

Dior begins sending data breach notifications to U.S. customers

By Bill Toulas

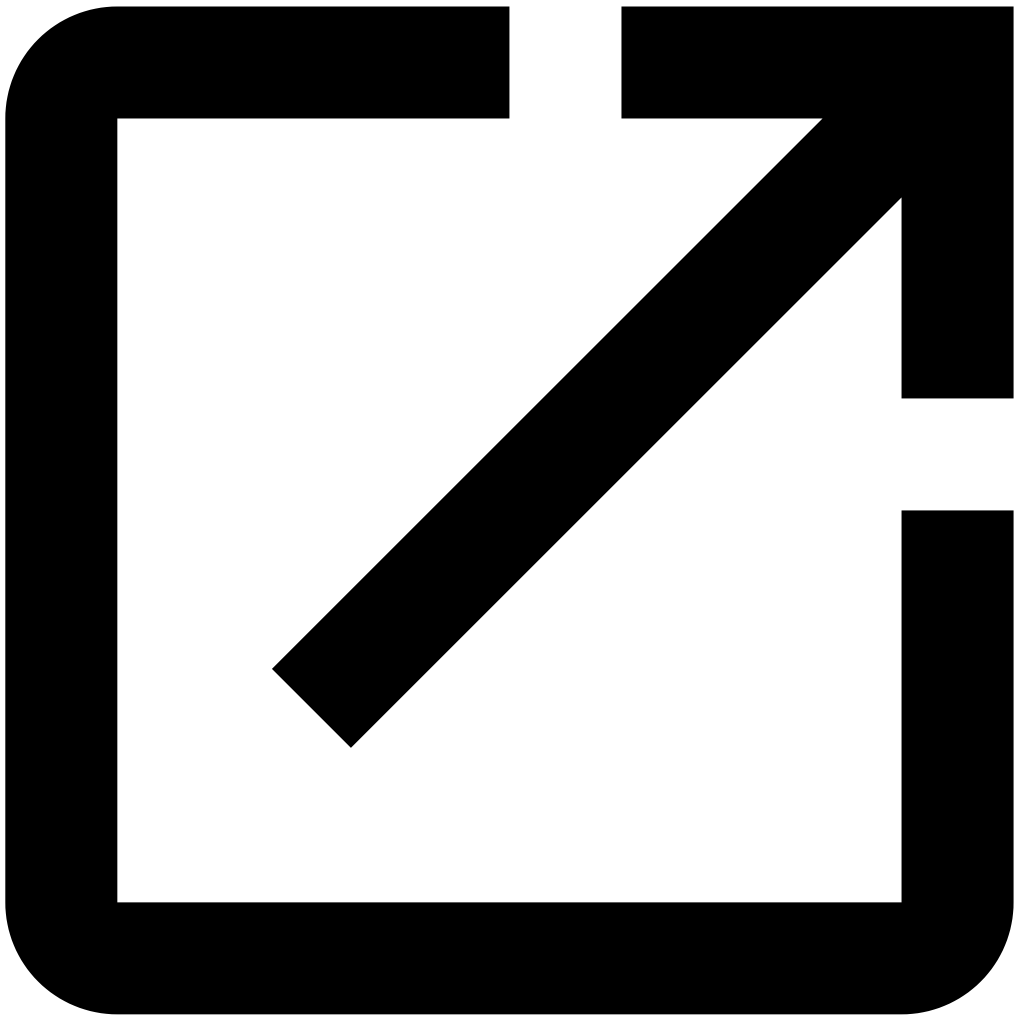
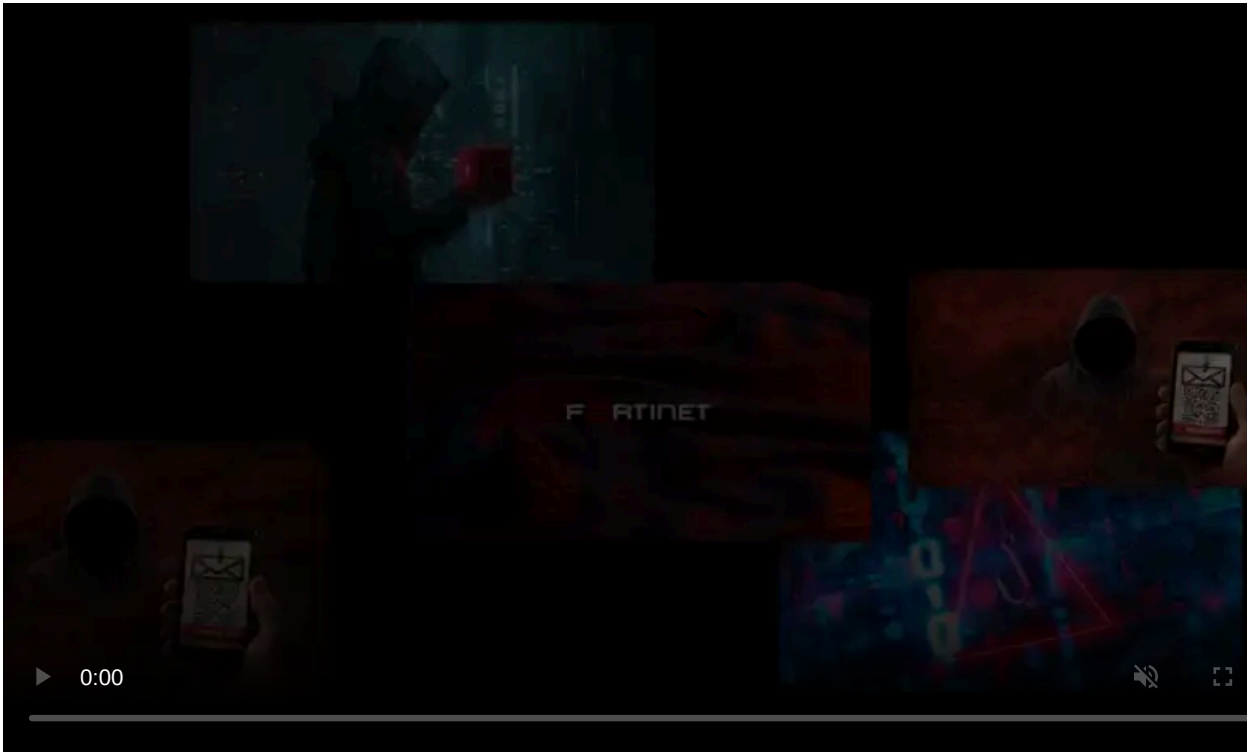
Published: 2025-07-21 · Archived: 2026-04-06 00:26:56 UTC



