

July 18, 2025

VIA ONLINE PORTAL

Office of the Washington Attorney General
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504

To Whom It May Concern:

We are writing on behalf of Christian Dior Couture SAS (“Dior”) regarding a cybersecurity incident that has impacted certain personal information of Washington state residents. The information in this cover letter is intended to supplement our response to your Office’s reporting form.

On May 7, 2025, Dior identified a potential cybersecurity incident. Dior promptly conducted an investigation, supported by leading third-party cybersecurity experts. The investigation determined that on January 26, 2025, an unauthorized party was able to gain access to a Dior database that contained information about Dior clients. The information contained in the database varied by individual, but may have included: first and last name, contact information, address, date of birth, passport or government ID number, and Social Security Number. Dior promptly took steps to contain the incident, and it has no evidence of subsequent unauthorized access to Dior systems.

Dior has taken steps designed to enhance 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.

Dior is offering a complimentary 24-month membership of Experian IdentityWorksSM credit monitoring to the 10,878 Washington state residents that are being notified in connection with this incident. This product provides individuals with credit monitoring and fraud resolution services, as well as identity theft insurance. Additionally, Dior will provide the notified individuals with guidance on how to protect against identity theft, including information on placing a fraud alert or credit freeze on their credit files, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and contact information for the Federal Trade Commission and the three major credit bureaus.

In order to communicate promptly about this incident, Dior will be sending a notice to impacted state residents via U.S. First Class Mail. A template is attached as **Exhibit A**.

If you have any questions, I can be reached by email at vmohan@gibsondunn.com or directly by telephone at (650) 849-5345.

Thank you for your attention to this matter.

Sincerely,



Vivek Mohan
GIBSON, DUNN & CRUTCHER LLP

Return Mail Processing
PO Box 999
Suwanee, GA 30024

DIOR

247 1 73548 *****AUTO**ALL FOR AADC 006

SAMPLE A. SAMPLE - L02

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



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 IdentityWorksSM monitoring, please contact **1-833-918-5938**.



ATTACHMENT A
Instructions for Activating 24 Month Three Bureau Credit Monitoring Experian IdentityWorksSM

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent (see contact details in the letter). If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Identity Restoration: Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

Fraud Detection Tools: While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** October 31, 2025 (Your Activation Code below will not work after this date.)
- **Visit** the Experian IdentityWorksSM website to enroll:
<http://www.experianidworks.com/3bcredit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorksSM online, please contact Experian's customer care team at 1-833-918-5938 by October 31, 2025. Be prepared to provide engagement number B147873 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKSSM MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorksSM. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorksSM:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorksSM ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the US Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, please review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax
Equifax Information Services
LLC
P.O. Box 105069
Atlanta, GA 30348-5069
1-888-836-6351
www.equifax.com

Experian
Experian Inc.
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
TransUnion LLC
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com



Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland); or (410) 576-6300
www.marylandattorneygeneral.gov

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free); or 1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/publications/protect-your-identity>

Bureau of Internet and Technology ("BIT")
28 Liberty Street
New York, NY 10005
(212) 416-8433
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:
North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina); or (919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:
Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon); or (503) 378-4400
www.doj.state.or.us

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:
Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202) 727-3400
www.oag.dc.gov



