June 23, 2023

Office of the Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines IA 50319

RE: Data Security Event

Wilton Reassurance Company and its affiliates, Wilcac Life Insurance Company, Wilton Reassurance Life Company of New York, and Texas Life Insurance Company (collectively, "Wilton Re") are submitting this notice to provide your office with information regarding a cybersecurity event that may have resulted in unauthorized access to consumer personal information ("PI"). Wilton Re is based in Norwalk, Connecticut and provides life, accident, and health insurance.

On June 7, Wilton Re was informed by its vendor, PBI Research Services ("PBI"), that Wilton Re records maintained by PBI were subject to unauthorized access related to the MOVEit vulnerability (CVE-2023-34362). This vulnerability existed in a file transfer service offered by Progress Software, which PBI uses to transfer certain data related to Wilton Re's insurance customers. The attack has been attributed to the "CL0P" group. According to PBI's forensic investigation, as well as public and government sources, the vulnerability allowed unauthorized actors to gain access to information within the MOVEit file transfer portal and exfiltrate that data. On June 7, PBI informed Wilton Re that the nature of the vulnerability allowed the attackers to bypass the encryption in place on the MOVEit portal and obtain the data in plaintext.

On June 12, based on its own internal investigation Wilton Re determined that some consumer personal information was likely affected. PBI is also actively investigating the incident to determine precisely which individuals have been affected. PBI most recently updated us on June 21; based on the information we have to date, we believe that the name, date of birth, Social Security Number, and policy number of 8,858 Iowa residents may have been impacted. Wilton Re continues to work closely with PBI to identify affected individuals. Wilton Re will ensure that any impacted individuals are notified and offered free credit monitoring and identity theft protection.

Wilton Re ceased sending any data to PBI while the issue is being resolved. PBI reports that it has applied all patches and has taken additional measures to protect its systems and consumer data.

Prior to signing the contract with PBI, dated May 3, 2019, Wilton Re pressed PBI on its cybersecurity program and determined that PBI's cybersecurity program sufficiently addressed the terms required by Wilton Re's Third Party Contracting Policy. As part of that policy, Wilton Re required PBI to warrant the following related to its cybersecurity controls:

1. That it maintains privacy and security controls designed to protect the security of the services and the data maintained therein;
2. It will complete an annual SOC 2, Type II audit and monthly network vulnerability scan and provide copies of the results and audits to clients upon request;
3. It will maintain a business continuity plan;
4. It will encrypt production data maintained to provide its services both in transit and at rest;
5. It will maintain production data in the United States;
6. Prompt notification of a security event;

7. Purge all “bulk data” within 90 days; and
8. Restrict access to use of data to certain individuals.

A third-party SOC 2 Type 2 audit also determined that PBI’s controls “were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met.”

We notified our primary insurance regulators beginning June 8, and continue to notify and update other regulators. While we have not notified law enforcement of this incident, we understand PBI and other entities have notified them. We will update your office as to any material developments.

Should you have any questions please do not hesitate to contact our outside counsel: Michael Bahar (MichaelBahar@eversheds-sutherland.com or +1.202.383.0882) or Alexander Sand (AlexanderSand@eversheds-sutherland.com or +1.512.721.2721).