Information on Third-Party Vendor Security Incident

Brighthouse Financial was recently informed that certain customer data was compromised due to a security incident at a third-party vendor, PBI Research Services (PBI). Brighthouse Financial and many other insurance carriers use PBI to meet certain regulatory obligations by providing death matching services. The security incident was caused by a vulnerability involving the MOVEit file transfer system, which impacted numerous organizations and governmental agencies around the world. PBI has provided assurances that their instance of the MOVEit vulnerability has been remediated.

As of now, Brighthouse Financial believes that substantially all of the compromised data relates to policies in two Brighthouse Life Insurance Company (BLIC) legacy blocks of business: a block of corporate-owned life insurance; and a block of long-term care insurance.

This incident did not impact any Brighthouse Financial information systems. Brighthouse Financial takes our customers' data privacy seriously. Immediately upon learning of these data incidents, Brighthouse Financial began working with relevant third parties to identify and notify individuals who may have been impacted. The notification process is ongoing and impacted individuals will be offered free credit monitoring services.

While we continue to investigate the impact of this incident, we do not believe that it will have a material adverse effect on our business, operations, or financial results.

Frequently Asked Questions

Who may have been impacted?

The security incident did not impact any Brighthouse Financial information systems.

As of now, Brighthouse Financial believes that substantially all of the compromised data is specific to two Brighthouse Life Insurance Company (BLIC) legacy blocks of business: a block of corporate-owned Life Insurance; and a block of long-term care insurance.

What personal information may have been compromised?

At this stage of the investigation, Brighthouse Financial believes the compromised data elements may include first name, last name, Social Security number, date of birth, gender, state, zip code, and policy number. The notification process is ongoing and impacted individuals will be offered free credit monitoring services.

How will I know if my data was accessed in connection with this incident?

Immediately upon learning of this incident, Brighthouse Financial began working with relevant third parties to identify and notify individuals who may have been impacted. The notification process is ongoing and impacted individuals will be offered free credit monitoring services.

Was Brighthouse Financial the only company impacted by this security incident?

No. Brighthouse Financial is one of numerous organizations and governmental agencies around the world impacted by the MOVEit security incident.

How do I know that my data is secure with Brighthouse Financial?

Brighthouse Financial is committed to protecting the security, confidentiality, and integrity of the personal information shared with us. We continuously monitor and evaluate the evolving cybersecurity risk landscape and remain vigilant in taking proactive measures to address emerging threats. In addition to adhering to the privacy rights afforded to consumers by various federal and state laws, our cybersecurity and data privacy programs and related policies establish a robust operational framework and standards for the collection, storage, and management of personal data across our company—applicable to all employees and third-party vendors.

Who should I contact if I am concerned about my data?

If you have any questions about this situation, please call the Brighthouse Financial Privacy Team hotline (844-474-8372, option 2), which is available Monday through Friday between 8:00 a.m. and 4:00 p.m. (ET).