Genworth

3100 Albert Lankford Drive
Lynchburg, Virginia 24501
434.948-5219
Frankie.Viar@genworth.com
genworth.com

July 13, 2023

Sent via electronic mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Anthony Brown:

We are writing to notify you that Genworth North America Corporation experienced a security event through the use of its third-party vendor, Pension Benefits Information, LLC, dba PBI Research Services, ("PBI").

Genworth North America Corporation, on behalf of its affiliate insurance companies Genworth Life and Annuity Insurance Company, Genworth Life Insurance Company, and Genworth Life Insurance Company of New York (collectively, "Genworth"), uses PBI to, among other things, satisfy applicable regulatory obligations to search various databases to identify the deaths of insured persons under life insurance policies, and to identify the deaths of insured persons under long-term care insurance, and annuity policies which can impact premium payment obligations and benefit eligibility. For life insurance policies and annuity contracts, this helps identify the possible eligibility of beneficiaries for death benefits even prior to the submission of claims, or for policies that beneficiaries may not know exist.

Genworth also uses PBI for its insurance company clients for whom Genworth has assumed, reinsures, and/or administers business. Genworth is notifying you on behalf of those companies whose data was involved, which are listed in Appendix A to this letter.

PBI advised Genworth of a security event connected to a vulnerability in the MOVEit file transfer software that PBI uses. The occurrence of the event was May 29, 2023, and the end date was May 30, 2023. On June 2, 2023, PBI implemented the patches provided by Progress Software, the producer of MOVEit. The Cybersecurity and Infrastructure Security Agency has publicly stated that, according to open-source information, the CL0P Ransomware Gang was behind the MOVEit Transfer security event[1].

On June 16th, PBI advised Genworth that specific Genworth files were compromised due to the security event. Genworth determined that the files involved in this security event included the information of approximately 51,495 individuals in Maryland where approximately 232 of those individuals are deceased. Please also see in Appendix A the number of individuals associated with each of the companies on behalf of which Genworth is providing this notice.

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a; visited on July 1, 2023.

On behalf of Genworth and the companies noted in Appendix A, PBI will provide notifications to all impacted individuals, which are anticipated to begin mailing on or around July 14, 2023. PBI is offering all impacted living individuals with 24 months of credit monitoring, fraud consultation, and identity theft restoration services through Kroll at no cost to the individuals. Details of this offer and instructions on how to activate these services are enclosed with each notification letter to individuals. Additionally, PBI will provide notifications to families or personal representatives of all deceased individuals with instructions on how to protect their loved one's information. All letters describe what happened, what personal information was involved, what PBI is doing, and what the person can do to protect their information. A sample copy of each notification letter is attached.

The personal information data elements impacted for the customers includes one or more of the following: First and Last Name, SSN, Date of Birth, Zip Code, State, Policy Number, Individual's Role (ex., Annuitant, Joint Insured, Owner, etc.), and general product type. For customers who are deceased, the additional personal information data elements include City, Date of Death, and the source of that information.

The personal information data elements impacted for insurance agents includes one or more of the following: Master Agent ID, First/Middle/Last Name, Birthdate, Resident Address/City/State/Zip Code, Primary Preferred Address/City/State/Zip Code. "Master Agent ID" is the insurance agent's SSN. For insurance agents who are deceased, the additional personal information data elements include Date of Death and the source of that information.

PBI has advised Genworth that PBI notified federal law enforcement regarding this security event. Genworth does not use the MOVEit software applications on any company system and this was not a breach of Genworth's information systems. Please note, however, that Genworth maintains a written information security program for our operations and information systems.

If you should have any questions regarding this notice, please direct them to my attention at Frankie.Viar@genworth.com, datasecurityteam.genworth@genworth.com, or at 434 948-5219.

