IceMiller

One American Square | Suite 2900 | Indianapolis, IN 46282-0200

Chicago Columbus DuPage County, Ill.
Indianapolis New York Philadelphia Washington, D.C.

January 29, 2024

SID BOSE
DIRECT NUMBER: 312-236-2243
SID.BOSE@icemiller.com

CONFIDENTIAL

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

Office of the Iowa Attorney General
Consumer Protection Division
Attn: Security Breach Notification
1305 E. Walnut St.
Des Moines, Iowa 50319

Re: Written Notification of a Security Breach

To Whom It May Concern:

On behalf of my clients, Bankers Life and Casualty Company ("Bankers Life"), I am hereby submitting a written notification of a security breach, in compliance with Iowa Code Chapter 715C.

On November 29, 2023, Bankers Life became aware that a sophisticated threat actor, believed to be "Scattered Spider," targeted the Verizon cellular account belonging to a company senior officer. The threat actor conducted a highly coordinated, and complex "SIM swapping" attack, which the threat actor was able to do because Verizon, without proper authorization or appropriate verification from the senior officer, allowed the senior officer's phone number to be swapped (or 'ported over') to what we believe was the threat actor's phone.

This enabled the threat actor to overcome multi-factor authentication protections, along with other security measures employed by Bankers Life to prevent cyber criminals from accessing its data. It appears that the threat actor was able to bypass the multi-factor authentication and other common security controls, because of the "SIM swapping." The threat actor was then able to gain access to certain company data, which included certain personal information of residents, including, name, social security number, date of birth, and policy number(s).

When Bankers Life first became aware of the incident, it immediately took steps to contain any unauthorized access and launched a full investigation. Bankers Life also promptly notified law enforcement, and began working with the Federal Bureau of Investigation, and the Offices of the United States Attorneys. The Federal Bureau of Investigation and the Offices of the United States Attorneys also have reason to believe that the threat actor is indeed "Scattered Spider."

Bankers Life promptly disabled the senior officer's corporate access, reset passwords for personnel, and blocked the threat actor's potential access. Bankers Life also scanned its

environment, and implemented additional security measures designed to prevent the reoccurrence of this type of an event. In addition, Bankers Life hired an external forensics investigator to conduct an investigation and took steps to further restrict and monitor access to our systems, and to enhance security procedures.

On January 16, 2024, Bankers Life discovered which potential individuals may be impacted by this event. At this time, Bankers Life has no evidence to suggest that any other company systems, accounts or personnel were impacted. The attack was not the result of a vulnerability in Bankers Life's systems, products, or services. To date, there is no evidence that the threat actor had any access to Bankers Life's customer environments. Furthermore, through its investigation, Bankers Life believes that the threat actor's intention was to target the company itself rather than the personal information of the individuals. Accordingly, Bankers Life has no evidence at this time that any individual was actually targeted or that individuals are at any risk of fraud or identity theft.

Nonetheless, out of an abundance of caution, we are notifying **1,192** Iowa residents. A copy of the notices that will be sent to the affected Iowa residents on or around January 26, 2024, is attached herewith. Credit monitoring and identity theft protection services will be offered to the affected Iowa residents for a period of twelve (12) months.

If you require further information about this matter, please contact me by telephone at (317) 236-2243 or via email at Sid.Bose@icemiller.com.

Sincerely,

ICE MILLER, LLP

Sid Bose

Attachment: Exhibit A Individual Notification Letter (Adult)
Exhibit B Individual Notification Letter (Minor)

EXHIBIT A
Template Notification (Adult)

BANKERS LIFE®

Return Mail to IDX:
PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/bankerslife

January 26, 2024

<<Variable Data 4>>

Dear <<First Name>> <<Last Name>>,

At Bankers Life[1] we take our customers' privacy seriously. For this reason, we are writing to let you know about an event that may affect the privacy of some of your personal information. Although we have no reason to believe that you are at any risk of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened

On November 29, 2023, we discovered that a sophisticated threat actor targeted the cellular account belonging to a company senior officer. The threat actor conducted a highly coordinated, and complex "SIM swapping" attack, which the threat actor was able to do because a retailer for one of the top nationwide wireless carriers, without proper authorization or appropriate verification from the senior officer, allowed the senior officer's phone number to be swapped to what we believe was the threat actor's phone.

At Bankers Life, we employ a variety of security measures to prevent cyber criminals from accessing our data and data entrusted to us. Based on our investigation and response to this event, however, it appears the threat actor was able to bypass the multi-factor authentication and other common security controls the company had in place that were designed to protect the company's data. Because of the "SIM swapping," the threat actor was then able to gain access to certain company data.

When we first discovered the incident, we promptly notified law enforcement, and began working with the Federal Bureau of Investigation, the Offices of the United States Attorneys, and a full investigation is underway.

We have no evidence to suggest that any other company systems, accounts or personnel were impacted.

<<Variable Data 5>>

[1] Bankers Life is the marketing brand of Bankers Life and Casualty Company, Medicare Supplement insurance policies issued by Colonial Penn Life Insurance Company and Washington National Insurance Company, and select policies sold in New York by Bankers Conseco Life Insurance Company, a New York licensed insurance company.

What Information Was Involved

We believe that the threat actor's intention was to target the company itself. We have no reason to believe that your personal information was targeted by the threat actor. Nonetheless, we are providing you with this notice out of an abundance of caution because we believe the threat actor targeted Bankers Life, which included some of your personal information.

The personal information may have included your name, social security number, date of birth, and policy number(s) <<Variable Data 6>>.

