EXHIBIT 1

We represent Sentinel Security Life Insurance Company and Atlantic Coast Life Insurance Company and their current and former affiliates (collectively "the Companies") with offices located at P.O. Box 25837, Salt Lake City, Utah 84125, and are writing to notify your office of an incident that may affect the security of certain personal information relating to twenty-four (24) Maine residents. By providing this notice, the Companies do not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

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 computer systems of the Companies 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 information related to certain individuals was included in the affected files. As part of the review, the Companies took steps to validate the data and confirm necessary address information to prepare for notification. Although the Companies have no evidence to indicate that any information was misused in connection with this incident, the Companies are providing notice of this incident out of an abundance of caution.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, treatment information, and health insurance policy number.

Notice to Maine Residents

On December 30, 2025, the Companies provided written notice of this incident to twenty-four (24) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. On December 30, 2025, the Companies also posted notification of this incident in a conspicuous location on their websites and sent notification to major media outlets in Maine. A copy of the website posting is attached here as ***Exhibit B***. A copy of the press release issued to major media outlets is attached here as ***Exhibit C***.

Other Steps Taken and To Be Taken

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. The Companies are also working to implement additional safeguards and training to their employees. The Companies are providing access to credit monitoring and identity

restoration services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Further, the Companies notified federal law enforcement regarding the incident.

Additionally, the Companies providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to relevant institutions. The Companies are providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

The Companies are providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: March 30, 2026
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

December 30, 2025

NOTICE OF <<Variable Text 1: SECURITY INCIDENT/DATA BREACH>>

Dear <<First Name>> <<Last Name>>:

Sentinel Security Life Insurance Company and Atlantic Coast Life Insurance Company and their current and former affiliates (collectively "the Companies") write to inform you of an incident that may affect the privacy of some of your information. This notice provides you with additional information about the incident, the Companies' response, and steps you can take to further protect your information against identity theft and fraud, should you 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 computer systems of the Companies 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 December 17, 2025, the Companies completed their review and determined that information related to you was included in the affected files.

What Information Was Involved? The review determined that your name and the following elements were present in the relevant files: <<Variable Text: Data Elements>>. Please note that the Companies are not aware of any information being subject to actual or attempted misuse as a result of this incident, and the Companies are notifying you out of an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of personal information are among the Companies' highest priorities, and the Companies follow strict security measures to protect information in their care. Upon being alerted to suspicious activity through existing security procedures, the Companies promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of the Companies' systems, reviewing the contents of relevant data for sensitive information, and notifying potentially impacted individuals. As part of the Companies' 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. The Companies notified federal law enforcement regarding this incident and are also notifying applicable regulatory authorities, as necessary.

As an added precaution, the Companies would like to offer you <<twelve (12)/twenty-four (24)>> months of complimentary access to credit monitoring and identity restoration services through IDX. If you wish to receive these services, you should follow the enrollment instructions below as the Companies are unable to activate these services on your behalf.

What You Can Do. The Companies encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for any suspicious activity and to detect errors. Instances of suspicious activity can be reported to the appropriate bank, credit union, credit card company, health insurance company, or other relevant institution. You can find more information about obtaining a free copy of your credit report, protecting against potential identity theft and fraud, and other resources available to you in the enclosed *Steps You Can Take to Help Protect Personal Information*. You may also enroll in the complimentary monitoring services available to you; detailed instructions for enrolling in these services are enclosed.

For More Information. The Companies understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call 1-844-419-5502, between the hours of 9 a.m. and 9 p.m. Eastern Time, Monday through Friday. You may also write to the Companies at P.O. Box 25837, Salt Lake City, Utah 84125.

Sincerely,

Sentinel Security Life Insurance Company and Atlantic Coast Life Insurance Company

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is March 30, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-844-419-5502 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

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. Consumers may also directly 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers 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, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, 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 consumers wish to place a credit freeze or fraud alert, please 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, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers 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, consumers 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 the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://oag.maryland.gov.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 44 Rhode Island residents that may be impacted by this event.

EXHIBIT B

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; http://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.

EXHIBIT C

Sentinel Security Life Insurance Company and Atlantic Coast Life Insurance Company Provide Notice of Data Security Event

Salt Lake City, Utah, December 30, 2025 – Today, Sentinel Security Life Insurance Company and Atlantic Coast Life Insurance Company and their current and former affiliates (collectively "the Companies") issued notice of a data security event that potentially affected information related to certain individuals.

On April 15, 2025, the Companies discovered suspicious network activity and immediately took steps to secure their environment and launched an investigation into the nature and scope of the activity. The investigation determined that an unauthorized actor accessed certain systems of the Companies 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 information related to certain individuals was included in the affected files. 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 information, 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 media release and a posting on their websites to notify present or former policyholders or certificate holders of the Companies, beneficiaries under policies issued by the Companies, or other persons, including persons who may have done business with or interacted with the Companies. The Companies are not aware of any actual or attempted misuse of anyone's information in connection with this incident.

Individuals seeking additional information regarding this incident may call a toll-free assistance line the Companies established at (844) 419-5502.

Individuals can also find information on how they can help protect their personal information, along with additional resources on the Companies' websites at https://www.sslco.com/ or https://www.aclico.com/. As a precautionary measure, the Companies encourage potentially affected individuals to remain vigilant against incidents of identity theft or fraud by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should be promptly reported to the appropriate bank, credit card company, health insurance company, or other relevant institution.

The Companies take this incident and the security of the information in their care very seriously. 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.

###