Sincerely,

Frank E. Viar
Director of Operational Risk and Crisis Management

Appendix A

Company Name	Number of all Individuals Impacted in Maryland
Brighthouse Life Insurance Company	1,693
Highmark Blue Cross Blue Shield Company	3
RiverSource Life Insurance Company	1,575
RiverSource Life Insurance Company of New York	24
Equitable Financial Life Insurance Company	62
Union Fidelity Life Insurance Company	2

<<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, dba PBI Research Services ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including <<b2b_text_1(data owner)>>, or for a third party acting on their behalf. PBI is providing notice of a third-party software event that affected the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event at the time of this mailing, 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 your 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 at the time of this mailing, 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 insurance company. Please also review the enclosed *Steps You Can Take to Protect Personal Informatio*n, 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) 373-9043, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402 or to the insurance company at 3100 Albert Lankford Drive, Lynchburg, VA 24501.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

Steps You Can Take To 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, free of charge, 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:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the prior two to five years;
- Proof of current address, such as a current utility bill or telephone bill;

[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.

- A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
- 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/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 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 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/.

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

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

To the Estate/Next of Kin of:
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3(Notice of Data Breach)>>

To the Personal Representative / Next of Kin of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Pension Benefit Information, LLC, dba PBI Research Services ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including <<b2b_text_1(data owner)>>, or for a third party acting on their behalf. PBI is providing notice of a third-party software event that affected the security of some of your loved one's information. Although we have no indication of identity theft or fraud in relation to this event at the time of this mailing, we are providing you with information about the event, our response, and additional measures you can take to help protect your loved one's 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 your loved one's 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 your loved one were present in the server at the time of the event: Name, Date of Death and the source of that information, and <<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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your loved one's account statements and monitoring your loved one's free credit reports, if available, for suspicious activity and to detect errors and to report suspected identity theft incidents to the insurance company. Please also review the enclosed *Steps You Can Take to Protect Your Loved One's Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information.

For More Information. If you have additional questions, you may call our toll-free assistance line at (866) 373-9043, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402 or to the insurance company at 3100 Albert Lankford Drive, Lynchburg, VA 24501.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

Steps You Can Take To Protect Your Loved One's Personal Information

Monitor Your Loved One's Accounts

Authorized individuals, a spouse, or an executor of an estate may request a copy of a loved one's credit report or flag a loved one's credit file with an alert. In most cases, a flag will prevent the opening of new credit accounts in your loved one's name. If you have not already done so, you may request that your loved one's credit report is flagged with the following alert: **"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (name and relationship to your loved one)."**

Individuals to list in this alert may include:

- next surviving relative, and/or
- another authorized relative, and/or
- executor/trustee of the estate, and/or
- a law enforcement agency.

You may also request a copy of your loved one's credit report to review whether there are any active credit accounts that need to be closed or any pending collection notices that need to be addressed. A request for a flag on your loved one's credit file or for a copy of your loved one's credit report must be in writing and should include the below information:

Information Related to your loved one:

- Legal name
- Social Security number
- Date of birth
- Date of death
- Last known address
- A copy of the death certificate or letters testamentary. A "letters testamentary" is a document issued by a court or public official authorizing the executor of a will to take control of a deceased person's estate.

Information related to the individual requesting the information or placing the alert:

- Full name
- Copy of a government issued identification
- Address for sending final confirmation
- In the case of an executor, include the court order or other document indicating the executor of the estate

Mailing and contact information for the three major credit bureaus is as follows:

Experian	**TransUnion**	**Equifax**
P.O. Box 9701 Allen, TX 75013 1-888-397-3742 www.experian.com/blogs/ask-experian/reporting-death-of-relative/	P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com/blog/credit-advice/reporting-a-death-to-tu	P.O. Box 105139 Atlanta, GA 30348-5139 1-800-685-1111 www.equifax.com/personal/education/credit/report/credit-steps-after-death/

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your loved one's 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 their loved one has 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; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.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. Fees may be required to be paid to the consumer reporting agencies. <<b2b_text_4(There are approximately [#] Rhode Island residents that may be impacted by this event.)>>

Genworth

3100 Albert Lankford Drive
Lynchburg, Virginia 24501
434.948-5219
Frankie.Viar@genworth.com
genworth.com

November 7, 2023

Sent by electronic mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Anthony Brown:

Genworth North America Corporation and its subsidiary insurance companies (collectively, Genworth) are writing to supplement our last notice dated on July 31, 2023, regarding the security event at our third-party vendor, Pension Benefits Information, LLC, dba PBI Research Services (PBI).

