enterprises du Québec* report concerning Tiffany & Co. Canada, communicated herewith as **Exhibit P-11**.

19. As appears from the previous allegations and exhibits above, the Defendants are acting together with LVMH itself and other LVMH related entities, through a very complicated and convoluted global corporate structure. They are clearly interrelated and operating a common enterprise in Quebec and Canada. In addition, the facts alleged below clearly also link the data breach to the same global LVMH structure and entities. Defendants are therefore solidarily liable for the damages claimed by the Plaintiff and Class Members here. Plaintiff reserves the right to amend these proceedings in order to include further documents and/or further solidarily liable defendants herein.

The Situation

20. On or about **January 26, 2025**, unauthorized third parties gained access to Dior's systems and obtained, accessed, and exfiltrated the personal information and personal

data of its customers (hereinafter the **"Dior Data Breach"**).

21. As mentioned above, Dior is part of and in fact beneficially owned by LVMH.

22. Indeed, the Dior Data Breach affected the personal information and data of Dior customers worldwide, including in Canada and the province of Quebec.

23. The compromised data included, without limitation, customer contact information, dates of birth, passport and government-issued identification numbers, and Social Security Numbers (SSNs) in the USA. This constitutes highly sensitive information, the unauthorized exposure of which placed the affected Class Members at significant risk of fraud, identity theft, and other forms of harm.

24. The Dior Data Breach was first reported in **South Korea**, where affected customers began receiving notification of the breach before those in other jurisdiction. The breach itself was only discovered and confirmed by Dior on or about **May 7, 2025**, namely 102 days after the initial intrusion. Dior subsequently began sending breach notifications to customers on or about May 13, 2025, in certain jurisdictions.

25. A sample of the July 18, 2025 Dior notice to US affected customers, available online, is communicated herewith as **Exhibit P-12** (hereinafter the **"Dior Notice"**). The Dior Notice is dated an excessive total of 175 days after the Dior Data Breach had apparently occurred and/or commenced and an excessive 73 days after Dior was apparently first made aware of the breach, and reads as follows:

DIOR

NOTICE OF DATA BREACH

July 18, 2025

Dear Sample A. Sample,

At the House of Dior, we take the security of your personal information very seriously. We are writing to let you know about a recent cybersecurity incident that impacted a database we use to hold your personal

information. We are contacting you to explain the circumstances of the incident, the types of information involved, and steps you can take.

What happened? On May 7, 2025, we identified a potential cybersecurity incident. We promptly conducted an investigation, supported by leading third-party cybersecurity experts. Our investigation determined that an unauthorized party was able to gain access to a Dior database that contained information about Dior clients on January 26, 2025. Dior promptly took steps to contain the incident, and we have no evidence of subsequent unauthorized access to Dior systems.

What information was involved? The Dior database contained personal information such as first and last name, contact information, address, date of birth, and other information you may have provided to Dior, such as a passport or government ID number, including in a small number of cases, Social Security Number. **Importantly, no payment information, including bank account or payment card information, was contained in the database accessed.**

What are we doing? We have conducted an investigation with the support of leading third-party cybersecurity experts and notified law enforcement. We have taken steps designed to enhance our network security and help prevent future incidents. The third-party cybersecurity experts have verified that the incident is contained, and that there is no evidence that the unauthorized third party was able to access Dior systems except on January 26, 2025.

To help protect your identity, we are offering you a complimentary 24-month membership of Experian IdentityWorksSM credit monitoring. This product provides you with credit monitoring, fraud resolution services, and identity theft insurance. If you would like to take advantage of this offer, please follow the steps in the instructions on Attachment A.

What can you do? We recommend you remain vigilant for incidents of fraud and identity theft. We also recommend that you continue to review your financial accounts, account statements, and free credit reports for any suspicious activity. Attachment A to this letter contains more information about steps you can take to protect yourself against potential fraud and identity theft.

For more information: We remain committed to maintaining the security of your personal information. For any questions or concerns about this letter

or support with enrollment to the Experian IdentityWorks monitoring, please contact **1-833-918-5938.**

...

CHRISTIAN DIOR COUTURE
30, avenue Montaigne, 75008, Paris

26. As appears from the Dior Notice, Dior has confirmed and admitted that the affected Class Members will suffer inconvenience and that: "We recommend that you remain vigilant for incidents of fraud and identity theft. We also recommend you continue to review your financial accounts, account statements, and free credit reports for any suspicious activity.".

27. Accordingly, Dior is confirming and admitting that the affected Class Members are now at risk of fraudsters using the stolen information and date in order to commit identity theft and/or fraud.

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

- First and last name,
- Contact information,
- Address,
- Date of birth,
- Other information provided to Dior such as passport or government ID number,
- Social Security Number.

29. This information is highly sensitive and essential to the security of the affected Class Members. In particular, the date of birth, passport number or other government ID number, and Social Security Number (or Social Insurance Number in Canada) are critical data point frequently used in identity verification and, if exposed, significantly increases the risk of identity theft and/or fraud.

30. That being said, the Christian Dior Privacy Policy (Exhibit P-7), confirms that Dior indeed

collects much more information from its customers, namely:

> "Depending on your interactions with us, personal data we receive may include information related to:
>
> - Your identity and your contact details (e.g., name, address, email address, date of birth)
> - Your interests and your preferences (as you may provide in creating your Dior profile);
> - Your purchases (in store or online, including your orders, their tracking information, your purchase invoices, the amount and type of your purchase) and any returns or exchanges;
> - Your in store or online digital experiences (there is a short term collection of photos or images in relation to virtual beauty technology; however, our online digital and try-on experiences are operated by third-party vendors, and no information can be retrieved by Dior or any of its partners after your session closes), as per our contracts with these vendors;
> - Your use of our online images, including when you visit and interact with them, what pages you accessed, and your interaction with our features. We also receive information to help detect and prevent consumer fraud, including but not limited to browser and keyboard language settings, whether data is automatically filled or manually entered, whether data is manually entered or copy and pasted, and proxy detection (dior.com, social media pages, partner websites (e.g. for events) and databases (e.g. for data storage and maintenance));
> - Your Dior account log-in information when you create an account on dior.com;
> - Your financial information to process your orders;
> - Your requests through our client services or our public relations department;
> - Your publications and mentions of our products on social networks;
> - The Dior events you attend;
> - The Dior hospitality locations you attend (such as our cafés);
> - Any self-reported undesirable side-effects concerning any of our products (for Parfums Christian Dior products)."

