

# CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200  
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700  
Fax: (610) 567-0712

[www.C-WLAW.com](http://www.C-WLAW.com)

JOHN LOYAL  
[jloyal@c-wlaw.com](mailto:jloyal@c-wlaw.com)

JASON MICHAEL GOODWIN  
[jgoodwin@c-wlaw.com](mailto:jgoodwin@c-wlaw.com)

A Mid-Atlantic Litigation Firm

Visit us online at  
[www.C-WLAW.com](http://www.C-WLAW.com)

RECEIVED

JAN 19 2021

CONSUMER PROTECTION

January 8, 2021

**Via Mail**

Office of Attorney General  
33 Capitol Street  
Concord, New Hampshire 03302

***RE: Security Incident Notification***

To Whom It May Concern:

I serve as counsel for the County of Mercer ("Mercer"), and provide this notification to you of a recent data security incident suffered by Mercer. On or around September 6, 2019, Mercer County became aware of a potential compromise to one of its email accounts. Upon discovery, Mercer immediately took steps to secure the affected accounts, which included resetting the passwords required to access the affected employee email account and implementing additional email and network security measures. Further, Mercer promptly began investigating the incident, which included engaging a third-party expert forensics firm. It was ultimately determined that one email account experienced unauthorized access.

Upon confirmation of the unauthorized access to the Mercer employee email account, Mercer's third-party forensic experts immediately investigated whether the affected email account contained individuals' sensitive information. On December 23, 2019, after thorough investigation, Mercer learned that the unauthorized access may have allowed access to individuals' personal information. No residents of New Hampshire were identified at this time, nor was it believed that New Hampshire residents would be identified. On November 11, 2020, after further investigation, Mercer obtained additional address information for impacted individuals. At this time, Mercer learned that the potentially impacted data included information relating to one (1) resident of New Hampshire.

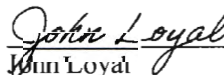
Mercer will be promptly notifying the affected individual on January 8, 2021 and is providing them with complimentary credit monitoring for one (1) year. A copy of the drafted notification letter is attached hereto. Mercer is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:

  
John Loyal



KELVIN S. GANGES  
Chief of Staff

**COUNTY OF MERCER**  
OFFICE OF THE COUNTY ADMINISTRATOR  
McDade Administration Building  
640 South Broad Street  
P.O. Box 8068  
Trenton, New Jersey 08650-8068

BRIAN M. HUGHES  
County Executive



LILLIAN L. NAZZARO, ESQ.  
County Administrator

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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

**RE: Important Security Notification. Please read this entire letter.**

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

We are writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information, as well as access to resources, so that you can better protect against the possibility of misuse of your personal information.

**What Happened:**

On September 6, 2020, Mercer County became aware of a potential compromise to one of its email accounts. Upon discovery, Mercer County immediately undertook a thorough investigation, with the assistance of an independent expert forensic company to analyze County systems. It was ultimately determined that one account was subject to unauthorized access, which may have allowed access to your personal information. Mercer County immediately contacted law enforcement and worked with prosecutors, the FBI and local police. The unauthorized actors have since been detained and prosecuted by the United States Attorney's Office.

While we have no information to suggest that any information was misused during this incident, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your accounts. We take great care in the security of our technology systems, and regret that this incident has occurred.

**What Information Was Involved:**

The personal information that could have been accessed by the unauthorized individual may have included your first and last name in combination with one or more of the following data elements: Social Security number, tax identification number, date of birth, passport number, driver's license number, financial account number, routing number, username and password, mother's maiden name, marriage certificate, digital signature, medical diagnosis, treatment information, medical history, medical record number and/or health insurance information.

**What We are Doing:**

Mercer County has taken every step necessary to address the incident, and is committed to fully safeguarding all of the information that you have entrusted to us. Upon learning of this incident, we immediately took actionable steps to secure the affected account, which includes implementing additional security measures. We likewise retained a forensic firm to conduct a thorough investigation.

**Credit Monitoring:**

As a safeguard, we have arranged for you to activate, at no cost to you, in identity monitoring services for one year provided by Kroll, a data breach and recovery services expert. Due to privacy laws, we cannot activate you directly. Additional information regarding how to activate the complimentary identity monitoring service is enclosed.

**What You Can Do:**

In addition to activating the complimentary identity monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

**For More Information:**

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-833-971-3309  
8:00 am to 5:30 pm Central Time, Monday through Friday excluding major US holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "Lillian L. Nazzaro". The signature is fluid and cursive, with the first name being the most prominent.

Lillian L. Nazzaro, Esq.  
Mercer County Administrator

## ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

**Kroll provides you with the following features:**

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

### **How to Activate: You can sign up online.**

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your complimentary identity monitoring services.

You have until **April 6, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

If you have questions, please call 1-833-971-3309, Monday through Friday from 8:00 am to 5:30 pm Central Time.

Due to privacy laws, we cannot activate you directly. Activating this service will not affect your credit score. Activation is available online only as no offline options are available at this time.

### **PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE**

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

#### **TransUnion**

Fraud Victim Assistance Dept.  
P.O. Box 6790  
Fullerton, CA 92834  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

#### **Experian**

National Consumer Assistance  
P.O. Box 1017  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **Equifax**

Consumer Fraud Division  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

### **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security 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 security freeze on your credit report. The process to place a security freeze requires that you directly contact each of the credit reporting companies. You can do so online or through the mail. The necessary types of information include your full name, social security number, date of birth, current address, all addresses where you have lived during the last two years, email address, a copy of a utility bill, bank or insurance statement and a copy of a government-issued id card, such as a driver's license or state id card.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. 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.

## **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

## **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

## **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

## **RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)**

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [https://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](https://files.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

## **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at <http://www.annualcreditreport.com>. Under Rhode Island and Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).
- **For New York residents**, you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection/>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).
- **For Rhode Island Residents**, the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov> or 401-274-4400.