Genworth is updating its previous notification to advise mailings to impacted residents in your state are complete for Genworth and its insurance company clients for which Genworth has notified you on their behalf ("Companies"). Additionally, the final total number of Maryland residents impacted for Genworth is revised from 53,495 to 53,988, where 242 individuals of that number are deceased. Please see attached Appendix A for the final total number of Maryland residents impacted for Companies.

If you should have any questions regarding this notice, please direct them to my attention at Frankie.Viar@genworth.com, datasecurityteam.genworth@genworth.com, or at 434 948-5219.

Sincerely,

Frank E Viar

Frank Viar
Director of Operational Risk and Crisis Management

Appendix A

Company Name	Number of all Individuals Impacted in Maryland	Number of Deceased Individuals of those Impacted in Maryland
Brighthouse Life Insurance Company	1,693	16
Highmark Blue Cross Blue Shield Company	4	0
RiverSource Life Insurance Company	1,582	11
RiverSource Life Insurance Company of New York	24	0
Equitable Financial Life Insurance Company	63	0
Union Fidelity Life Insurance Company	4	0
Combined Insurance Company of America	356	1
Blue Cross Blue Shield of Louisiana	1	0
Blue Cross Blue Shield of Oklahoma	2	0
Blue Cross Blue Shield of Nebraska	2	0

Genworth

3100 Albert Lankford Drive
Lynchburg, Virginia 24501
434.948-5219
Frankie.Viar@genworth.com
genworth.com

July 17, 2023

Sent via electronic mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Anthony Brown:

Genworth North America Corporation (Genworth) is writing to supplement our initial notice sent on July 13, 2023, regarding the security event through the use of our third-party vendor, Pension Benefits Information, LLC, dba PBI Research Services.

Please see attached a revised Appendix A, which is updated to include additional companies, on whose behalf Genworth is providing notification.

Additionally, the approximate total number of Maryland residents impacted for Genworth is revised from 51,495 to 51,511.

If you should have any questions regarding this notice, please direct them to my attention at Frankie.Viar@genworth.com, datasecurityteam.genworth@genworth.com, or at 434 948-5219.

Sincerely,

Frank E Viar

Frank Viar
Director of Operational Risk and Crisis Management

Appendix A

Company Name	Number of all Individuals Impacted in Maryland
Brighthouse Life Insurance Company	1,693
Highmark Blue Cross Blue Shield Company	3
RiverSource Life Insurance Company	1,575
RiverSource Life Insurance Company of New York	24
Equitable Financial Life Insurance Company	62
Union Fidelity Life Insurance Company	2
Combined Insurance Company of America	180
Blue Cross Blue Shield of Louisiana	1
Blue Cross Blue Shield of Oklahoma	2
Blue Cross Blue Shield of Nebraska	2

Genworth

3100 Albert Lankford Drive
Lynchburg, Virginia 24501
434.948-5219
Frankie.Viar@genworth.com
genworth.com

July 31, 2023

Sent via electronic mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Anthony Brown:

Genworth North America Corporation (Genworth) is writing to supplement our last notice provided on July 17, 2023, regarding the security event through the use of our third-party vendor, Pension Benefits Information, LLC, dba PBI Research Services (PBI).

Genworth is updating its previous notification to advise that Genworth and certain of its insurance company clients for whom Genworth has provided notification on their behalf are sending an additional letter to provide your residents with notification of the security event within the 45 days required by your state's law. Two sample copies of this notification are attached. Genworth has also provided additional consumer and deceased consumer templates on behalf of certain of its insurance company clients. Two sample copies of this notification are attached.

