NASSAU

One American Row
P.O. Box 5056
Hartford, CT 06102-5056

860-403-5000
www.nfg.com

August 31, 2023

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Data Security Incident

To Whom it May Concern:

Pursuant to Iowa Code §§ 715C.1, 715C.2, I am writing to inform you of a cybersecurity event impacting Nassau Life and Annuity Company, one of its affiliates ("Nassau"), or a block of business administered by Nassau.

In July 2023, Nassau began an investigation and made an initial assessment to notify certain governmental bodies or supervisory authorities of a cybersecurity event. Specifically, on June 8th we received formal written notice from illumifin ("illumifin"), which administers blocks of in force policies for Nassau, that certain data related to Nassau customers was compromised and perhaps unlawfully acquired by a threat actor leveraging a vulnerability in the MOVEit file sharing platform. illumifin notified us that Pension Benefit, LLC ("PBI"), a third-party vendor that performs research services to illumifin, had discovered that a threat actor exploited that vulnerability in their instance of the MOVEit Transfer software to obtain unauthorized access to PBI's data on May 29 and May 30, 2023. illumifin shared certain files with Nassau to allow Nassau to investigate the provenance and details of the compromised information. We worked diligently to verify the data and on July 25th confirmed that the data relates to Nassau customers. Moreover, this initial assessment indicates that the name, Social Security Number, policy number and/or date of birth of 739 Iowa residents may have been compromised.

Nassau takes this matter very seriously and is doing everything it can to work closely with illumifin and others that have been impacted by this event to ensure that our customers and appropriate law enforcement and regulatory officials are promptly notified. We understand that illumifin has already notified federal law enforcement officials, has been working diligently to identify all the individuals whose data has been compromised, and that PBI will inform those individuals. A written notice will be sent to each affected individual at the address of record.

Nassau values the security of our customers' data. We understand that the MOVEit vulnerability may have impacted other third-party service providers, so we have proactively reached out to our top-tier vendors to confirm whether any additional customer data has been impacted. In addition, Nassau is analyzing our own cybersecurity and data security practices in accordance with our cybersecurity program and will continue to work with our existing risk management providers to identify, quantify, and mitigate the inherent risk in sharing sensitive data with vendors and business partners. These services help us analyze, rate, and monitor the security performance of third parties

in our vendor portfolio and provide a clear picture of the state of our portfolio's risk, allowing us to monitor companies within our portfolio and triage any concerns based on the risk they present to our business.

Nassau will continue to assess any obligations in connection with the cybersecurity event and is committed to answering any questions you may have. We will report any additional, relevant information, as appropriate. A copy of Nassau's privacy policy is enclosed with this letter as Exhibit A.

If you have any questions regarding this submission, please do not hesitate to contact Terry Davis, Vice President & Chief Information Security Officer, at tedavis@nfg.com or (860) 403-5633, Hayley Maldonado, Counsel, at hmaldonado@nfg.com or (860) 403-5540, or Marissa Zimmer, Director of Compliance, at mzimmer@nfg.com or (407) 547-3362.

***

Nassau claims confidential treatment for this letter and the information contained herein or attached hereto (together, the "Confidential Material"). The Confidential Material is furnished pursuant to Iowa Code §§ 715C.1, 715C.2 and concern, among others: (1) A description of how the nonpublic information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers; (2) How the cybersecurity event was discovered; (3) The identity of the source of the cybersecurity event; (4) The period during which the information system was compromised by the cybersecurity event; (5) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed; and (6) A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur. Accordingly, Nassau hereby requests, pursuant to Iowa Code §§ 715C.1, 715C.2 that the Confidential Material and all other documents and communications provided to the Office of the Attorney General of Iowa with regard to this matter be afforded confidential treatment.

In accordance with Iowa Code §§ 715C.1, 715C.2 and other applicable laws and regulations, Nassau submits the Confidential Material to your office with the request that it be kept in a non-public file and that only staff of your office have access to it. Should your office receive any request for any of the Confidential Material, pursuant to the Iowa Open Records Law or otherwise, Nassau requests that the undersigned be immediately notified of such request, and be furnished a copy of all written materials pertaining to such request (including but not limited to the request and any determination relating thereto), and that Nassau be given an opportunity to object in advance to any such disclosure.

