First Security Benefit Life Insurance
and Annuity Company of New York

Administration Office:
PO Box 750497
Topeka, KS 66675-0497

November 21, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Report of Security Breach Pursuant to NH Rev. Stat. Ann. 349-C:20

To Whom it May Concern:

I am writing to supplement a notice provided to your office by First Security Benefit Life Insurance Company of New York ("FSBL" or the "Company") on July 27, 2023, which is attached for your reference.

Clear Spring Life and Annuity Company ("CSLAC") notified FSBL late in the day on November 20, 2023, that three additional New Hampshire residents, who are current or former FSBL consumers ("Impacted Individuals"), were impacted by a ransomware incident. The Impacted Individuals will be notified by Clear Spring Life and Annuity Company ("CSLAC") on November 21, 2023, bringing the total number of Impacted Individuals who reside in New Hampshire and have been notified regarding this incident to four.

CSLAC has advised that the notice will be substantially in the form attached to this letter.

Please contact the undersigned at . should you need further information or have any additional questions.

Sincerely,

Paige Blevins-Jones
Assistant Counsel

Attachments

First Security Benefit Life Insurance
and Annuity Company of New York

Administration Office:
PO Box 750497
Topeka, KS 66675-0497

July 27, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Report of Security Breach Pursuant to NH Rev. Stat. Ann. 359-C:19 et. seq.

To Whom it May Concern:

On July 13, 2023, Clear Spring Life and Annuity Company ("CSLAC") notified First Security Benefit Life Insurance and Annuity Company of New York (the "Company") of a ransomware incident that may have affected personal information belonging to one or more of the Company's current or former contract holders, and their beneficiaries, annuitants, and payees (the "Impacted Individuals"). CSLAC is retrocessionaire to certain of the Company's liabilities under an Indemnity Retrocession Agreement between the Company and CSLAC (formerly Guggenheim Life and Annuity Company), pursuant to which it administers the contracts at issue. CSLAC's July 13 notice included the following information:

> On February 9, 2023, CSLAC was alerted to the existence of sophisticated ransomware on its information technology infrastructure. CSLAC immediately took steps to isolate and secure its systems and investigate the incident. CSLAC retained a leading third-party forensics firm to conduct a thorough investigation, secure its systems, remediate any risks, and methodically bring its systems back online once such systems were validated as clean.
>
> Together with its forensics experts, CSLAC scanned its systems for, and remediated, any identified indicators of compromise and rebuilt systems prior to bringing them back online. In addition, CSLAC has deployed additional advanced endpoint detection and monitoring tools on the newly restored systems for an added layer of security and visibility across its network.
>
> Through its investigation, CSLAC determined that the malicious actor accessed and acquired certain files from its systems. The process of locating personal information in the acquired files, matching that information to individuals, and in some cases obtaining addresses, was complex. The ransomware incident involved approximately 4,393 Impacted Individuals in total, including three Impacted Individuals who resides in New Hampshire, and the files potentially accessed by the attacker contained personal information including

CSLAC also alerted the Federal Bureau of Investigation and provided complete information regarding identified indicators of compromise. CSLAC did not pay a ransom.

CSLAC has advised that it will be reporting the ransomware incident to your office separately with respect to any CSLAC consumers who were potentially impacted.

The Company is continuing to investigate this matter and will supplement this incident report if developments warrant any change to the information provided herein.

The Company is not aware, and CSLAC has advised that it is not aware, of any fraudulent or malicious use of personal information of the affected New Hampshire residents at this time. CSLAC is sending the attached notice, on the Company's behalf, via first class mail to the affected New Hampshire residents on July 28, 2023, and CSLAC has arranged to make credit monitoring and identity protection services by IDX available to the individual at no cost for two (2) years. This includes access to assist the individual with credit restoration, a $1,000,000 insurance reimbursement policy, and credit monitoring services as described in the attached form of notice.

By providing this notice, the Company does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Please feel free to contact me at if you need additional information or if I can answer any questions.

Sincerely,

Paige Blevins
Assistant Counsel

Encl.

Clear Spring
Life and Annuity Company
P.O. Box 989728
West Sacramento, CA 95798-9728

<<Estate of>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

November 21, 2023

Notice of Data Breach

Dear <<Estate of>> <<First Name>> <<Last Name>>,

We are writing to inform you of an incident that may have affected your personal information and are providing you with information on additional steps you can consider taking to protect your personal information.

You are receiving this notice because you are, or previously were, associated with an annuity contract or life insurance policy issued or assumed by First Security Benefit Life Insurance and Annuity Company of New York, which is administered by our company, Clear Spring Life and Annuity Company (formerly Guggenheim Life and Annuity Company).

What Happened

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of Investigation.

As part of our investigation, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems. We have been analyzing the impacted files to understand what personal information may be at risk. The process of locating personal information in the acquired files and matching that information to individuals was complex and took many months to complete. While we were able to utilize software and other automation tools to complete parts of the data analysis and provide notices to certain affected individuals in July, other parts of the analysis required further research and manual review of large data files which took several more months to complete. We are now in the process of notifying additional individuals whose personal information we believe to have been included in the acquired files, including you.

What Information Was Involved

The type of personal information at risk differs from individual to individual but may have included the following information relating to you:

What We Are Doing

Together with our forensics experts, our team scanned our systems for, and remediated, any identified indicators of compromise. Out of an abundance of caution, we have deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network. We

will also continue to make infrastructure enhancements to strengthen and harden the security posture of our network and systems in the days, months, and years ahead.

In addition, we are offering you identity theft protection services through IDX, the data breach and recovery services expert. The IDX identity protection package includes: Experian, Equifax, and TransUnion credit monitoring, CyberScan™ dark web monitoring, identity theft insurance (for up to $1,000,000 with no deductible), and fully managed identity restoration services. In some states, these services are required by law. We are offering these services to all affected individuals free of charge for , regardless of their state of residence.

What You Can Do

We encourage you to enroll and contact IDX with any questions. To enroll in the free identity protection services, please scan the QR code on the first page, or call (888) 331-6462 or go to https://app.idx.us/account-creation/protect and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is

Once you enroll in these identity protection services, IDX will help you resolve issues if you determine your identity is compromised. To receive the credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. If you do not have a credit file or are under the age of 18, you will not be able to register for the credit monitoring services, but you will receive CyberScan™ dark web monitoring, identity theft insurance, and the fully managed identity restoration services from IDX.

Although we have not identified any suspicious activity pertaining to your associated annuity contract or life insurance policy and have not received any reports of misuse of your information, it is always a good practice to be vigilant and closely review and monitor your financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.

IDX representatives have been fully informed regarding the incident and are ready to answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed "Additional Steps You Can Take" document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (888) 331-6462 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Robert Stanton
Chief Operating Officer, Clear Spring Life and Annuity Company

(Enclosure)

IDX
The Privacy Platform

Additional Steps You Can Take

1. Website and Enrollment. Scan the QR code or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your unique Enrollment Code provided at the top of the letter.

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 (888) 331-6462 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. It is always advisable to remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, IDX will assign you an ID Care Specialist who will work on your behalf.

You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General of your state.

5. Place Fraud Alerts with any of the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying

need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The **Federal Trade Commission** also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street,

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting and Identity Security Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting and Identity Security Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting and Identity Security Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting and Identity Security Act. You can review your rights pursuant to the Fair Credit Reporting and Identity Security 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 (toll free within North Carolina) or 601-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were 0 Rhode Island residents impacted by the incident. Under Rhode Island law, you have the right to obtain any police report filed in regard to the incident.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.