31. The July 2025 Christian Dior Privacy Policy (Exhibit P-8) is quasi identical to the above, adding the following in the second item listed:

> "Your Dior profile with information you may provide when creating your account (a) in a boutique (such as with your interests and your preferences) or (b) on dior.com (to manage your wish lists or see your transactions);".

32. This 175-day delay between the Dior Data Breach occurring and/or commencing and Defendants' first detection of the Dior Data Breach confirms the significant deficiencies and inadequacy in Defendants' security systems and IT protocols, which failed to provide timely alerts, pop-ups, messages, protection, etc. regarding the Dior Data Breach when it began. In addition, Defendants waited further months before starting to notify the affected clients. All of these represent faults and negligence committed by the Defendants, which left the affected Class Members fully exposed to greater risks of fraud and identity theft.

33. Thereafter, on or about **April 8, 2025**, unauthorized third parties gained access to Tiffany & Co.'s systems and obtained, accessed, and exfiltrated the personal information and personal data of its customers (hereinafter the "**Tiffany & Co. Data Breach**").

34. As mentioned above, Tiffany & Co. is part of LVMH.

35. Indeed, the Tiffany & Co. Data Breach similarly impacted customers worldwide, including in Canada and the province of Quebec. The breached data included, without limitation, customer names, addresses, phone numbers, email addresses, internal customer ID numbers, and purchase history. Again, this is extremely sensitive information that can pose a significant threat to the affected Class members' privacy and security.

36. That being said, the Tiffany & Co. Privacy Policy, which was apparently updated after the Tiffany & Co. Data Breach, a copy of which is communicated herewith as **Exhibit P-13**, confirms that Tiffany & Co. indeed collects much more information from its customers, namely:

> "We collect personal information about you through various Channels as described above. The types of personal information we collect include:
>
> - contact information (such as name, postal address, email address, and mobile or other telephone number);
> - username and password;
> - payment information (such as your payment card number, expiration date, authorization number or security code, delivery address, and billing address);
> - customer service information (such as customer service inquiries, comments, and repair history);
> - photographs, comments and other content you provide;
> - information regarding your personal or professional interests, date of birth, marital status, demographics, and experiences with our products and contact preferences;
> - information you submit in connection with a career opportunity at Tiffany, such as contact details, information in your résumé (including work history, education and language skills) and details about your current employment;
> - purchase and transaction information;
> - contact information you provide about friends or other people you would like us to contact;
> - location data (such as data derived from your IP address, country and/or zip code) and the precise geolocation of your mobile device where we have provided notice and choice, as appropriate;
> - clickstream data and other information about your online activities (such as information about your devices, browsing actions and usage patterns), including across the Online Channels and third-party websites, that we obtain through the use of cookies, web beacons and similar technologies (see our Cookie Policy);
> - information we may obtain from our third-party service providers; and other personal information we obtain through our Channels. We also use the information in other ways for which we provide specific notice at the time of collection and obtain your consent to the extent required by applicable law. For example, if you are approved for Tiffany Select Financing, we use the personal information you provide on your application form and that we receive from consumer reporting agencies or your employer to assess your application, verify your creditworthiness and to manage our risks and, if you are approved to receive financing, for purposes related to the extension of credit, and the administration of the credit facility, including any collection of debt.

- Information you provide in connection with an application for Tiffany Select Financing, including contact information, date of birth, and employment information (such as employer and income)"

37. Tiffany Korea was the first to officially confirm the breach and issue notifications to affected customers in **South Korea**, just as had occurred during the Dior Data Breach detailed above.

38. The Tiffany & Co. Data Breach was apparently discovered by Tiffany & Co. two days after Dior had discovered the Dior Data Breach, namely on or about **May 9, 2025**. This was an excessive 31 days after the breach in question had occurred and/or commenced. Customer notifications only began 17 days later on or about **May 26, 2025**.

39. This 31-day delay between the Tiffany & Co. Data Breach occurring and/or commencing and Defendants' first detection of the Tiffany & Co. Data Breach confirms the significant deficiencies and inadequacy in Defendants' security systems and IT protocols, which failed to provide timely alerts, pop-ups, messages, protection, etc. regarding the Tiffany & Co. Data Breach when it began. In addition, Defendants waited a further 17 days before starting to notify the affected clients. All of these represent faults and negligence committed by the Defendants, which left the affected Class Members fully exposed to greater risks of fraud and identity theft.

40. In addition, LVMH and members of its group, including Dior (as detailed above) had already been alerted to the Dior Data Breach. Nonetheless, Tiffany & Co. did not secure its own systems and permitted and facilitated the Tiffany & Co. Data Breach to occur and/or continue.

41. Both the Dior Data Breach and the Tiffany & Co. Data Breach were first confirmed by Defendants in **South Korea** (and the same is true for the June 7, 2025 Louis Vuitton Data Breach detailed hereinbelow).

42. In fact, on or about **June 7, 2025**, unauthorized third parties gained access to Louis Vuitton's systems and obtained, accessed and exfiltrated the personal information and personal data of its customers, including Plaintiff and the other Class Members (hereinafter the "**Louis Vuitton Data Breach**").

