July 25, 2025

Office of the Attorney General
Hoover State Office Bldg.
1305 E. Walnut
Des Moines, IA
50319

RE: Data security event

On July 17, 2025, at 12:17 pm CDT, Allianz Life Insurance Company of North America (AZLNA) became aware of suspicious activity within a third-party cloud-based CRM system used by AZLNA. We immediately began an investigation into the suspicious activity and terminated access to accounts associated with the suspicious activity at 2:17 pm CDT on July 17, 2025.

Based on our investigation to date, it appears that on July 16, 2025, a malicious threat actor gained unauthorized access to the CRM system used by AZLNA and two of its US affiliates using a social engineering technique. Based on queries run on the CRM instance during the window of compromise, it appears the threat actor was able to obtain personal information related to the majority of AZLNA's customers, financial professionals, and select AZLNA's employees. The impacted tables within the CRM database may have included information such as names, addresses, dates of birth, and Social Security numbers.

To proactively respond to this incident, in addition to terminating access to the accounts associated with the suspicious activity we also implemented additional safeguards to our business processes and controls, including:

- An immediate temporary shut-down of our secure website for customers and financial professionals for the weekend of July 19 and 20.
- Once the website re-opened, we implemented heightened security monitoring of the secure website.
- We added a high level of scrutiny, including enhanced analysis and authentication, for any transactions or account changes initiated since the incident.
- We implemented additional controls for payments and customer account changes.

While our investigation remains ongoing, there is currently no indication the threat actor was able to gain access to AZLNA's company network or any additional systems outside of the CRM instance. We believe the company's systems, including the CRM instance, have been secured.

In addition to leveraging in-house cybersecurity and forensics resources, we have engaged through counsel a leading cyber forensic consultant to assist in the investigation. We have also been in contact with the FBI regarding this incident. We and our advisors are working rapidly to determine the scope and nature of the incident, ensure our systems are secure, and identify any affected individuals whose personal information may have been subject to unauthorized access. Once identified, we will provide notice and an offer of two years of complimentary identity monitoring services to all affected individuals.

As our investigation continues, we will provide updated information as appropriate and available. In the meantime, please do not hesitate to reach out with any questions: Alexander Sand (alexandersand@eversheds-sutherland.com, 512-721-2721) or Chris Bloomfield (chrisbloomfield@eversheds-sutherland.com, 202-383-0357).