HUNTON ANDREWS KURTH

HUNTON ANDREWS KURTH LLP
200 PARK AVENUE
NEW YORK, NY 10166-0005

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

LISA J. SOTTO
DIRECT DIAL: 212 • 309 • 1223
EMAIL: lsotto@HuntonAK.com

FILE NO: 096442.0000001

September 7, 2023

Via E-mail (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing to notify you regarding a data security issue.

On May 31, 2023, Kirkland & Ellis LLP ("Kirkland" or the "Firm") was informed by its third-party software provider, Progress Software, of a cybersecurity issue involving the provider's MOVEit Transfer solution. MOVEit is a file transfer tool used by many organizations, including Kirkland, to support the transfer of data files. After learning of the issue, Kirkland quickly initiated an investigation and took steps to secure its relevant systems. Kirkland has been working with leading cybersecurity experts to determine the nature and scope of the issue. Kirkland also reported the issue to law enforcement and put in place additional monitoring measures to further protect its systems.

Through Kirkland's investigation, the Firm found that, between around May 27 and May 31, 2023, an unauthorized third party obtained certain of Kirkland's files that were transferred through the MOVEit tool. Kirkland has been working diligently with the support of a third-party vendor to review the affected files to understand their nature and scope. Based on this review, on approximately July 27, 2023, Kirkland concluded that certain affected files contained personal information such as name and Social Security number. The types of affected personal information varied by individual.

Kirkland has been taking steps to identify mailing address information for affected individuals and preparing to notify them. Based on these efforts, on September 7, 2023, the Firm began notifying affected Maryland residents of the issue. To date, the Firm has notified approximately one Maryland resident of the issue. The Firm has arranged to offer 24 months

HUNTON
ANDREWS KURTH

of identity protection and credit monitoring services at no cost to the affected individual. Attached for your reference is a copy of the notice being sent to the affected individual.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

Lisa J. Sotto

Lisa J. Sotto

Enclosure

KIRKLAND & ELLIS LLP

AND AFFILIATED PARTNERSHIPS

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 7, 2023

J9570-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to notify you of an issue that involves certain of your personal information. As a law firm, Kirkland & Ellis LLP obtains certain personal information in the course of providing legal services to clients. We take the safeguarding of this information very seriously and are providing this notice to explain what happened and the actions we took in response.

What Happened?

On May 31, 2023, we were informed by our third-party software provider, Progress Software, of a cybersecurity issue involving its MOVEit Transfer solution. MOVEit is a file transfer tool used by many organizations, including us, to support the transfer of data files. After learning of the issue, we quickly initiated an investigation and took steps to secure our relevant systems. Through our investigation, we found that, between around May 27 and May 31, 2023, an unauthorized third party obtained certain of our files that were transferred through the MOVEit tool.

What Information Was Involved?

We have been working diligently to review the affected files to understand their nature and scope. Based on this review, we recently concluded that certain affected files contained personal information such as name, contact information, date of birth, and Social Security number. The types of affected personal information varied by individual.

What We Are Doing

We have been working with leading cybersecurity experts to determine the nature and scope of the issue. We also reported the issue to law enforcement and put in place additional monitoring measures to further protect our systems.

What You Can Do

We regret any inconvenience this may cause and are informing you about this issue so you can take steps to help protect your information. Steps you can take include:

- Register for Identity Protection Services. We have arranged to offer you credit monitoring and identity restoration services for 24 months at no cost to you.
- Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at (877) 322-8228.
- Remain Vigilant. We encourage you to review your account statements for suspicious activity and monitor your free credit reports.
- Review the Enclosed Reference Guide. The enclosed Reference Guide provides information on registration for identity protection services and recommendations on the protection of personal information.

For More Information

If you have any questions regarding this issue, please call 888-397-0098, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please be prepared to provide your engagement number B103549.