What We Are Doing

When we first learned of this activity, we began an investigation and immediately took steps to contain any unauthorized access. We promptly disabled the senior officer's corporate access, reset passwords for personnel, and blocked the threat actor's potential access. We also scanned our environment, and implemented additional security measures designed to prevent the reoccurrence of this type of an event. In addition, we engaged federal law enforcement and hired an external forensics investigator to conduct an investigation and took steps to further restrict and monitor access to our systems and to enhance security procedures. We have also enhanced our policyholder safeguards to provide added protection to your personal information.

While we have no reason to believe your personal information was targeted or used, we would like to help protect your information from any potential unauthorized use. To that end, we are offering identity theft protection services through IDX, a leading provider of identity protection services. IDX services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

IDX experts are available Monday through Friday from 6 am - 6 pm Pacific Time. **Please note the deadline to enroll is April 28, 2024**. The enclosed Reference Guide includes additional information on steps you can take to monitor and protect your personal information.

We encourage you to remain vigilant in monitoring your account statements and insurance transactions for incidents of fraud and identity theft, and to promptly report such incidents. We encourage you to routinely review bills, notices, statements, and explanation of benefits that you receive from financial institutions, hospitals, doctors and health insurance companies.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps 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) 256-2082 or go to https://response.idx.us/bankerslife for any additional questions you may have.

Sincerely,

Bankers Life

Enclosure

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/bankerslife and follow the instructions for enrollment using your 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) 256-2082 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. We recommend that you 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 them 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 our 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, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that 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.

5. Place Fraud Alerts with 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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 information will not be able to use that information to open new accounts or borrow money in your name. You will 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.

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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.

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.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting 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 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 Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your 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.

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**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

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

EXHIBIT B
Template Notification (Minor)

BANKERS LIFE®

Return Mail to IDX:
PO Box 480149
Niles, IL 60714

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/bankerslife

January 26, 2024

<<Variable Data 4>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

At Bankers Life[1] we take our customers' privacy seriously. For this reason, we are writing to let you know about an event that may affect the privacy of some of your child's personal information. Although we have no reason to believe that your child is at any risk of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your child's information, should you feel it appropriate to do so.

What Happened

On November 29, 2023, we discovered that a sophisticated threat actor targeted the cellular account belonging to a company senior officer. The threat actor conducted a highly coordinated, and complex "SIM swapping" attack, which the threat actor was able to do because a retailer for one of the top nationwide wireless carriers, without proper authorization or appropriate verification from the senior officer, allowed the senior officer's phone number to be swapped to what we believe was the threat actor's phone.

At Bankers Life, we employ a variety of security measures to prevent cyber criminals from accessing our data and data entrusted to us. Based on our investigation and response to this event, however, it appears the threat actor was able to bypass the multi-factor authentication and other common security controls the company had in place that were designed to protect the company's data. Because of the "SIM swapping," the threat actor was then able to gain access to certain company data.

When we first discovered the incident, we promptly notified law enforcement, and began working with the Federal Bureau of Investigation, the Offices of the United States Attorneys, and a full investigation is underway.

We have no evidence to suggest that any other company systems, accounts or personnel were impacted.

<<Variable Data 5>>

[1] Bankers Life is the marketing brand of Bankers Life and Casualty Company, Medicare Supplement insurance policies issued by Colonial Penn Life Insurance Company and Washington National Insurance Company, and select policies sold in New York by Bankers Conseco Life Insurance Company, a New York licensed insurance company.

What Information Was Involved

We believe that the threat actor's intention was to target the company itself. We have no reason to believe that your child's personal information was targeted by the threat actor. Nonetheless, we are providing you with this notice out of an abundance of caution because we believe the threat actor targeted Bankers Life's information, which included some of your child's personal information.

The personal information may have included your child's name, social security number, date of birth, and policy number(s) <<Variable Data 6>>.

What We Are Doing

When we first learned of this activity, we began an investigation and immediately took steps to contain any unauthorized access. We promptly disabled the senior officer's corporate access, reset passwords for personnel, and blocked the threat actor's potential access. We also scanned our environment, and implemented additional security measures designed to prevent the reoccurrence of this type of an event. In addition, we engaged federal law enforcement and hired an external forensics investigator to conduct an investigation and took steps to further restrict and monitor access to our systems and to enhance security procedures. We have also enhanced our policyholder safeguards to provide added protection to your child's personal information.

While we have no reason to believe your child's personal information was targeted or used, we would like to help protect your child's information from any potential unauthorized use. To that end, we are offering identity theft protection services through IDX, a leading provider of identity protection services. IDX services include: <<12/24>> months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do

IDX experts are available Monday through Friday from 6 am - 6 pm Pacific Time. **Please note the deadline to enroll is April 28, 2024**. The enclosed Reference Guide includes additional information on steps you can take to monitor and protect your child's personal information.

We encourage you to remain vigilant in monitoring account statements and insurance transactions for incidents of fraud and identity theft, and to promptly report such incidents. We encourage you to routinely review bills, notices, statements, and explanation of benefits that you receive from financial institutions, hospitals, doctors and health insurance companies.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps 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) 256-2082 or go to https://response.idx.us/bankerslife for any additional questions you may have.

Sincerely,

Bankers Life

Enclosure

Recommended Steps to Help Protect Your Child's Information

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/bankerslife and follow the instructions for enrollment using your child's Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at (888) 256-2082 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled your child 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 our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that your child falls victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if your child ever experiences 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 your child has 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.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below 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 child's credit files.

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

5. 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.

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.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting 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 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 Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your 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.

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**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

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