Should the Office of the Attorney General of Iowa decide to grant such a request, Nassau requests that it be given at least ten (10) business days' advance notice of any such decision to enable it to pursue any remedies that may be available. In such event, Nassau requests that you telephone and email its counsel rather than rely on the United States mail for such notice. You may make such notification directly to the undersigned at tedavis@nfg.com or our outside counsel, Daniel Alvarez, at dalvarez@willkie.com. If the Office of the Attorney General of Iowa is not satisfied that the enclosed materials are exempt from disclosure pursuant to FOI, Nassau stands ready to supply further particulars, and to request a hearing on the claim of exemption.

Furthermore, the production of the Confidential Material to the Office of the Attorney General of Iowa is not intended to, and does not, waive any privilege or protection.

The requests set forth in the preceding paragraphs also apply to any memoranda, notes, transcripts, or other writings of any sort that are made by, or at the request of, any employee of your office (or any governmental agency) and which (1) incorporate, include, or relate to any Confidential Material; or (2) refer to any conference, meeting, or telephone conversations between Nassau's current or former employees, representatives, agents, auditors, or counsel on the one hand, and employees of your office (or any other governmental agency) on the other, relating to Confidential Material.

The Confidential Material is provided in an effort to facilitate the ongoing discussions between Nassau and the Office of the Attorney General of Iowa. Nassau reserves all rights.

Sincerely,

Terry Davis
Vice President & Chief Information Security Officer

EXHIBIT A

Nassau Privacy Statement

NASSAU

Effective Date: 9/10/2018

This Privacy Statement is provided on behalf of Nassau Life and Annuity Company, Nassau Life Insurance Company, Nassau Life and Annuity Insurance Company, and PHL Variable Insurance Company ("The Company," "we," "our," "us").

The Company respects your concerns about privacy and values the relationship we have with you. This Privacy Statement describes the types of information we collect about you, how we use the information, with whom we share it, the choices available to you regarding our use of the information, and how you can contact us about our privacy practices.

1. What Information Does This Privacy Statement Apply To?

This Privacy Statement applies to the collection, use, and disclosure of information from and about you by The Company in order to offer you products and services, determine whether you qualify for our products and services, and administer your account. This Privacy Statement also applies to the collection, use, and disclosure of information from and about you by The Company on our website (www.nfg.com), through our mobile application, through telephone communications, email communications, joint marketing agreements, and through agreements with nonaffiliated third parties.

2. What Information Does The Company Collect?

We may obtain information about you when you choose to provide it to us and when we collect it from third parties.

Information That You Or Others Provide

You may choose to provide information to us in a number of ways, such as when you request a quote, apply for a policy, sign up for promotions or newsletters, purchase our products, register on our website, post or provide content, or otherwise interact with us. The types of information you may provide to us include:

- Information we receive from you on applications or other forms or in order to provide you with a quote or illustration (such as name, address, city, state, ZIP code, email address, telephone number, birth date, household information, marital status, information about beneficiaries, and education);
- Information about your transactions and relationships with us, our affiliated companies, and others (such as products or services purchased, account balances, your policy coverage, premiums, and payment history). Financial and payment information (such as social security number, net worth, assets, income, payment card number, expiration date, account number, and billing address);
- Medical information (such as information about your health status or condition, payment for health care, etc.);
- Product preferences, advertisement preferences, and other information about how you use our website;
- Content you submit or post on our website (such as photographs, videos, reviews, articles, comments, or any other information you provide to us or post);
- Employment information;
- Records and copies of your correspondence (including email addresses), if you contact us.

We also may collect information about you from third parties, such as:

- Information we receive from a consumer reporting agency (such as information about your creditworthiness and credit history);
- Information we receive from third parties in order to issue and service your policies (such as motor vehicle reports and medical information);
- Information we receive from third party social media sites.

Investigative Consumer Reports

In some cases, we may request an independent reporting agency to prepare an investigative consumer report which contains information related to your personal characteristics, finances, general reputation, character, and mode of living. Information obtained primarily through personal interviews with friends, neighbors or associates. You have the right to be interviewed in connection with the preparation of such a report. Upon written request, a complete disclosure of the nature and scope of such a report, if one is made, will be provided as well as the name, address and phone number of the reporting agency so that you may request a copy of your report. If the information in a consumer report leads us to not approve your application or to charge an extra premium we will notify you and provide the reporting agency's name, address and phone number. We will never use the information we receive from an investigative consumer

report for marketing purposes. You should be aware that when an independent consumer reporting agency prepares such a report, they may keep it and disclose it to other companies upon request.

Medical Information Bureau

Information regarding your insurability will be treated as confidential. The Company, or its reinsurers may, however, make a brief report thereon to MIB, LLC, which operates an information exchange on behalf of insurance companies that are members of MIB Group Inc. If you apply to another MIB member company for life or health insurance coverage, or a claim for benefits is submitted to such company, MIB, upon request, will supply such company with the information in its file.