The House of Dior (Dior) is sending data breach notifications to U.S. customers informing them that a May cybersecurity incident compromised their personal information.

Dior is a French luxury fashion house, part of the LVMH (Moët Hennessy Louis Vuitton) group, which is the world's largest luxury conglomerate.

The Dior brand alone generates an annual revenue of over \$12 billion, operating hundreds of boutiques worldwide.



Visit Advertiser website [GO TO PAGE](#)

The security incident occurred on January 26, 2025, but the company only became aware of it on May 7, 2025, launching internal investigations to determine its scope and impact.

"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," reads the [notice sent to affected individuals](#).

"Dior promptly took steps to contain the incident, and we have no evidence of subsequent unauthorized access to Dior systems."

Based on the findings of the investigation, the following information has been exposed:

- Full names
- Contact details
- Physical address
- Date of birth
- Passport or government ID number (in some cases)
- Social Security Number (in some cases)

The company clarifies that no payment details, such as bank account or payment card information, were contained in the compromised database, so this information remains safe.

Law enforcement was notified accordingly, while third-party cybersecurity experts were engaged to help contain the incident.

Recipients of the data breach notification are advised to remain vigilant for scams and phishing attempts, and to closely monitor the activity in their financial accounts to identify and report any suspicious activity.

Meanwhile, the letter encloses instructions on enrolling in a 24-month credit monitoring and identity theft protection package free of charge, redeemable until October 31, 2025.

The date of the incident matches that of a previous disclosure by Dior, which [confirmed impact in South Korea and China](#).

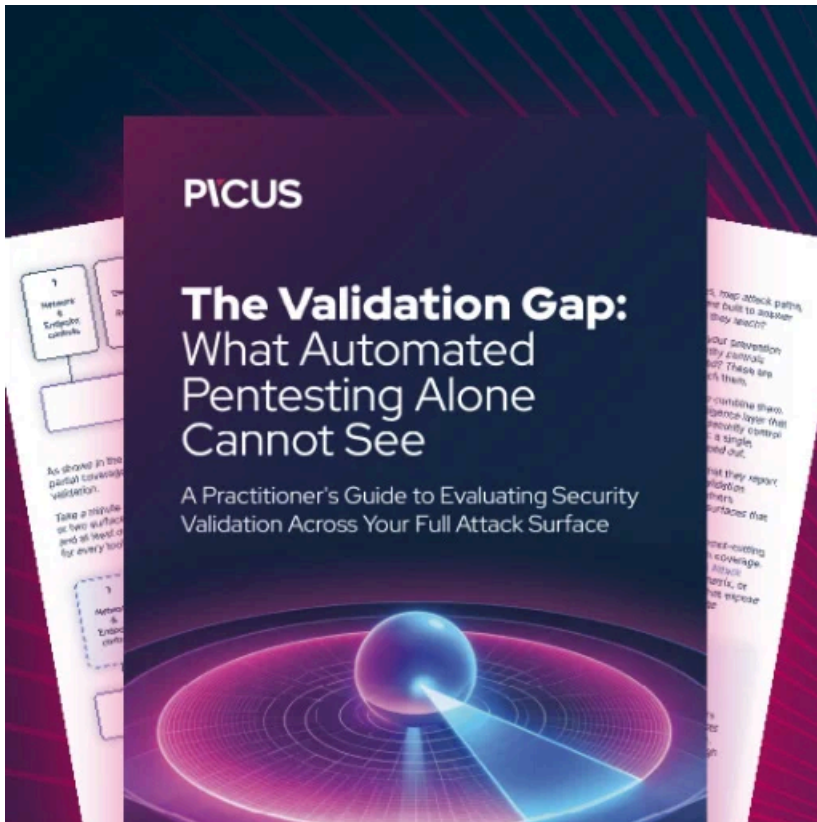
Louis Vuitton, also a brand of the LVMH group, [recently disclosed a data breach](#) that impacted customers in the UK, South Korea, and Turkey.

Although a spokesperson for the firm didn't respond to our requests for clarification, BleepingComputer learned that the incidents at Louis Vuitton and Dior were part of the same cyberattack.

The attack is believed to be linked to the ShinyHunters extortion group, which gained access to LVMH customer information by breaching a third-party vendor's database.

If that is the case, Louis Vuitton is likely to follow with a similar disclosure concerning U.S. customers.

BleepingComputer has contacted Dior to learn how many U.S. customers were impacted, but we have not yet received a response.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/dior-begins-sending-data-breach-notifications-to-us-customers/>