43. The Louis Vuitton Data Breach affected and breached the personal information and data of all Louis Vuitton customers around the world, including Canada (and Quebec).

44. It was on **July 2, 2025** that Louis Vuitton proports to having been made aware of the Louis Vuitton Data Breach for the first time (namely an excessive 25 days after the data breach has occurred and/or commenced). Louis Vuitton then began the process of notifying

affected customers across multiple jurisdictions worldwide.

45. On or about the week of July 7, 2025, Louis Vuitton issued data breach notifications to its customers in **South Korea** and Turkey, but not to Canadians.

46. On or about July 11, 2025, notifications were sent to affected customers in the United Kingdom, Italy, and Sweden, but not to Canadians.

47. On or about July 17, 2025, Louis Vuitton notified its customers in Hong Kong, but not to Canadians.

48. On or about July 21, 2025, Louis Vuitton notified its customers in Australia, but not to Canadians.

49. Finally, it was only on or about **July 23, 2025** that Louis Vuitton started notifying some of its Canadian customers, including the Plaintiff.

50. There is presently no confirmation as to how many times the unauthorized third parties accessed the Louis Vuitton systems and customer data between June 7, 2025 and July 2, 2025.

51. This 25-day delay between the Louis Vuitton Data Breach occurring and/or commencing and Defendants' first detection of the Louis Vuitton Data Breach confirms the significant deficiencies and inadequacy in Defendants' security systems and IT protocols, which failed to provide timely alerts, pop-ups, messages, protection, etc. regarding the Louis Vuitton Data Breach when it began. In addition, Defendants waited close to a further month before starting to notify the affected clients. All of these represent faults and negligence committed by the Defendants, which left the Plaintiff and affected Class Members fully exposed to greater risks of fraud and identity theft.

52. In addition, LVMH and members of its group, including Dior and Tiffany & Co. (as detailed above) had already been alerted to the Dior Data Breach and the Tiffany & Co. Data Breach. Nonetheless, Louis Vuitton did not secure its own systems and permitted and facilitated the Louis Vuitton Data Breach to occur and/or continue.

53. Plaintiff only received the following email from Louis Vuitton on July 23, 2025, a copy of which is communicated herewith as **Exhibit P-14** (hereinafter the "**LV Notice**"), namely an excessive 21 days after the Louis Vuitton Data Breach was first apparently discovered by Louis Vuitton, and an excessive total of 46 days after the Louis Vuitton Data Breach had apparently occurred and/or commenced:

From: Louis Vuitton <notification@service.louisvuitton.com>
Date: July 23, 2025 at 1:05:46 PM EDT
To: (...)
Subject: Important information regarding your personal data from Louis Vuitton Canada
Reply-To: Service Client <no_reply_eng.ca@louisvuitton.com>

Can't see the images? View in browser

LOUIS VUITTON

Important information regarding your personal data from Louis Vuitton Canada

Dear Client,

We regret to inform you that an unauthorized third party temporarily accessed our system and obtained some of your information.

We would like to reassure you that no password nor financial information—such as credit card information, bank details, or other financial accounts, was contained in the database accessed.

At Louis Vuitton, we highly value the trust and the confidential nature of our relationship with you. Hence, the incident is now contained, we have further strengthened the protection of our systems, and we have engaged with leading experts in cybersecurity.

What Happened?

Despite all security measures in place, on July 2, 2025, we became aware of a personal data breach resulting from the exfiltration of certain personal data of some of our clients following an unauthorized access, on 7 June 2025, to our

system.

We would like to assure you that our cybersecurity teams have taken care of the incident with the utmost diligence and attention. Technical measures were immediately taken to contain the incident after its occurrence, notably by blocking the unauthorized access. Louis Vuitton teams are mobilized to cooperate with the competent authorities which have been notified.

What Personal Data Was Involved?
According to our investigation, we have determined that this incident may have concerned some of your personal data: first name, last name, gender, country, phone number, email address, postal address, date of birth, purchases and preferences data.

Our recommendation
Given the nature of the data involved, we warmly recommend that you remain vigilant against any unsolicited communication or other suspicious correspondence, including emails, phone calls or text messages. While we have no evidence that your data has been misused to date, phishing attempts, fraud attempts, or unauthorized use of your information may occur. You should never disclose your Louis Vuitton password to anyone, and you can rest assured that Louis Vuitton will never ask you to disclose it.

Our Commitment to You
At Louis Vuitton, we highly value the trust and the confidential nature of our relationship with our clients. We sincerely apologize for any inconvenience this situation may cause you. Please rest assured that the security and protection of your personal data remain an utmost priority for us. All efforts are constantly being deployed to help prevent similar incident in the future.
For any further questions, please do not hesitate to contact us via the contact details below.
Thank you for your continued trust in Louis Vuitton.

Sincerely,
Louis Vuitton Canada

Customer Service: +1 866 VUITTON --
canadafr@contact.louisvuitton.com

Louis Vuitton Canada
150 Bloor Street West - suite M003 -
M5S 2X9 - Toronto
Canada

Information importante de la part de Louis Vuitton Canada relative à vos données personnelles

Cher(e) Client(e),

Nous avons le regret de vous informer qu'un tiers non autorisé a temporairement pu accéder à notre système et obtenir certaines informations vous concernant.

Nous tenons à vous assurer qu'aucun mot de passe ni aucune information financière telles que des données de carte de paiement, des coordonnées bancaires ou d'autres documents de nature financière ne figurait dans la base de données concernée.

Chez Louis Vuitton, nous attachons une grande importance à la confiance que vous nous accordez et à la confidentialité de nos relations.

Nous avons ainsi renforcé la protection de nos systèmes, fait appel à des experts en cybersécurité et l'incident est désormais maîtrisé.

