

STATE OF NH
DEPT OF JUST

2019 NOV 20 AM 11:46

Matthew H. Meade
Direct 412-566-6983
mmeade@eckertseamans.com

November 14, 2019

VIA FIRST CLASS MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

This notice is provided on behalf of my client Chester County, Pennsylvania ("County"), pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). The County recently learned that there may have been unauthorized access to some personally identifiable information maintained by the County, including information regarding one (1) New Hampshire resident. That information included name and Social Security number maintained in the County employees' business email accounts. As the result of its investigation, the County determined that information in five (5) County employee email accounts may have been impacted.

On August 29, 2019, the County learned that a large number of emails had been sent from a single County email account without authorization. As soon as the County learned about this incident, it launched an investigation to understand what happened and, more importantly, to prevent something like this from happening again. The County learned that its employees received emails that led to incidents of unauthorized access to a total of five (5) County email accounts that took place between August 3, 2019, and September 5, 2019. The investigation revealed that the email accounts were used by employees from the Chester County Youth Center, District Attorney's Office, Health Department, Department of Community Development, and the Coroner's Office.

As of the date of this letter, the County is not aware of any inappropriate use of the personal information involved. When the County discovered this incident, it immediately disabled the affected email accounts and had the users reset their passwords. The County scanned its email system to detect and neutralize any potentially dangerous emails or unauthorized activity. To further enhance email and network security and to help prevent similar occurrences in the future, the County has taken or will be taking the following steps:

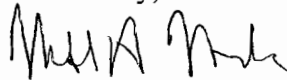
1. Closely monitoring and restricting outside access to its systems;
2. Increasing password complexity requirements;
3. Adding two factor authentication for remote access;
4. Strengthening its filtering to help block dangerous emails;
5. Updating its response procedures to more quickly and effectively respond to incidents;
6. Enhancing its cyber training and providing regular communications in order to increase cyber awareness; and
7. Regularly reviewing email boxes to remove or archive outdated information that the County no longer needs.

In addition, each affected individual will be offered one (1) year of identity theft protection services, at no cost.

The County notified one (1) New Hampshire resident via U.S. Mail on November 13, 2019. A copy of the notice sent to the affected New Hampshire resident is attached.

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

Sincerely,



Matthew H. Meade

MHM/
Enclosure



THE COUNTY OF CHESTER



COMMISSIONERS
Michelle Kichline
Kathi Cozzone
Terence Farrell

OFFICE OF THE COMMISSIONERS
313 W. Market Street
P.O. Box 2748
West Chester, PA 19380-0991
(610) 344-6100
www.chesco.org

November 13, 2019

[Name]
[Address]
[City, State, Zip]

NOTICE OF DATA SECURITY INCIDENT

Dear [Name]:

We are writing to tell you about a recent email incident that may have exposed personal information that you provided to Chester County to unauthorized access. As a result of our investigation, we determined that some personal information that we maintained about a small number of our residents and their families may have been accessed without authorization. We take this matter very seriously because we know how important your personal information is to you. **At this time, we have no indication that any of this personal information has been inappropriately used by anyone.** We are providing this notice to you as a precautionary measure, to inform you and to explain steps that you can take to protect your information.

What Happened

On August 29, 2019, we learned that a large number of emails had been sent from a single County email account without authorization. As soon as we learned about this, we launched an investigation to understand what happened and, more importantly, to prevent something like this from happening again. We learned that County employees received emails that led to incidents of unauthorized access to a total of 5 County email accounts between August 3, 2019 and September 5, 2019. Our investigation showed that the email accounts were used by employees from the Chester County Youth Center, District Attorney's Office, Health Department, Department of Community Development, and the Coroner's Office.

What Information Was Involved

On September 19, 2019, we first found out that personal information was contained in the email accounts. For this reason and because we could not identify what specific information was accessed, we reviewed the entire contents of each of the employees' email boxes to find out what was in each email, who may have been affected and where those people resided. That information may have included your name, address, date of birth, and Social Security or driver's license number. The specific information is dependent on the County department or office that you dealt with or that provided services to you.

What We Are Doing About It

When we discovered this incident, we immediately disabled the affected email accounts and had the users reset their passwords. We scanned our email system to detect and neutralize any potentially dangerous emails or unauthorized activity. To further enhance email and network security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Closely monitoring and restricting outside access to our systems;
2. Increasing password complexity requirements;
3. Adding two factor authentication for remote access;
4. Strengthening our filtering to help block dangerous emails;
5. Updating our response procedures to more quickly and effectively respond to incidents;
6. Enhancing our cyber training and providing regular communications in order to increase cyber awareness;
and
7. Regularly reviewing email boxes to remove or archive outdated information that we no longer need.

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

What You Can Do

Although we are not aware of any inappropriate use of your personal information, we are notifying you so that you can take steps to protect yourself. We recommend that you remain vigilant to the possibility of fraud and identify theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity. If you find any unauthorized or suspicious activity, you should contact local law enforcement.

We strongly encourage you to take the following preventative measures to help detect and mitigate any misuse of your information:

1. We are offering you a complimentary, one-year membership with Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please see the additional information provided in this letter.
2. Report any incidents of suspected identity theft to your local law enforcement and state Attorney General.

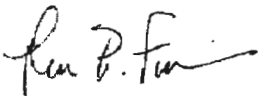
If you suspect unauthorized or suspicious activity, you can contact us and we recommend that you use the complimentary Identity Restoration service: www.ExperianIDWorks.com/restoration.

For More Information

If you have any questions or concerns about this incident, you may contact us by calling us at 1 800 692 1100 and press "O" between the hours of 8:30 a.m. and 4:30 p.m., Monday through Friday.

We sincerely apologize for any inconvenience and concern this incident has caused you. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Very truly yours,



Thomas P. Furman, CPCU
Privacy Officer

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the Federal Trade Commission 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. 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 P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com
--	---	--

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1 888 EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.

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. 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.

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 www.consumer.ftc.gov/articles/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 Georgia, New Jersey, and Puerto Rico 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 to obtain such additional report(s).

STATE SPECIFIC INFORMATION

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 27699-9001
www.ncdoj.gov
Toll-free: 1-877-566-7226

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH
EXPERIAN IDENTITYWORKS MEMBERSHIP:**

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

- Ensure that you **enroll by: January 28, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: [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 **877.890.9332** by **January 28, 2020**. Be prepared to provide engagement number **XXXXXX** 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 877.890.9332. 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 one year 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.