Additionally, the approximate total number of Maryland residents impacted for Genworth is revised from 51,511 to 53,495. Please also see attached a revised Appendix A, which is updated to provide a new estimate of Maryland residents impacted for Combined Insurance Company of America.

If you should have any questions regarding this notice, please direct them to my attention at Frankie.Viar@genworth.com, datasecurityteam.genworth@genworth.com, or at 434 948-5219.

Sincerely,

Frank Viar
Director of Operational Risk and Crisis Management

Appendix A

Company Name	Number of all Individuals Impacted in Maryland
Brighthouse Life Insurance Company	1,693
Highmark Blue Cross Blue Shield Company	3
RiverSource Life Insurance Company	1,575
RiverSource Life Insurance Company of New York	24
Equitable Financial Life Insurance Company	62
Union Fidelity Life Insurance Company	2
Combined Insurance Company of America	351
Blue Cross Blue Shield of Louisiana	1
Blue Cross Blue Shield of Oklahoma	2
Blue Cross Blue Shield of Nebraska	2

Genworth

3100 Albert Lankford Dr.
Lynchburg, VA 24501

Important Update July 31, 2023 from

Customer service
999.999.9999
M–TH: 8:30AM – 6PM EST
FRI: 9AM – 6PM EST
genworth.com

[NAME]
[ADDR2]
[ADDR]
[CITY, ST ZIP]

Dear [NAME]:

Genworth was recently notified by PBI Research Services (PBI) that **your personal information was involved in a data security event** that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses. PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

PBI advised that the event occurred from May 29, 2023 to May 30, 2023. On June 2, 2023, PBI implemented the patches (or fixes) provided by Progress Software, the producer of MOVEit. On June 16, 2023, PBI advised Genworth that specific Genworth files containing policyholder and agent information were compromised.

For customers, the exposed information includes one or more of the following: social security number, first and last name, date of birth, zip code, state of residence, policy number, the role of the individual (ex. Annuitant, Joint Insured, Owner, etc.), and general product type. For agents, the exposed information includes one or more of the following: social security number, first, middle, and last name, date of birth, full address, and a preferred full address.

While no Genworth information systems or business operations were impacted by this event, we take very seriously our responsibility to protect the data you entrust to us—and we expect the same from our vendors. Unfortunately, a vulnerability in the MOVEit software was exploited, enabling the PBI security event.

To help you monitor for identify theft, PBI is providing 24 months of credit monitoring, fraud consultation, and identity theft restoration services from Kroll , free of charge. Please watch for a letter from PBI in an envelope with the PBI logo with activation instructions for this coverage. If you have not received the mailing by August 15th (or you discarded it), you can call Genworth (888.436.9678) to learn how to activate your credit protection services.

You can visit genworth.com/moveit for up-to-date FAQs on the security event and Genworth's response, as well as tips on protecting your identity. Please also see our **Guide to Protecting Yourself from Identity Theft**. While the MOVEit event has impacted many organizations globally, Genworth remains focused on protecting your personal information within our own systems and those of our vendors.

Thank you very much,

Tom McInerney
President & CEO
Genworth

---

1 Your letter from PBI will provide you with your specific data elements.

2 https://enroll.krollmonitoring.com

Guide to Protecting Yourself from Identity Theft

You should remain vigilant and review your financial statements, credit card bills and free credit reports for errors or suspicious or unusual activity. If you suspect you are a victim of identity theft, you can report this to law enforcement, including your Attorney General, local police, and the Federal Trade Commission. The Federal Trade Commission can also provide information about the steps you can take to avoid identify theft, and can be reached at 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261; www.identitytheft.gov; and 600 Pennsylvania Avenue NW, Washington, D.C. 20580.