Que s'est-il passé ?

Malgré toutes les mesures de sécurité en place, le 2 juillet 2025, nous avons pris connaissance d'une violation de données : un accès non autorisé à notre système le 7 juin 2025 a conduit à l'extraction de données personnelles de certains de nos clients.

Nous tenons à vous assurer que nos équipes de cybersécurité ont traité cet incident avec la plus grande diligence et attention. Des mesures techniques ont immédiatement été prises pour maîtriser l'incident, notamment en bloquant l'accès non autorisé. Les équipes Louis Vuitton sont mobilisées et coopèrent avec les

autorités compétentes qui ont été notifiées.

Quelles ont été les données personnelles concernées ?

Sur la base des résultats de l'enquête, cet incident peut concerner certaines de vos données personnelles :
Prénom, Nom, Sexe, Pays, Numéro de téléphone, Adresse électronique, Adresse postale, Date de naissance, Données d'achats et de préférences.

Nos recommandations

Compte tenu de la nature des données concernées, nous vous recommandons de rester particulièrement vigilant face à toute communication non sollicitée ou autre correspondance suspecte, incluant des courriels, des appels téléphoniques ou des SMS. Bien que nous ne disposions d'aucune preuve à ce jour sur l'utilisation frauduleuse de vos données, des tentatives d'hameçonnage, de fraude ou une utilisation non autorisée de vos données, peuvent se produire. Votre mot de passe Louis Vuitton ne doit jamais être divulgué et vous pouvez être assuré que Louis Vuitton ne vous demandera jamais de le communiquer.

Notre engagement envers vous

La Maison attache la plus grande importance à la confiance que nos clients nous accordent ainsi qu'à la confidentialité de nos relations.

Nous vous prions de bien vouloir nous excuser pour tout désagrément que cette situation pourrait vous causer. La sécurité et la protection de vos données personnelles demeurent une priorité absolue et nous déployons constamment tous les efforts nécessaires afin d'éviter qu'un incident similaire ne se reproduise à l'avenir.
Pour toute information complémentaire, nous vous invitons à nous contacter via les coordonnées ci-dessous.
Nous vous remercions de la confiance que vous continuez à accorder à Louis Vuitton.

Sincèrement,
Louis Vuitton Canada

Service Client : +1 866 VUITTON --

canadafr@contact.louisvuitton.com

Louis Vuitton Canada
150 Bloor Street West - suite M003 -
M5S 2X9 - Toronto
Canada

54. As appears from the LV Notice, Louis Vuitton has confirmed and admitted that the Plaintiff and the Class Members will suffer inconvenience and that "given the nature of the data involved, we warmly recommend that you remain vigilant against any unsolicited communication or other suspicious correspondence, including emails, phone calls or text messages.".

55. Louis Vuitton further admits in the LV Notice that "phishing attempts, fraud attempts, or unauthorized use of your information may occur.".

56. The Plaintiff and the Class Members can therefore reasonably rely on these admissions, namely that the Louis Vuitton Data Breach represents a reasonably real and current threat and risk of fraud.

57. Accordingly, Louis Vuitton 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 commit identity theft and/or fraud.

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

- First name,
- Last name,
- Gender,
- Country,
- Phone number,
- Email address,
- Postal address,
- Date of birth,
- Purchases,
- Preferences data.

59. This information is highly sensitive and essential to the security of the Plaintiff and Class

members. In particular, the date of birth is a critical data point frequently used in identity verification and, if exposed, significantly increases the risk of identity theft and/or fraud.

60. Furthermore, the purchase history data is financial in nature and may reveal an individual's spending habits and overall financial capacity (especially when dealing with the purchase of ultra luxury items such as those sold by Louis Vuitton). Such financial data gives fraudsters immediate insight into the economic profile and potential value of a target, aside from assisting fraudsters in their social engineering and phishing attempts.

61. Additionally, the term "preferences data" used in the LV Notice is purposely vague and undefined, creating even more uncertainty for Plaintiff and the Class Members. This category may include far more detailed or intrusive information than is immediately apparent, thereby exacerbating concerns regarding the scope of the Louis Vuitton Data Breach. In addition, all additional information or data which has been exfiltrated will assist fraudsters in their social engineering and phishing attempts.

62. That being said, the Louis Vuitton Canada Privacy Policy (available on its Canadian website), a copy of which is communicated herewith as **Exhibit P-15**, confirms that Louis Vuitton indeed collects much more information from its customers, namely:

> "The Personal Information we collect or receive varies depending on how you interact with us.
>
> We collect contact information.
>
> This may include your name, address, telephone number or e-mail address. For example, we might collect this Personal Information if you sign up for an online account or participate in an event. We might also collect contact information if you fill out a customer information card.
>
> We collect account information.
>
> We collect information in order to provide you with an account, including email address and password, in addition to name and contact information.
>
> We collect payment information.
>
> For example, we may collect your credit card number, billing and shipping address when you buy merchandise. We collect Personal Information you submit or post, or when you contact us.
>
> We may collect Personal Information you post in a public space on our Platform, such as when you leave a product review. We may also collect Personal Information when you send us a message through the "Contact" page, use a "wish list," use live chat, utilize the online appointment service, use similar entry points on our Platform, or when you enter a promotion. We may also collect audio recordings, and other information when you contact us.

We collect Personal Information you submit or post, or when you contact us.

We may collect Personal Information you post in a public space on our Platform, such as when you leave a product review. We may also collect Personal Information when you send us a message through the "Contact" page, use a "wish list," use live chat, utilize the online appointment service, use similar entry points on our Platform, or when you enter a promotion. We may also collect audio recordings, and other information when you contact us.

We collect social media information.

We may collect Personal Information you post on our social media pages. We may also collect your social media profile information and information posted on your page.

We collect demographic information.

