# Allianz Life Insurance Impacted By Third Party Breach





On July 16, 2025, Allianz Life Insurance Company of North America experienced a data breach. According to a filing with the Office of the Maine Attorney General, the incident was described as an “external system breach.”

At this time, there is no further information about the data that may be compromised, or how many individuals may be affected. While the threat actor behind this attack is also unknown, there are some initial similarities to Scattered Spider, a group that has recently changed targets from retail to insurance.

Below, security leaders weigh in on this attack.

## Security Leaders Weigh In

### Boris Cipot, Senior Security Engineer at Black Duck:

This breach highlights that the biggest threats don’t always come from direct attacks, but often a combination of vulnerabilities across the entire supply chain. In this case, the attacker used multiple techniques: social engineering to obtain access rights and a third-party solution as a backdoor into the system.

Organizations must take a holistic view of their security posture. The supply chain is often the weakest link and must not be overlooked. Allianz responded appropriately by

notifying the authorities and the affected customer, and by offering credit and identity monitoring services. However, impacted individuals should remain vigilant. The stolen data could still be used in follow-up social engineering attempts. Be cautious of unsolicited messages, especially those containing links or attachments. Don’t click on links or open files unless you’re absolutely sure they’re legitimate.

## Mr. Piyush Pandey, CEO at Pathlock:

This breach is a stark reminder of how critical it is to have a comprehensive security and governance program around enterprise business applications such as CRM platforms, which store a massive amount of sensitive customer PII.

Specifically, it flags to us that it’s no longer enough for enterprises to rely on basic identity provisioning. Instead, it’s important to embrace real-time access risk analysis that continuously monitors whether corporate accounts have the right level of access based on their current context and behavior, not just their job title or group membership.

Additionally, it highlights the importance of adopting a cross-application governance model that can flag excessive privileges, identify dormant or high-risk accounts, and revoke inappropriate access before it can be exploited – and do so across the entire business application footprint.

And let’s not forget the compliance angle. For insurance companies, breaches of this nature can lead to compliance penalties under the laws like the Gramm-Leach-Bliley Act (GLBA) and other data protection regulations.

## Mr. Agnidipta Sarkar, Chief Evangelist at ColorTokens:

While this does resemble Scattered Spider, it could also be ShinyHunter. Yes, the attack originated through a third-party CRM platform; however, the compromised data included

personally identifiable information (PII) related to the majority of Allianz Life’s 1.4 million customers, financial professionals, and select employees. This poses a lot of questions about how the supply chain security was managed and monitored. The incident also raises questions about regulatory compliance, particularly under laws like the Cybersecurity Information Sharing Act of 2015, set to expire in September 2025, and state-specific data breach notification requirements.

The exposure of PII poses significant risks to affected individuals, including identity theft, financial fraud, and phishing attacks. Victims may face unauthorized access to financial accounts, credit card fraud, or even medical identity theft, given Allianz Life’s role in life insurance and annuities. There were other similar breaches recently at Aflac and Anthem and to some extent, Allianz Life’s offer of 24 months of credit monitoring and identity theft protection through Kroll, could probably help many victims.

https://www.securitymagazine.com/articles/101797-allianz-life-insurance-impacted-by-third-party-breach