You may want to consider placing a fraud alert and/or credit freeze on your credit file by calling any of the consumer reporting agencies. They will notify the other agencies to do the same. A fraud alert tells creditors to contact you before they open a new account in your name or change your existing accounts. A fraud alert will, however, make it harder to take advantage of 'instant credit' offers from retailers. A free credit freeze will restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can request a credit freeze online, by phone, or by mail. You will also need to answer questions to verify your identity and will need to provide your Social Security Number, a copy of your photo ID, and proof of your residence.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/creditreport-services/	https://www.experian.com/help/	https://www.transunion.com/credithelp
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

You can get a free credit report once a year from each of the three agencies. Go to annualcreditreport.com or call 877-322-8228. You may order one, two or all three credit reports at the same time or you may stagger your requests over a 12-month period to keep an eye on the accuracy and completeness of the information in your reports.

Residents of Maryland
You can obtain information about how to avoid identity theft from the Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202. 888-743-0023. www.oag.state.md.us/idtheft/index.htm
E-mail: idtheft@oag.state.md.us.

Residents of New Mexico
The federal Fair Credit Reporting Act provides you certain rights regarding your credit. You may review these rights at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Important Update July 31, 2023
from

3100 Albert Lankford Dr.
Lynchburg, VA 24501

Customer service
999.999.9999
M–TH: 8:30AM – 6PM EST
FRI: 9AM – 6PM EST

[NAME]
[ADDR2]
[ADDR]
[CITY, ST ZIP]

Dear [NAME]:

We were recently notified that **your personal information was involved in a data security event** that took advantage of a vulnerability in the widely-used MOVEit file transfer software used by PBI Research Services (PBI). PBI is a vendor used to scan various databases to identify deaths that have occurred under an insurance policy.

PBI advised that the event occurred from May 29, 2023 to May 30, 2023. On June 2, 2023, PBI implemented the patches (or fixes) provided by Progress Software, the producer of MOVEit. On June 18, 2023, we were advised files containing customer information were compromised.

For customers, the exposed information includes one or more of the following: social security number, first and last name, date of birth, zip code, state of residence, policy number, the role of the individual (ex. Annuitant, Joint Insured, Owner, etc.), and general product type.

We take very seriously our responsibility to protect the data you entrust to us—and we expect the same from vendors. Unfortunately, a vulnerability in the MOVEit software was exploited, enabling the PBI security event.

To help you monitor for identify theft, **PBI is providing 24 months of credit monitoring, fraud consultation, and identity theft restoration services from Kroll , free of charge. Please watch for a letter from PBI in an envelope with the PBI logo with activation instructions for this coverage.** If you have not received the mailing by August 15th (or you discarded it), you can call us at 999.999.9999 to learn how to activate your credit protection services. Please also see our **Guide to Protecting Yourself from Identity Theft.**

While the MOVEit event has impacted many organizations globally, we remain focused on protecting your personal information.

Thank you very much,

Customer Service

---

1 Your letter from PBI will provide you with your specific data elements.

2 https://enroll.krollmonitoring.com

Guide to Protecting Yourself from Identity Theft

You should remain vigilant and review your financial statements, credit card bills and free credit reports for errors or suspicious or unusual activity. If you suspect you are a victim of identity theft, you can report this to law enforcement, including your Attorney General, local police, and the Federal Trade Commission. The Federal Trade Commission can also provide information about the steps you can take to avoid identify theft, and can be reached at 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261; www.identitytheft.gov; and 600 Pennsylvania Avenue NW, Washington, D.C. 20580.

You may want to consider placing a fraud alert and/or credit freeze on your credit file by calling any of the consumer reporting agencies. They will notify the other agencies to do the same. A fraud alert tells creditors to contact you before they open a new account in your name or change your existing accounts. A fraud alert will, however, make it harder to take advantage of 'instant credit' offers from retailers. A free credit freeze will restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can request a credit freeze online, by phone, or by mail. You will also need to answer questions to verify your identity and will need to provide your Social Security Number, a copy of your photo ID, and proof of your residence.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/creditreport-services/	https://www.experian.com/help/	https://www.transunion.com/credithelp
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

You can get a free credit report once a year from each of the three agencies. Go to annualcreditreport.com or call 877-322-8228. You may order one, two or all three credit reports at the same time or you may stagger your requests over a 12-month period to keep an eye on the accuracy and completeness of the information in your reports.