We may collect your birthdate, age, gender and zip or postal code. We may also collect information that could identify you and relates to your hobbies, interests and shopping behavior.

We collect Personal Information about your purchases.

We may collect Personal Information about the purchases you make online or in stores. This could include the products you purchased and their prices. We also collect information about the services you have purchased.

We collect device information.

For example, we may collect the type of device you use to access our Platform. We may also collect your device identifier, IP address or mobile operating system.

We collect product and Platform usage information.

If you use our connected products (i.e., products that are connected to the internet in order to transmit data or be controlled remotely; such as our Tambour Horizon Connected Watch) ("Connected Products"), we may collect information regarding your use of such products (such as which feature on your product you use the most), as well as geolocation information if necessary to provide you the service you requested.

We also collect information about when and how people visit and interact with our websites, including what pages they accessed, and their interaction with the website features, such as chat and videos. We also receive information to help detect and prevent consumer fraud, including but not limited to browser and keyboard language settings, whether data is automatically filled or manually entered, whether data is manually or copy pasted, and proxy detection. We and/or our partners may use tools described herein to collect some of this information.

We collect location information.

For example, we may collect precise location information from your device. This may include information about your exact location when you use our Platform. We may also collect this Personal

> Information in the background when our mobile applications are not in use. For more information about your options related to the collection of your location information, see the Choices section below.
>
> We collect video surveillance footage in our stores.
>
> We use video surveillance in our stores in order to detect and address security and safety incidents, shoplifting, other potentially illegal activities, and adequate staffing. If you enter our store, your images may be collected for these purposes.
>
> We collect Sensitive Personal Information.
>
> Certain of the Personal Information we collect also falls under the sub-category of "Sensitive Personal Information" as defined by certain laws, such as your unique physical characteristics. We may also collect Sensitive Personal Information for the purpose of managing possible adverse effects caused by our cosmetic products in accordance with our legal obligations as a cosmetics manufacturer and for reasons of substantial public interest. Additionally, in the context of a claim regarding an adverse effect, this Sensitive Personal Information may be processed to manage your claim and to establish, exercise or defend legal claims. If we collect Sensitive Personal Information, then we only collect and use such information as necessary to provide goods and services to you and do not use such information to infer characteristics about you.
>
> We collect other Personal Information.
>
> If you use our website, we may collect information about the browser you're using. We might look at what site you came from, or what site you visit when you leave us. We might look at how often you use the app and where you downloaded it. We might also review information regarding your interactions with our communications, such as email and chat. We may also collect information such as survey responses when you are responding to a survey, or other information that you provide to us."

63. Defendants, who required the personal and financial information of its customers in the context of the marketing and sale of their 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.

64. When a Data Breach affecting many thousand Consumers occurs, Defendants 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.

65. This lawsuit stems from Defendants' multiple and repeated failures to follow these obligations, as detailed above (for a period of over 7 months since at least January 2025).

66. The different parts of the global data breach detailed above were reported by multiple

media outlets, as appears from the various articles reporting the issue, communicated herewith as **Exhibit P-16**, *en liasse*.

67. Notwithstanding the fact that the LVMH group members (including Defendants) were dealing with the Data Breach and notifying affected clients around the world for many months, Defendants only chose to start notifying Canadian Louis Vuitton Class Members such as the Plaintiff only on July 23, 2025, with many Class Members never being notified at all.

68. The July 14, 2025 Securityweek.com article entitled "Louis Vuitton Data Breach Hits Customers in Several countries" (included in P-16), confirms *inter alia* the following:

> Data breach notifications have been published on Louis Vuitton websites or privately sent out for customers in the United Kingdom, South Korea, and Turkey. Other countries may be impacted as well.
>
> ...
>
> The incidents reported in each country appear to be connected, based on the type of information that has been compromised and the date when the breach was detected, June 7.
>
> Press releases issued in Korea and Turkey indicate that the hackers gained initial access nearly one month before the intrusion was detected.
>
> In Turkey, the company reported that the breach impacted nearly 143,000 residents. The same statement reveals that the incident involved a compromised account related to a third-party service provider.

69. The July 18, 2025 bleepingcomputer.com article entitled "Louis Vuitton says regional data breaches tied to same cyberattack" (included in P-16), confirms *inter alia* the following:

> Luxury fashion giant Louis Vuitton confirmed that breaches impacting customers in the UK, South Korea, and Turkey stem from the same security incident, which is believed to be linked to the ShinyHunters extortion group.
>
> Since last week, the retailer has been notifying customers that their info was exposed in a data breach, first in South Korea, then in Turkey, and on Friday in the United Kingdom. After publishing, BleepingComputer learned that notifications also went to customers in Italy and Sweden.
>
> ...

> When BleepingComputer asked if the Louis Vuitton and Dior breaches were part of the same cyberattack, a LVMH spokesperson said there was no additional information they could share at this time.
>
> However, sources have told BleepingComputer that the LVMH breaches are linked to an attack by the ShinyHunters extortion group, which gained access and stole data from a third-party vendor's database.
>
> ...
>
> ShinyHunters is a prolific threat actor tied to numerous data theft campaigns, including those against Salesforce and PowerSchool, as well as the SnowFlake attacks, which impacted Santander, Ticketmaster, AT&T, Advance Auto Parts, Neiman Marcus, and Cylance.

70. The July 24, 2025 the register.com article entitled "Eau no! Dior tells customers their data was swiped in cyber snafu" (included in P-16) indeed confirms that the Dior Data Breach and the Louis Vuitton Data Breach were related and both perpetrated by the same abovementioned ShinyHunters extortion group:

> The attack is believed to be the work of ShinyHunters, a prolific data-slurping crew previously linked to digital burglaries at a range of tech firms and fashion brands. The same group is also suspected in a recent attack on Louis Vuitton, which, like Dior, is part of luxury mega-conglomerate LVMH.

