ECKERT
SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

RECEIVED
DEC 05 2022
CONSUMER PROTECTION

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

December 2, 2022

VIA FIRST CLASS MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Data Security Incident

Dear Attorney General Formella:

This notice is provided on behalf of my client, CentiMark Corporation ("CentiMark"), following an incident that may have involved the names, dates of birth, Social Security numbers, driver's license numbers, and/or bank account and routing numbers of sixteen (16) New Hampshire residents. CentiMark is a commercial roofing company headquartered in Canonsburg, Pennsylvania. CentiMark will provide written notice to impacted individuals later today, via U.S. Mail. The notice letter includes general advice on how to protect one's identity and obtain free credit reports and security freezes, as well as instructions for enrolling in a one-year, complimentary membership with Experian for credit monitoring and identity theft services for those whose Social Security number and/or driver's license number was potentially involved. A copy of the notice letter is enclosed and additional details on the incident are below.

In August of 2022, CentiMark discovered and stopped a ransomware attack, in which an unauthorized third party accessed some of CentiMark's computer network. Thereafter, CentiMark began a prompt investigation of the incident with the assistance of legal counsel and a nationally recognized digital forensics firm. After working diligently to determine the nature and scope of the incident, the investigation revealed that there was intermittent unauthorized access to CentiMark's servers between August 7, 2022 and August 11, 2022. Through the investigation, CentiMark learned that it would be unable to determine what specific information the unauthorized third party viewed within or acquired from CentiMark's network. Therefore, CentiMark undertook a comprehensive review of all potentially impacted files in order to determine who may have been affected, what information may have been involved, and where those people reside. Beginning on October 20, 2022, CentiMark discovered that the potentially impacted files contained personal information belonging to New Hampshire residents.

Because cyber threats are always evolving, CentiMark is continuously working to identify and mitigate threats and evaluate its IT security protocols to protect sensitive data. To further enhance its security and help prevent similar occurrences in the future, CentiMark has taken, or will be taking, the following steps:

1. Increasing password complexity requirements and the frequency of password changes;
2. Adding multi-factor authentication for employee accounts; and

ECKERT
SEAMANS
ATTORNEYS AT LAW

3. Reviewing and strengthening our policies and procedures regarding data security.

In addition, consistent with compliance obligations and responsibilities, CentiMark is providing notice of this incident to appropriate state regulators.

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

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure

CENTIMARK

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

December 2, 2022

i6797-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 SSN_DL ONLY
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA SECURITY INCIDENT

Dear Sample A. Sample:

We are writing to tell you about a recent incident that may have involved unauthorized access to your personal information. CentiMark is a commercial roofing company headquartered in Canonsburg, Pennsylvania. We take this matter very seriously because we are committed to the privacy and security of all information in our possession. In an abundance of caution, we are providing this notice to inform you of the incident, offer complimentary identity monitoring services, and suggest ways that you can help protect your information, should you feel it necessary to do so.

What Happened

On August 11, 2022, CentiMark discovered and stopped a ransomware attack, in which an unauthorized third party accessed some of CentiMark's computer network. We immediately launched an investigation to determine the nature and scope of the unauthorized activity with the assistance of a nationally recognized digital forensics firm. Our investigation determined that there was intermittent unauthorized access to our servers between August 7, 2022 and August 11, 2022. Through the investigation, we learned that we would be unable to determine what specific information the unauthorized third party viewed within or acquired from our network. While we were unable to say definitively if your information was accessed or acquired by the unauthorized third party, we are notifying you of the incident in an abundance of caution.

What Information Was Involved

We found no evidence that personal information has been misused; however, it is possible that the following information about you could have been accessed by an unauthorized third party: first and last name, date of birth, Social Security number, and/or driver's license number.

What We Are Doing About It

As soon as we discovered the unauthorized activity, we worked quickly to secure our network and to investigate this incident. Our investigators also searched Dark Web sources and found no indication that any of our data had been released or offered for sale as a result of this incident. To further enhance our security and help prevent similar occurrences in the future, we have taken, or will be taking, the following steps:

1. Increasing password complexity requirements and the frequency of password changes;
2. Adding multi-factor authentication for employee accounts; and
3. Reviewing and strengthening our policies and procedures regarding data security.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state regulators.

What You Can Do

At this time, we are not aware of any misuse of your information. However, we recommend that you take the following preventative measures to help detect and mitigate any misuse of your information.

1. Enroll in a complimentary, [Extra1]-month membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to $1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.

2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

The privacy and security of your information is important to us, and we remain committed to protecting it. If you have any questions or concerns about this incident, you may call us toll-free at (888) 274-8110, Monday through Friday 9 AM – 11 PM EST, and Saturday and Sunday 11 AM – 8 PM EST. Be prepared to provide your engagement number:

Sincerely,

Greg Wilson
Chief Information Officer

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/ for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or

bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing ad

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 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.

Additional Helpful Information

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 at the information provided above.

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.

STATE SPECIFIC INFORMATION

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Toll-free: 1-888-743-0023

NEW MEXICO residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
http://www.dos.ny.gov/consumerprotection

New York Attorney General
1-800-771-7755
http://www.ag.ny.gov/home.html

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
Toll-free: 1-877-566-7226

RHODE ISLAND residents: There were 3 Rhode Island residents impacted by this incident. You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
Toll-free: 1-401-274-4400

VERMONT residents: You may obtain information about fighting identity theft, placing a security freeze and obtaining a free copy of your credit report from the Vermont Attorney General's Office website. If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, you may call the Vermont Attorney General's Office.

Office of the Attorney General
109 State St.
Montpelier, VT 05609
http://ago.vermont.gov/
Toll-free (VT only): 1-800-649-2424
1-802-828-3171

ADDITIONAL DETAILS REGARDING YOUR [Extra1]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by**: **March 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**:

If you have questions about the product, 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) 274-8110** by **March 31, 2023**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian. 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, Equifax and Transunion files 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(888) 274-8110**. 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 (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 this Identity Restoration support is available to you for [Extra1] 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. You will also find self-help tips and information about identity protection at this site.

* 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.