Sentinel Security Life Insurance Company
Notice of Data Event

Sentinel Security Life Insurance Company and its current and former affiliates (collectively "the Companies") are providing notice of a cyber incident that may impact the privacy of certain present or former policyholders or certificate holders of Sentinel Security Life Insurance Company, beneficiaries under policies issued by Sentinel Security Life Insurance Company, or other persons, including persons who may have done business with or interacted with the Companies. The Companies are also providing written notice by mail to other individuals whose information may be impacted by the incident for whom the Companies have a mailing address, including, but not limited to, present and former policyholders of the Companies.

While the Companies are unaware of any actual or attempted misuse of information in relation to this incident, the Companies are providing details about the incident, their response, and resources available to help protect individuals' information against identity theft and fraud, should they determine it is appropriate to do so.

What Happened? On April 15, 2025, the Companies discovered suspicious network activity. In response, the Companies immediately took steps to secure their environment and launched an investigation to determine the nature and scope of the incident. The investigation determined that an unauthorized actor accessed certain Companies' computer systems between April 7, 2025, and April 15, 2025, and potentially accessed and/or acquired certain files stored on those systems. The Companies quickly began a thorough review of the relevant files to identify individuals with personal information that was potentially impacted. On or about December 17, 2025, the Companies completed their review and determined that sensitive information was included in the affected files.

What Information Was Involved? The information contained within the relevant files varies by individual and may include name, Social Security number, individual taxpayer identification number, financial account information, date of birth, medical, or health insurance information. While the Companies are providing notice of this incident via U.S. mail to individuals whose mailing address information is available and current, they are also providing notice of this incident via this posting to notify individuals for whom the Company may not have a valid mailing address. The Companies are not aware of any actual or attempted misuse of anyone's information in connection with this incident.

What We Are Doing. The Companies take this incident and the security of information within their care very seriously. Upon being alerted to suspicious activity through their existing security procedures, the Companies initiated incident response procedures, isolated relevant systems, and began an investigation to identify potentially affected individuals. As part of their ongoing commitment to the privacy of personal information in their care, the Companies are reviewing their policies, procedures, and processes related to the storage of, and access to, personal information to reduce the likelihood of a similar future incident.

As an added precaution, the Companies also secured the services of IDX to provide credit monitoring and identity restoration services for one year at no cost to affected individuals. If you

did not receive written notice of this incident but believe you may be affected, please contact their dedicated assistance line, which can be reached at (844) 419-5502, Monday through Friday from between 9:00am to 9:00pm, Eastern time, excluding U.S. holidays.

What You Can Do. The Companies encourage individuals to remain vigilant against incidents of identity theft and fraud and to review their accounts for any suspicious activity related to the use of their information, including with respect to financial or other accounts in their name. Individuals can find more information about obtaining a free copy of their credit report, protecting against potential identity theft and fraud, and other resources available to them in the below *Steps You Can Take to Help Protect Personal Information*.

For More Information. If you have further questions or concerns, please call (844) 419-5502, Monday through Friday from between 9:00am to 9:00pm, Eastern time, excluding U.S. holidays. You may also write to the Companies at P.O. Box 25837, Salt Lake City, Utah 84125.

Steps You Can Take To Help Protect Personal Information

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If an individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert that lasts seven years. Should they wish to place a fraud alert, they may contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in an individual's name without their consent. However, individuals should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a credit freeze on their credit report. To request a security freeze, individuals will need to provide the following information:

1. full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. date of birth;
4. addresses for the prior two to five years;
5. proof of current address, such as a current utility bill or telephone bill;

6. a legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should individuals wish to place a fraud alert or credit freeze, they may contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and their state Attorney General. This notice has not been delayed by law enforcement.