71. The July 21, 2025 independent.co.uk article entitled "Passport details among data leaked in Louis Vuitton cyberattack" (included in P-16), confirms *inter alia* the following:

> Hong Kong's privacy watchdog is investigating a data leak affecting about 419,000 customers at Louis Vuitton.
>
> Leaked information included names, passport details, addresses and email addresses as well as phone numbers, shopping history and product preferences, Hong Kong's Office of the Privacy Commissioner for Personal Data said.
>
> ...
>
> The Hong Kong watchdog said it had also launched an investigation into Louis Vuitton Hong Kong, including whether there had been delays in notifying authorities.
>
> ...
>
> It said the French head office had found suspicious activities on its computer system on June 13, discovered Hong Kong customers were affected on June 7, and then reported the breach to the watchdog on July 17.

> The luxury group reported similar breaches in its operations in South Korea and Britain earlier this month.

72. As reported in the P-16 articles, Louis Vuitton therefore permitted multiple groups to get into the Louis Vuitton systems at the same time, which further evidences the fact that Defendants' information security systems were grossly lacking and wholly inadequate, further demonstrating their faults and negligence.

73. Despite the fact that the Louis Vuitton Data Breach was announced in multiple media outlets, Louis Vuitton never published the information on its Canadian website or social media accounts. This decreased the likelihood that the Class Members would read the July 23, 2025 email and was surely intended to minimize the adverse effects of the Data Breach on Louis Vuitton's sales.

74. The same is true regarding the Dior Data Breach and the Tiffany & Co. Data Breach.

75. As mentioned above, Defendants in general and Louis Vuitton in particular were negligent in choosing to wait excessive amounts of time before actually notifying the affected Customers (Class Members), leaving them at greater risk of fraud and identity theft, although Defendants have and had the proper contact information and financial means in order to quickly reach the Class Members.

76. Moreover, Defendants failed to confirm that they would indemnify and hold the Class Members harmless of any losses or damages suffered as a result of the Data Breach.

77. Defendants 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. In fact, and as appears from the Dior Notice (P-12) sent to affected customers in the USA, Dior offered credit monitoring, fraud resolution services, and identity theft insurance to affected customers, free of charge for a period of 24 months. That being said, and for no apparent or legal reason, Louis Vuitton has offered the Plaintiff and Canadian Class Members absolutely nothing.

78. Defendants including Louis Vuitton have therefore 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.

79. Defendants were negligent and committed faults in this regard since they 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 relevant notice for whatever reason including change of address or bounce-back of emails).

80. By choosing not to automatically activate both credit agencies' credit monitoring services and by not posting the proper fraud alerts for all Class Members, Defendants 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 Defendants including Louis Vuitton are not offering this and has not paid to automatically activate these services.

81. The LV Notice provides a 1-866-VUITTON number to call for information. The agents answering said telephone hotline:

a) are unable to confirm which information was actually stolen regarding the individual Class Members;
b) confirm that Louis Vuitton is not offering any credit monitoring services, insurance or other protections whatsoever to the Class Members;
c) confirm that all Louis Vuitton clients worldwide have been affected and have been apparently addressed the LV Notice.

82. In addition, the 1-866-VUITTON number starts with a French-only automated voice service, without any option to switch to English, increasing the likelihood that English only speaking Class Members will not be able to navigate the automated service and therefore not be able to ask for help or more information.

83. As mentioned above, after becoming aware of the Data Breach, Louis Vuitton waited an excessive number of days before starting to contact some but not all of the Class Members in order to inform them of Data Breach. Dior and Tiffany & Co. were similarly also negligent in the same way.

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

85. Defendants including Louis Vuitton are hereby summoned to confirmed whether they communicated with the unauthorized third parties who perpetuated the Data Breach, to confirm whether they 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.

86. 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.

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

88. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. By letting the excessive amounts of days pass before starting to notify affected Class Members (as detailed above), with many Class Members not even informed yet at all, Defendants failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class Members.

89. Class Members 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;

90. 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.

91. 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 Defendants' loss of the information (as confirmed in the Notice);

d) To inform their financial institutions of the loss of the information by the

Defendants 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.

92. 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. Defendants are solely responsible for these costs or fees paid by the Class Members and for the inconvenience caused to Class Members in this regard.

93. In addition, the Defendants violated the Law but transferring and storing the Class Members personal and financial data and information outside of Canada (and outside of Quebec).

94. 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 Defendants and subsequently lost by Defendants as detailed above constitutes an unlawful violation of the Class Members' fundamental rights, which make Defendants 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, 17, 28, 29, and 93.1 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;

e) Sections 1, 2, 8-12, 16, 17, 40-42, 215-228, 253, 261-272 of the Consumer Protection Act, Chapter P-40.1;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF

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

96. As mentioned above, Plaintiff only received the P-14 LV Notice email on July 23, 2025, informing her for the first time that the Data Breach had occurred and that Louis Vuitton had permitted unauthorized third-party individuals to gain access to her personal information.

97. Plaintiff is very careful and cautious about protecting her personal information, credit file and data.

98. The protection of her personal information, credit file, and data is even more important to Plaintiff since she was already the victim of identity theft approximately ten years ago (she has no knowledge as to who perpetuated the identity theft and related fraud, and the fraudster was never identified. That identity theft and fraud was not related to Defendants).

99. This is why *inter alia* she is filing the present proceedings without divulging her name, in order to further reduce the risks of damages, fraud and identity theft.

