

Allianz Life confirms data breach impacts majority of 1.4 million customers

By Lawrence Abrams

Published: 2025-07-26 · Archived: 2026-04-05 15:03:16 UTC



Insurance company Allianz Life has confirmed that the personal information for the "majority" of its 1.4 million customers was exposed in a data breach that occurred earlier this month.

"On July 16, 2025, a malicious threat actor gained access to a third-party, cloud-based CRM system used by Allianz Life Insurance Company of North America (Allianz Life)," an Allianz Life spokesperson told BleepingComputer.

"The threat actor was able to obtain personally identifiable data related to the majority of Allianz Life's customers, financial professionals, and select Allianz Life employees, using a social engineering technique."



Visit Advertiser website [GO TO PAGE](#)

"We took immediate action to contain and mitigate the issue and notified the FBI. Based on our investigation to-date, there is no evidence the Allianz Life network or other company systems were accessed, including our policy administration system."

"Our investigation is ongoing and we began the process of reaching out to individuals impacted with dedicated resources to assist them. This incident is related only to Allianz Life, which currently has 1.4 million customers."

Allianz Life is a US-based provider of annuities and life insurance for over 1.4 million Americans. The company is owned by Allianz SE, a global financial services group headquartered in Germany, serving more than 128 million customers.

The company first revealed the breach in a mandatory filing with [Maine's Attorney General's Office](#) on Saturday, issuing a placeholder notification alerting of the breach.

"The consumer notice will be provided once Allianz has identified the affected individuals," reads the placeholder notification.

While Allianz Life declined to answer questions about the threat actor and whether they were being extorted, BleepingComputer has learned that the attack is believed to have been conducted by the ShinyHunters extortion group.

ShinyHunters is a group of threat actors who are linked to multiple high-profile data breaches and attacks, including those against [PowerSchool](#) and the [SnowFlake attacks](#), which impacted [Santander](#), [Ticketmaster](#), [AT&T](#), [Advance Auto Parts](#), [Neiman Marcus](#), and [Cylance](#).

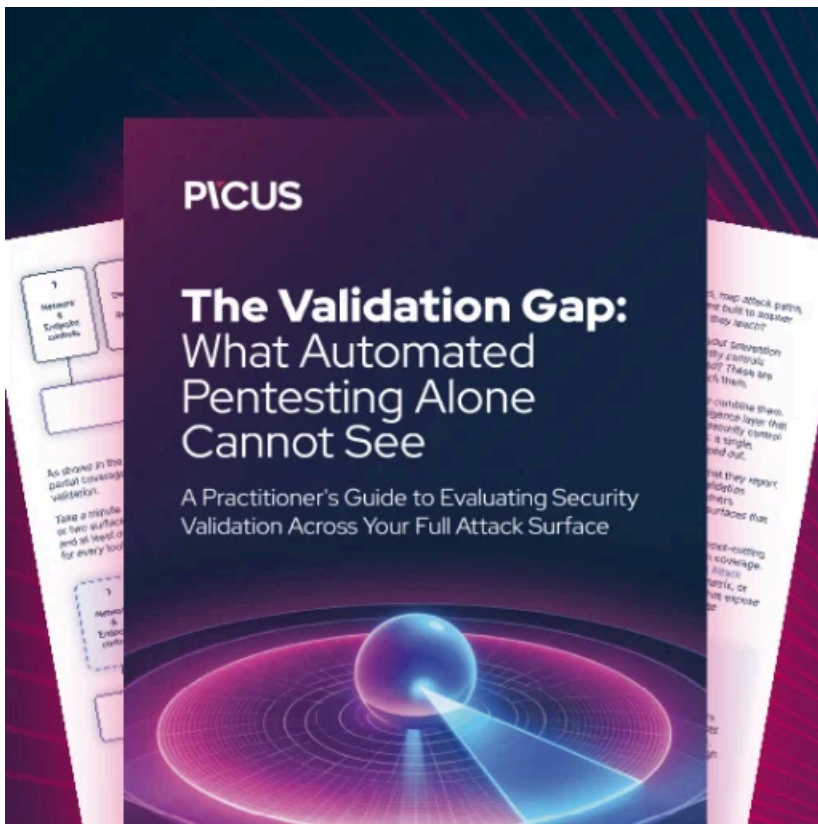
While multiple ShinyHunters members have [been arrested](#) over the [past few years](#), including a [recent arrest in France](#), the hacking group continues to conduct attacks.

Last month, Mandiant warned that ShinyHunters had begun to [target Salesforce CRM customers](#) in social engineering attacks.

During these attacks, the hackers impersonate IT support personnel, requesting the targeted employee accept a connection to Salesforce Data Loader, a client application that allows users to import, export, update, or delete data within Salesforce environments.

Once the connection is accepted, the threat actors use Salesforce Data Loader to exfiltrate data from Salesforce, which is then used to extort the company.

BleepingComputer asked Allianz Life if the CRM is Salesforce, but the spokesperson declined to comment.



[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/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/>