

Karen Bridges
Direct Dial: (312) 642-7127
E-mail: kbridges@mcdonaldhopkins.com

December 6, 2024

VIA EMAIL (Idtheft@oaq.state.md.us)

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

Re: Pyramid ETC Companies, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Pyramid ETC Companies, LLC (“Pyramid”) located at 275 Franklin Turnpike, Ramsey, NJ 07446, regarding a recent security incident. I am writing to provide notification of an incident at Pyramid that may affect the security of personal information of approximately four (4) Maryland residents. By providing this notice, Pyramid does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about September 18, 2024, Pyramid discovered that an unauthorized actor gained access to the network environment. Upon learning of this issue, Pyramid immediately worked to contain the threat and secure the internal environment. Specifically, Pyramid commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been compromised as a result of this incident. Pyramid also reported this incident to the FBI. After an extensive forensic investigation, Pyramid discovered on November 15, 2024 that the impacted systems, which were accessed between September 3, 2024 and September 18, 2024, contained some personal information. On December 2, 2024, Pyramid discovered that some of the impacted individuals are Maryland residents.

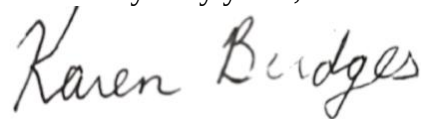
To date, Pyramid is not aware of any reports of identity fraud or financial fraud for any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Pyramid wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Pyramid is providing the affected residents with notification of this incident, commencing on or about December 6, 2024. The notice will be in substantially the same form as the letter attached hereto. Pyramid is also offering the affected residents with complimentary credit monitoring services. Pyramid is advising the affected residents to always remain vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis. Pyramid is also advising

the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Pyramid, protecting the privacy of personal information is a top priority. Pyramid is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Further, Pyramid continues to evaluate and improve, where appropriate, its administrative and technical safeguards including its policies, procedures, protocols, and tools to protect its network environment.

If you have any additional questions, please contact me at (312) 642-7127 or kbridges@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink that reads "Karen Bridges". The signature is written in a cursive, flowing style.

Karen Bridges

Encl.

Pyramid ETC Companies, LLC
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 6, 2024

Dear [REDACTED]

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

The privacy and security of the personal information we maintain is of the utmost importance to Pyramid ETC Companies, LLC. As such, we are writing to you today with an important update regarding a recent data security incident that may have involved some of your personal information. We want to provide you with details about the incident we recently experienced, explain the services we are making available to you, and assure you that we are continuing to take significant measures to protect your information.

What Happened?

We recently discovered that an unauthorized actor gained access to our network environment.

What Are We Doing?

Upon learning of this issue, we immediately worked to contain the threat and secure our internal environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been compromised as a result of this incident. After an extensive forensic investigation, we discovered on November 15, 2024 that the impacted systems, which were accessed between September 3, 2024 and September 18, 2024, contained some of your personal information as described in more detail below.

What Information Was Involved?

The unauthorized actor gained access to some of your personal information, specifically your first and last name and [REDACTED]

What Can You Do?

We have no reason to believe that your information has been or will be misused as a direct result of this incident. However, out of an abundance of caution and in an effort to protect you from potential misuse of your information, we are offering a **complimentary** [REDACTED] month membership of identity theft protection services through IDX. IDX identity protection services include: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. The deadline to enroll in these services is March 6, 2025.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files and/or obtaining a free credit report, below. Additionally, we recommend that you always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We are committed to maintaining the privacy and security of the personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information and will continue to do so following this incident.

If you have any further questions regarding this incident, please call our toll-free response line at [REDACTED]. The response line is available Monday through Friday, from 9am to 9pm Eastern, excluding major US holidays. We sincerely apologize for this incident and for any inconvenience this may have caused you.

Sincerely,

Pyramid ETC Companies, LLC
[REDACTED]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring.

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

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [REDACTED]-month credit monitoring services, we recommend that you place an initial one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.



Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

September 16, 2024

VIA E-MAIL

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

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We represent the Cannon Corporation ("Cannon Design") located 50 Fountain Plaza, Suite 200 Buffalo, New York 14202, and we are writing to supplement our previous notification to your office in regard to an incident that may affect the security of certain personal information relating to Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Cannon Design does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 25, 2023, Cannon Design became aware of suspicious activity in their computer network. Upon learning of this activity, Cannon Design took prompt steps to confirm the security of their network and minimize any disruptions to their operations. Cannon Design launched an investigation to determine the nature and scope of the incident. They determined that an unauthorized third party gained access to certain parts of their network between January 19, 2023 and January 25, 2023. Following this determination, Cannon Design reviewed the information was contained in the impacted network to identify individuals whose information was impacted and reviewed internal Cannon Design records to identify address information for impacted individuals. That review was concluded on May 3, 2024. Cannon Design is notifying impacted individuals out of an abundance of caution because the investigation determined that certain information was accessed or acquired by the unauthorized third party.

The information that could have been subject to unauthorized access includes name, address, Social Security number, driver's license number or other government ID number, and individual taxpayer ID.

Notice to Maryland Residents

As previously reported, on or about August 19, 2024, Cannon Design provided written notice of this incident to three hundred twenty-five (325) Maryland residents. On or about September 16, 2024, Cannon Design provided written notice of this incident to one hundred seventy-five (175) Maryland residents. In total, five hundred (500) Maryland residents were notified of this event. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Cannon Design moved quickly to investigate and respond to the incident, assess the security of Cannon Design systems, and identify potentially affected individuals. Further, Cannon Design notified federal law enforcement regarding the event. Cannon Design is also working to implement additional safeguards and training to its employees. Cannon Design is providing access to credit monitoring services for twenty-four (24) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Cannon Design is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Cannon Design is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Cannon Design is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/kzm
Enclosure

EXHIBIT A

CANNONDESIGN

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

M0205-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



September 16, 2024

NOTICE OF SECURITY INCIDENT

Dear Sample A. Sample:

The Cannon Corporation (“Cannon Design”) writes to inform you of a recent cyber incident that impacts some of your information. While we do not have any indication that any identity theft or fraud related to your information has occurred as a result of this incident, this notice provides you with additional information about the incident, our response, and steps you may take to further protect your information against identity theft and fraud, should you determine it is appropriate to do so.

What Happened? On or about January 25, 2023, Cannon Design became aware of suspicious activity in our computer network. Upon learning of this activity, Cannon Design took prompt steps to confirm the security of our network and minimize any disruptions to our operations. We launched an investigation to determine the nature and scope of the incident. We determined that an unauthorized third party gained access to certain parts of our network between January 19, 2023 and January 25, 2023. Following this determination, we reviewed the information that was contained in the impacted network to identify individuals whose information was impacted and reviewed internal Cannon Design records to identify address information for impacted individuals. That review was concluded on May 3, 2024. Cannon Design is notifying you out of an abundance of caution because the investigation determined that certain information relating to you was accessed by the unauthorized third party.

What Information Was Involved? Our investigation identified the following types of personal information were accessed without authorization: your name and [Extra1]. Cannon Design is not aware of any attempted or actual misuse of your information.

What We Are Doing. Cannon Design takes this incident and the security of information within our care very seriously. Upon discovery of this incident, we immediately launched an in-depth investigation to determine the full nature and scope of this incident and moved quickly to assess the security of our email accounts and notify affected individuals. As part of our ongoing commitment to the privacy of information within our care, we are working to implement additional security measures to further protect against similar incidents in the future. We will also be notifying state regulators, as required.

As an added precaution, we would like to offer you twenty-four months of complimentary access to credit monitoring services through Experian. If you wish to receive these services, you must enroll by following the below enrollment instructions as we are unable to activate these services on your behalf.

B130546

0000001



M0205-L01

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your accounts statements and credit reports to detect errors or suspicious activity. You can find more information about obtaining a free copy of your credit report, protecting against potential identity theft and fraud, and other resources available to you in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also enroll in the complimentary credit monitoring services available to you; detailed instructions for enrolling in these services are enclosed.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please contact us at 833-918-4990 between 8 am – 8 pm CST (excluding major U.S. holidays) on Monday through Friday. Please be prepared to provide your engagement number B130546. You may also write to us at 50 Fountain Plaza, Suite 200 Buffalo, New York 14202.

Sincerely,

Cannon Design

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** December 31, 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 product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-4990 by December 31, 2024. Be prepared to provide engagement number B130546 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.

* 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.



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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, 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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft

should also be reported to law enforcement and your 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, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fera.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, you have the right to obtain any police report filed in regard to this incident. There are 26 Rhode Island residents impacted by this incident.