100. At the time of receiving the LV Notice, Plaintiff was not subscribed to any credit monitoring services.

101. Very worried about protecting her credit file and assets after learning of the Louis Vuitton Data Breach, and in order to help protect herself from fraud and identity theft (since Louis Vuitton was not offering any protection at all, as mentioned above), Plaintiff subscribed to the Equifax Complete Premier credit monitoring service, offered by Equifax Canada, at a introductory rate of $4.95 (plus taxes) for the first month, followed by $24.95 per month (plus taxes), payable on an automatic recurring basis, which amounts she claims from Defendants solidarily as damages stemming directly from the Louis Vuitton Data Breach and the receipt of the LV Notice, the whole as more fully appears from her Equifax Canada email confirmation, communicated herewith as **Exhibit P-17**.

102. Indeed, and as alleged above, Defendants / Louis Vuitton should have offered such credit

monitoring services to the Plaintiff and the Class Members (for multiple years of coverage) when sending the LV Notice, but they have 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 Defendants.

103. As mentioned above, Dior entities have in fact offered 24 months of free credit monitoring, fraud resolution services and identity theft insurance to US Dior data breach affected customers but not to the Plaintiff and the Canadian Class Members. This represents further intentional faults and omissions committed by Defendnants.

104. This also represents admissions by the Defendants that credit monitoring, fraud resolution services, and identity theft insurance are required under the circumstances of such a data breach. Nonetheless, Defendants refuse to offer this to the Plaintiff and Class Members.

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

106. As a result of learning that her personal information was lost by Defendants, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and fear due to the loss of personal information, and this, aside from unexpected out-of-pocket expenses.

107. In order to save money, Defendants have 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.

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

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

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

111. Indeed, the P-16 news articles confirm further faults committed by Defendants and the other Defendants, namely that they failed to even encrypt the personal information of their clients and that they had failed to identify and remedy (or shut down) the vulnerabilities in their inadequate systems even after being made aware of the Data Breach.

Punitive Damages:

112. 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 Defendants were grossly and/or intentionally negligent and are solidarily liable to pay punitive damages to the Class Members.

113. In fact, without limiting the generality of the forgoing, Defendants were grossly negligent and/or intentionally negligent when they:

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 Defendants 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 (although they were already aware of the Dior Data Breach and yet permitted the Tiffany Data Breach and the Louis Vuitton Data Breach);

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

f. failed to close off and/or remedy the vulnerabilities in their 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. Defendants have repeatedly committed such faults putting their clients' information at great risk and such past faults and conduct further warrant the award of punitive damages.

114. Considering the above and considering the fact that Defendants have violated various laws which have been enacted in order to protect the Class Members' personal and/or financial information, Defendants are solidarily liable to pay at least $1,000 (*à parfaire*) to each Class Member in punitive damages due to the loss of private information itself, aside from any other compensatory and moral damages suffered by the Class Members.

115. Indeed, Plaintiff invokes and relies upon Article 93.1 of the *Act Respecting the Protection of Personal Information in the Private Sector* which provides for the minimum award of punitive damages in this particular situation, which applies herein (in favor of Plaintiff and each Class Member)*:*

> "Where the unlawful infringement of a right conferred by this Act or by articles 35 to 40 of the Civil Code causes an injury and the infringement is intentional or results from a gross fault, the court shall award punitive damages of not less than $1,000."

116. Defendants' 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.

117. Defendants' 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 of at least $1,000 (*à parfaire*) should be awarded to each Class Members.

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

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

119. Class Member had their personal information lost by Defendants as described hereinabove, and/or received a notice from Defendants.

120. 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. Defendants have already admitted and confirmed that the Plaintiff and the Class Members will suffer inconvenience as a result of the Data Breach (as confirmed in said notices).

121. 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.

122. 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.

123. 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.

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

125. 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.

126. Every Class Member can still fall victim to fraud or identity theft, in the future, due to Defendants' negligence in the safekeeping of their personal information and negligence in the way they handled themselves after being made aware of this Data Breach.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

127. 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.

128. 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 LVMH's various brands offered in Canada. Defendants are hereby summoned to confirm the total number of affect Class Members in Canada in general, and in Quebec particularly.

129. Class Members are numerous and are scattered across the entire province and country since Defendants offers its products across the country, including Quebec.

130. 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 Defendants. 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 Defendants' conduct would increase delay and expense to all parties and to the Court system;

131. 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;

132. 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;

133. 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;

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

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

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

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

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

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

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

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

138. 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 Defendants;
>
> **CONDEMN** Defendants solidarily to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendants' loss of Class Members' information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendants solidarily to pay $1,000, *sauf à parfaire*, to each Class Members as 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;

139. Plaintiff suggests that this class action be exercised as a national class action, 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 Defendants in the District of Montreal;

c) Defendants carry on business the same way across Canada, in Quebec (and in the District of Montreal);

d) Defendants who carry on business in Quebec and who have set up a complicated and convoluted global corporate LVMH structure are solidarily liable herein, in regard to the global data breach and the faults committed by Defendants in Quebec, as mentioned above.

e) Certain Defendants are domiciled in the District of Montreal, as mentioned above;

f) Defendants cannot attempt to hide behind their complicated and convoluted corporate structure, as detailed above;

g) Defendants have establishments, principal establishments, elected domiciles and attorneys in the District of Montreal;

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

140. 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 Defendants 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 Defendants' 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;

141. 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:

The LVMH Group: All persons in Canada: (i) whose personal or financial information was held by Defendants (or another member of the LVMH Moët Hennessy Louis Vuitton SE group of companies) and was compromised in the data breach which occurred between on or around January 26, 2025 and on or around June 7, 2025, or (ii) who received an email or letter from Defendants (or another member of the LVMH Moët Hennessy Louis Vuitton SE group of companies), as of May 13, 2025, informing them of such data breach;
The Louis Vuitton Subgroup: All persons in Canada: (i) whose personal or financial information held by Louis Vuitton was compromised in a data breach which occurred on or around June 7, 2025, or (ii) who received an email or letter from Louis Vuitton, dated on or about July 23, 2025, informing them of such data breach;
The Dior Subgroup: All persons in Canada: (i) whose personal or financial information held by Dior was compromised in a data breach which occurred on or around January 26, 2025, or (ii) who received an email or letter from Dior, dated between on or about May 13 and on or about July 18, 2025, informing them of such data breach;
The Tiffany & Co. Subgroup: All persons in Canada:

(i) whose personal or financial information held by Tiffany & Co. was compromised in a data breach which occurred on or around April 8, 2025, or

(ii) who received an email or letter from Tiffany & Co., dated on or about May 26, 2025, 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 Defendants commit faults regarding the storage and the safe-keeping of the personal information of the Class Members?