Sincerely,

KIRKLAND & ELLIS LLP

Reference Guide

We encourage affected individuals to take the following steps:

Register for Identity Protection Services. We have arranged with Experian to offer you identity restoration and credit monitoring services for 24 months at no cost to you. These Experian IdentityWorks services include:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

To activate your membership, please follow the steps below:

- Enroll by: **December 31, 2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: **ABCDEFGHI**

If you have questions about the services, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0098 by **December 31, 2023**. Please be prepared to provide engagement number **B103549** as proof of eligibility for the identity restoration services offered by Experian.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	(800) 525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	(888) 397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	(800) 680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755
(800) 788-9898
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)727-3400
www.oag.dc.gov

HUNTON
ANDREWS KURTH

HUNTON ANDREWS KURTH LLP
200 PARK AVENUE
NEW YORK, NY 10166-0005

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

LISA J. SOTTO
DIRECT DIAL: 212 • 309 • 1223
EMAIL: lsotto@HuntonAK.com

FILE NO: 096442.0000001

June 14, 2024

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of Kirkland & Ellis LLP ("Kirkland" or the "Firm") to provide an update regarding a data security issue. Kirkland previously notified your office about this issue on September 7, 2023. This update is intended to supplement that prior notification.

As indicated in Kirkland's prior notification to your office, Kirkland has been notifying affected individuals of a security issue involving the unauthorized acquisition of their personal information in files transferred through Progress Software's MOVEit Transfer solution. Please refer to Kirkland's prior notification for more details.

Since initially notifying your office, Kirkland has continued to coordinate with relevant clients to send additional notifications to affected individuals. As of May 28, 2024, Kirkland has notified approximately 780 affected Maryland residents. The Firm has arranged to offer 24 months of identity protection and credit monitoring services at no cost to the affected individuals. Attached for your reference is a sample of the notice sent to the affected individuals.

HUNTON
ANDREWS KURTH

Please do not hesitate to contact me if you have any questions.

Very truly yours,

Lisa J. Sotto

Lisa J. Sotto

Enclosure

KIRKLAND & ELLIS LLP
AND AFFILIATED PARTNERSHIPS

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 28, 2024

L3779-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 A
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to notify you of an issue that involves certain of your personal information. As a law firm, Kirkland & Ellis LLP obtains certain personal information in the course of providing legal services to clients. We take the safeguarding of this information very seriously and are providing this notice to explain what happened and the actions we took in response.

What Happened?

On May 31, 2023, we were informed by our third-party software provider, Progress Software, of a cybersecurity issue involving its MOVEit Transfer solution. MOVEit is a file transfer tool used by many organizations, including us, to support the transfer of data files. After learning of the issue, we quickly initiated an investigation and took steps to secure our relevant systems. Through our investigation, we found that, between around May 27 and May 31, 2023, an unauthorized third party obtained certain of our files that were transferred through the MOVEit tool.

What Information Was Involved?

We have been working diligently to review the affected files to understand their nature and scope. Based on this review, we concluded that certain affected files contained personal information such as name, contact information, date of birth, government-issued identification information (such as Social Security number, driver's license, or passport number), financial account details, health-related information, online account credentials (such as username or email and password or security answer) and certain employment-related information (such as compensation information). The types of affected personal information varied by individual.

What We Are Doing

We have been working with leading cybersecurity experts to determine the nature and scope of the issue. We also reported the issue to law enforcement and put in place additional monitoring measures to further protect our systems.

What You Can Do

We regret any inconvenience this may cause and are informing you about this issue so you can take steps to help protect your information. Steps you can take include:

- Register for Identity Protection Services. We have arranged to offer you credit monitoring and identity restoration services for 24 months at no cost to you.
- Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at (877) 322-8228.
- Remain Vigilant. We encourage you to review your account statements for suspicious activity and monitor your free credit reports.
- Review the Enclosed Reference Guide. The enclosed Reference Guide provides information on registration for identity protection services and recommendations on the protection of personal information.

For More Information

If you have any questions regarding this issue, please call **833-918-5079**, toll-free Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays). Please be prepared to provide your engagement number **B123478**.

Sincerely,

Kirkland & Ellis LLP

Reference Guide

We encourage affected individuals to take the following steps:

Register for Identity Protection Services. We have arranged with Experian to offer you identity restoration and credit monitoring services for 24 months at no cost to you. These Experian IdentityWorks services include:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

To activate your membership, please follow the steps below:

- Enroll by: **August 30, 2024** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your activation code: ABCDEFGHI

If you have questions about the services, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-5079 by **August 30, 2024**. Please be prepared to provide engagement number **B123478** as proof of eligibility for the identity restoration services offered by Experian.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	(800) 525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	(888) 397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	(800) 680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike* *a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755
(800) 788-9898
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)727-3400
www.oag.dc.gov