Upon receipt of a request from you, MIB will arrange disclosure of any information it may have in your file. You may contact MIB at 866-692-6901 or go to its website at www.mib.com to request disclosure online. If you question the accuracy of the information in MIB's file, you may contact MIB and seek a correction in accordance with the procedures set forth in the federal Fair Credit Reporting Act. The address of MIB's information office is 50 Braintree Hill Park, Suite 400, Braintree, MA 02184-8734.

The Company, or its reinsurers, may also release information in its file to other insurance companies to whom you may apply for life or health insurance, or to whom a claim for benefits may be submitted. Information for consumers about MIB may be obtained on its website at www.mib.com.

If you have questions or you wish to have a more detailed explanation or copies of the information we collect, please contact your producer or write to The Company directly. Write to: Nassau, Chief Underwriter, PO Box 22012, Albany, NY 12201-2012.

3. How Does The Company Use My Information?

We may use your information for the following purposes:

- offering you products and services, deciding if you qualify for our products and services, and servicing your account;
- establishing and verifying the identity and eligibility of website users;
- opening, maintaining, administering, managing, and servicing website user profiles, accounts or memberships;
- processing, servicing or enforcing transactions (including EFT, ACH, credit or debit card transactions);
- providing products, content, content suggestions, services, and support;
- conducting special events, sweepstakes, surveys, programs, contests, and other offers (and communicating with you about such events);
- analyzing and improving our products, services, or website (including developing new products and services; improving safety; managing our communications; analyzing our products; performing market research; performing data analytics; and performing accounting, auditing and other internal functions);
- providing users with product, service, or company updates;
- marketing and advertising our products or services as well as products and services of third parties (such as affiliates, subsidiaries, and business partners);
- responding to your inquiries or comments, or contacting you as necessary;
- operating and communicating with you about or through external social networking platforms;
- maintaining the security and integrity of our systems, including maintaining internal records;
- conforming to legal requirements or industry standards, complying with legal process, detecting and preventing fraud or misuse, defending our legal rights, or protecting others;
- as part of a merger, acquisition, bankruptcy, transfer, sale, corporate change, or any other transaction involving all or a portion of The Company's assets.

All information we collect may be aggregated and merged or enhanced with data from third party sources.

4. How Does The Company Share My Information?

We may disclose all of the information we collect (including your nonpublic personal financial information), as described in Section 2 above, to both affiliated and non-affiliated third parties, such as:

- To companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements;
- To financial services providers, such as life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents. We may also make such disclosures to an insurance institution, agent, insurance support organization, or self-insurer without your prior authorization, but only for purposes of (i) detecting or preventing fraud or other criminal activity; (ii) allowing the recipient to perform its function in connection with our insurance transactions; or (iii) as otherwise permitted by law;

- To a group plicyholder for reporting claims experience or for audit purposes;
- To a medical care institution or medical professional for purposes of verifying your insurance coverage or benefits, to inform someone of a medical condition of which that person might not be aware, or for conducting and operations or services audit to verify the individuals treated by the medical professional or at the medical care institution;
- To non-financial companies, such as retailers, direct marketers, airlines, and publishers;
- To third parties who help us with our business functions, such as service providers or suppliers. Examples of these service providers include entities that process credit card and other types of payments, help us moderate content posted on the Website, provide web hosting or analytics services, or who assist with marketing functions;
- To third parties involved in servicing and administering products and services on your behalf such as:
  - Your agent, broker or producer;
  - Banks;
  - Reinsurance companies;
  - Firms that assist us in the servicing of your policies;
  - Firms that assist in the printing or delivering of statements and notices;
- To other third parties for their own marketing purposes;
- To third parties for specific purposes permitted by law, such as:
  - If necessary to protect the safety, property, or other rights of us, our customers, or employees;
  - To comply with any court order, law, or legal process, including to respond to any government or regulatory request, or as otherwise required by law;
  - To State or federal regulators;
  - To auditors;
  - To law enforcement or another governmental authority for purposes of preventing or prosecuting fraud, or to report activities we reasonably believe are illegal;
  - With your consent in certain circumstances;

We may disclose information about our customers and our former customers to these third parties for the purposes described above.

We reserve the right to transfer information we have about you in the event we sell, transfer, or engage in another transaction involving all or a portion of our business or assets, or undertake another form of corporate change, including bankruptcy. Following such a sale, transfer, or transaction, or corporate change, you may contact the entity to which we transferred your information with any inquiries concerning the processing of that information.