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

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

(d) Are Defendants solidarily 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 Defendants;

CONDEMN Defendants solidarily to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendants' loss of Class Members' information, and **ORDER** collective recovery of these sums;

CONDEMN Defendants solidarily to pay $1,000, *sauf à parfaire*, to each Class Members as 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 Defendants' various brand and corporate websites, Facebook account(s), Instagram account(s) and X (formerly Twitter) account(s), and **ORDER** Defendants to send the notice by email with proof of receipt and by direct mail to all Class Members;

ORDER Defendants 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, July 25, 2025

(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: LVMH global website's history page (https://www.lvmh.com/en/our-group/history);

Exhibit P-2: Full list of *Maisons* (houses or brands) included in the LVMH group as listed on the https://www.LVMH.com/en/press webpage;

Exhibit P-3: Copy of the *Registre des enterprises du Québec* report concerning LVMH Fragrance Brands Canada Ltd.;

Exhibit P-4: Copy of the *Registre des enterprises du Québec* report concerning LVMH Watch & Jewelry Canada Ltd.;

Exhibit P-5: Copy of the *Registre des enterprises du Québec* report concerning Louis Vuitton Canada, Inc.;

Exhibit P-6: Parfums Christian Dior Canada Inc. Legal terms document on the Canadian website;

Exhibit P-7: Christian Dior Privacy Policy entitled Privacy Statement – Parfums Christian Dior (July 2025);

Exhibit P-8: Christian Dior Privacy Policy entitled Privacy Statement – Christian Dior Couture (July 2025);

Exhibit P-9: Copy of the *Registre des enterprises du Québec* report concerning Parfums Christian Dior Canada Inc.;

Exhibit P-10: Copy of the *Registre des enterprises du Québec* report concerning Christian Dior Couture Canada Inc.;

Exhibit P-11: Copy of the *Registre des enterprises du Québec* report concerning Tiffany & Co. Canada;

Exhibit P-12: The July 18, 2025 Dior Notice to US customers;

Exhibit P-13: The Tiffany & Co. Privacy Policy;

Exhibit P-14: The July 23, 2025 Louis Vuitton Notice email sent to Plaintiff;

Exhibit P-15: The Louis Vuitton Canada Privacy Policy;

Exhibit P-16: Various news articles, *en liasse*;

Exhibit P-17: The Equifax Canada confirmation email to the Plaintiff, dated July 25, 2025.

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, July 25, 2025

(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:

LVMH FRAGRANCE BRANDS CANADA LTD., legal person having its head office at 1002-180 Bloor Street West, Toronto, Province of Ontario, M5S 2V6, and having its elected domicile and *fondé de pouvoir* at 2000-630 boul. René-Lévesque Ouest, in the City and District of Montreal, Province of Quebec, H3B 1S6;

-and-

LVMH WATCH & JEWELRY CANADA LTD., legal person having its head office at 30 East Beaver Creek Road, Suite 212 Richmond Hill, Province of Ontario, L4B 1J2, and having its elected domicile at 26E-1501 avenue McGill College, in the City and District of Montreal, Province of Quebec, H3A 3M8;

-and-

LOUIS VUITTON CANADA, INC., legal person having its head office at 4999-199 ST Bay, Toronto, Province of Ontario, M5L 1A9, and having its *fondé de* pouvoir at 3000-1 Place Ville Marie, in the City and District of Montreal, Province of Quebec, H3B 4N8;

-and-

PARFUMS CHRISTIAN DIOR CANADA INC., legal person domiciled at 2000-630 boul. René-Lévesque Ouest, in the City and District of Montreal, Province of Quebec, H3B 1S6;

-and-

CHRISTIAN DIOR COUTURE CANADA INC., legal person domiciled at 2002-365 ST Bloor East, Toronto, Province of Ontario, M5W 3L4, and having its elected domicile at 2000-630 boul. René-Lévesque Ouest, in the City and District of Montreal, Province of Quebec, H3B 1S6;

-and-

TIFFANY & CO. CANADA, legal person having its head office at M108-150 Bloor Street West, Toronto, Province of Ontario, M5S 2X9, and having its principal establishment located at 1290 rue Sherbrooke Ouest, in the City and District of Montreal, Province of Quebec, H3G 1H5.

Defendants

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, July 25, 2025

(s) *Lex Group Inc.*

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

№.: 500-06-001402-250

(Class Action Division)
SUPERIOR COURT
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

A.

Plaintiff

vs.

LVMH FRAGRANCE BRANDS CANADA LTD.

-and-

LVMH WATCH & JEWELRY CANADA LTD.

-and-

LOUIS VUITTON CANADA, INC.

-and-

PARFUMS CHRISTIAN DIOR CANADA INC.

-and-

CHRISTIAN DIOR COUTURE CANADA INC.

-and-

TIFFANY & CO. CANADA

Defendants

APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION

ORIGINAL

Me David Assor

LEX GROUP
AVOCATS ATTORNEYS
WWW.LEXGROUP.CA

BL 5606

Lex Group Inc.
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7
T: 514.451.5500
F: 514.940.1605
@: davidassor@lexgroup.ca