Residents of Maryland
You can obtain information about how to avoid identity theft from the Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202. 888-743-0023. www.oag.state.md.us/idtheft/index.htm
E-mail: idtheft@oag.state.md.us.

Residents of New Mexico
The federal Fair Credit Reporting Act provides you certain rights regarding your credit. You may review these rights at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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

To the Estate/Next of Kin of:
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3(Notice of Data Breach)>>

To the Personal Representative / Next of Kin of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Pension Benefit Information, LLC, dba PBI Research Services ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, or for a third party acting on their behalf. PBI is providing notice of a third-party software event that affected the security of some of your loved one's information. Although we have no indication of identity theft or fraud in relation to this event at the time of this mailing, we are providing you with information about the event, our response, and additional measures you can take to help protect your loved one's 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 your loved one's 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 your loved one were present in the server at the time of the event: date of death and the source of that information, as well as <<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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your loved one's account statements and monitoring your loved one's free credit reports, if available, for suspicious activity and to detect errors and to report suspected identity theft incidents to the insurance company. Please also review the enclosed *Steps You Can Take to Protect Your Loved One's Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information.

For More Information. If you have additional questions, you may call our toll-free assistance line at (866) 373-9043, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402 or to the insurance company at 3100 Albert Lankford Drive, Lynchburg, VA 24501.

Sincerely,

The PBI Team

Steps You Can Take To Protect Your Loved One's Personal Information

Monitor Your Loved One's Accounts

Authorized individuals, a spouse, or an executor of an estate may request a copy of a loved one's credit report or flag a loved one's credit file with an alert. In most cases, a flag will prevent the opening of new credit accounts in your loved one's name. If you have not already done so, you may request that your loved one's credit report is flagged with the following alert: **"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (name and relationship to your loved one)."**

Individuals to list in this alert may include:

- next surviving relative, and/or
- another authorized relative, and/or
- executor/trustee of the estate, and/or
- a law enforcement agency.

You may also request a copy of your loved one's credit report to review whether there are any active credit accounts that need to be closed or any pending collection notices that need to be addressed. A request for a flag on your loved one's credit file or for a copy of your loved one's credit report must be in writing and should include the below information:

Information Related to your loved one:

- Legal name
- Social Security number
- Date of birth
- Date of death
- Last known address
- A copy of the death certificate or letters testamentary. A "letters testamentary" is a document issued by a court or public official authorizing the executor of a will to take control of a deceased person's estate.

Information related to the individual requesting the information or placing the alert:

- Full name
- Copy of a government issued identification
- Address for sending final confirmation
- In the case of an executor, include the court order or other document indicating the executor of the estate

Mailing and contact information for the three major credit bureaus is as follows:

Experian	**TransUnion**	**Equifax**
P.O. Box 9701 Allen, TX 75013 1-888-397-3742 www.experian.com/blogs/ask-experian/reporting-death-of-relative/	P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com/blog/credit-advice/reporting-a-death-to-tu	P.O. Box 105139 Atlanta, GA 30348-5139 1-800-685-1111 www.equifax.com/personal/education/credit/report/credit-steps-after-death/

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your loved one's 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 their loved one has 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; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.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. 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.)>>

pbi

<<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, dba PBI Research Services ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, or for a third party acting on their behalf. PBI is providing notice of a third-party software event that affected the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event at the time of this mailing, 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 your 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 at the time of this mailing, 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 insurance company. Please also review the enclosed *Steps You Can Take to Protect Personal Informatio*n, 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) 373-9043, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402 or to the insurance company at 3100 Albert Lankford Drive, Lynchburg, VA 24501.

Sincerely,

The PBI Team

Steps You Can Take To 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, free of charge, 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:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the prior two to five years;
- Proof of current address, such as a current utility bill or telephone bill;

[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.

- A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
- 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/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 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 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/.

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. 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.)>>