Your information may be stored in databases maintained by The Company (including local storage) or third parties, and may be disclosed to third parties for the purposes stated in this Privacy Statement, that are located within and outside the United States, including countries where privacy rules differ and may be less stringent than those of the country in which you reside.

5. Is My Information Secure?

The Company will take reasonable precautions to protect your information from loss, misuse or alteration. For example, we have procedures in place that limit internal access to personal information to only those employees who need to access it in order to perform business services or market products on behalf of The Company and our affiliates. We educate our employees on the importance of protecting the privacy and security of your information. We also maintain physical, electronic and procedural safeguards that comply with federal and state regulations to guard your personal information.

Please be aware, however, that any email or other transmission you send through the Internet cannot be completely protected against unauthorized interception. As a result, we ask that you not send any confidential information to The Company via e-mail.

6. What Choices Do I Have?

If you prefer that we not disclose nonpublic personal financial information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may opt out by sending us an email request to opt out to corporate.compliance@nfg.com or by calling us at 1-800-813-8180. Note that you can only opt out of sharing your nonpublic personal financial information with nonaffiliated third parties for certain purposes; you cannot opt out of sharing such information with nonaffiliated third parties who are service providers to us, who engage

in joint marketing efforts with us, who assist us with processing and servicing transactions, or as otherwise permitted by law.

You may also "opt-out," or unsubscribe, from our newsletters, special offers or discounts, or other marketing communications by following the unsubscribe instructions in any e-mail or other communication you receive from us. After doing so, you will not receive future promotional emails unless you open a new account, enter a contest, or sign up to receive newsletters or emails. Please note that even after unsubscribing we may still disclose information as permitted or required by law including, but not limited to, service related announcements, important information about your policy, state required notices, and other non-marketing communications about your account or purchases that you have made. Please allow up to 2 weeks for us to process your request.

You may access personal information we have recorded about you by submitting a written request which reasonably describes the information requested. This information will be provided to you within thirty (30) business days from the date your written request is received so long as it is reasonably locatable and retrievable by us. You may also request the correction, amendment or deletion of any recorded personal information that we have in our possession. We will notify you of our decision to comply with your request or our reasons for refusal within thirty (30) business days from the date your written request is received. In the event we refuse your request, you will be provided with the opportunity to file a concise statement setting forth what you believe to be the correct, relevant or fair information and the reasons you may disagree with our determination.

We store data for as long as it is necessary to provide the products and services described in this Privacy Statement and for our internal business purposes. If you would like us to delete information, you may contact us using the information below and we will take reasonable efforts to delete your information from our records, but may need to keep a copy for administrative purposes (such as documenting that a transaction occurred).

This policy is meant for general use in every state. Any provision in this policy that is in conflict with the laws of your state is hereby amended to conform with the standards in your state.

Residents of California, New Mexico, Vermont:
We will not disclose personal information about you to any unaffiliated third party without first obtaining your affirmative, opt-in consent, except as expressly permitted by law.

7. How Can I Contact The Company?

The Company is committed to working with you to obtain a fair and rapid resolution of any queries, complaints, or disputes about privacy. If you have submitted information to The Company and you would like to have it deleted from our databases or corrected, or if you have any other questions or comments regarding our privacy practices, please email us at corporate.compliance@nfg.com for more information.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3(Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Pension Benefit Information, LLC ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations. PBI is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication 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 or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: <<b2b_text_2(name, data elements)>>.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and to report suspected identity theft incidents to the institution. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

For More Information. If you have additional questions, you may call our toll-free assistance line at (866) 676-4324 Monday through Friday from 9:00 am to 6:30 pm Eastern Time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

Sincerely,

The PBI Team

Steps You Can Take To Help Protect Personal Information

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.[1]

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **Credit Monitoring**. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.
- **Fraud Consultation**. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration**. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

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 Colorado and Illinois residents, you may obtain additional information from the credit reporting agencies and the FTC about fraud alerts and security freezes. You may also obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa residents, you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. You may obtain information from the FTC and the Office of the Maryland Attorney General about steps to avoid identity theft.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also request a complimentary security freeze by contacting the three major credit reporting bureaus listed above.

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 Oregon residents, you are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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. Fees may be required to be paid to the consumer reporting agencies. <<b2b_text_4(For certain PBI clients, there are approximately [#] Rhode Island residents that may be impacted by this event.)>>