

# CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL  
jloyal@c-wlaw.com

JORDAN MORGAN  
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200  
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at  
www.C-WLAW.com

January 3, 2022

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

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

***RE: Security Breach Notification***

To Whom It May Concern:

I serve as counsel for D'Aurizio Law Offices, PLLC ("D'Aurizio"), located at 1780 East Ridge Road, Rochester, NY 14622, and provide this notification to you of a recent data security incident. By providing this notice, D'Aurizio does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On September 8, 2021, D'Aurizio became aware of a potential compromise to an email account belonging to an employee. Upon discovery, D'Aurizio immediately performed a password reset for the affected account and swiftly engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. Following a full and thorough investigation, it was confirmed that only one employee email account was subject to unauthorized access during this incident. Upon confirmation of the unauthorized access to the employee email account, D'Aurizio immediately investigated whether the affected email accounts contained individuals' sensitive information. On December 17, 2021, following a thorough investigation, D'Aurizio confirmed that a limited amount of personal information may have been accessed in connection with this incident.

At this time, D'Aurizio is aware of one (1) resident of Maryland who may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional Maryland residents are potentially affected.

D'Aurizio will promptly mail notification letters to the impacted individuals on January 3, 2022, and will offer the affected Maryland resident complimentary credit monitoring for twelve

(12) months. A copy of the draft notification letter is attached as ***Exhibit A***. The letter outlines the incident and provides potentially affected individuals with additional resources to protect their identity and monitor their credit history and personal accounts. As the letter indicates, D'Aurizio is offering credit monitoring services at D'Aurizio's expense. D'Aurizio is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal  
John Loyal, Esq.

## EXHIBIT A

<<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 a data security incident experienced by D'Aurizio Law Offices, PLLC ("D'Aurizio") that may have involved your information described below.

D'Aurizio takes the privacy and security of all information very seriously. While we have no evidence to suggest that any information was viewed or misused during this incident, it is crucial that we be as supportive and transparent as possible. That is why we are writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary identity monitoring services that we are offering.

**What Happened:**

On September 8, 2021, D'Aurizio became aware of a potential compromise to an email account belonging to an employee. Upon discovery, D'Aurizio immediately performed a password reset for the affected account and swiftly engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. Following a full and thorough investigation, it was confirmed that only one employee email account was subject to unauthorized access during this incident. Upon confirmation of the unauthorized access to the employee email account, D'Aurizio immediately investigated whether the affected email accounts contained individuals' sensitive information. On December 17, 2021, following a thorough investigation, D'Aurizio confirmed that a limited amount of personal information may have been accessed in connection with this incident.

Although the forensic investigation could not rule out the possibility that an unknown third-party actor may have accessed this information, there is no indication whatsoever that any information has been subject to attempted or actual misuse. However, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your information and your resources. We take great care in the security of our technology systems and regret that this incident has occurred.

**What Information Was Involved:**

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been viewed or misused. The personal information that could have been accessed by the unauthorized individual(s) may have included your first and last name, in combination with your <<b2b\_text\_1(data elements)>>.

**What We Are Doing:**

D'Aurizio has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Unfortunately, network intrusions have become more common and this incident is similar to those experienced by other companies across the country. Upon learning of this incident, we immediately secured the affected account, reset passwords, and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future. We retained a third-party forensic firm to conduct a thorough investigation and are offering you complimentary identity monitoring services.

**Identity Monitoring Services:**

As a safeguard, we have arranged for you to activate, at no cost to you, online identity monitoring service for 12 months. Due to privacy laws, we cannot register you directly. Additional information regarding how to activate the complimentary identity monitoring services is enclosed.

**What You Can Do:**

Sign up for Identity Monitoring Services – We encourage you to contact Kroll with any questions and to activate your free identity monitoring services at <https://enroll.krollmonitoring.com>, use your membership number, <<Membership Number s\_n>>, and follow the steps to receive your identity monitoring service online within minutes. Please note the deadline to activate is <<b2b\_text\_6(activation deadline)>>.

In addition to activating the complimentary identity monitoring services 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 any of your accounts, please promptly change your password and take additional steps to help protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. 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 (855) 618-3158, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. holidays) or write us at 1780 East Ridge Road, Rochester, NY 14622.

D'Aurizio has no relationship more important or more meaningful than the one we share with you. We wish to apologize for any worry or inconvenience that this incident may cause you or your family.

Sincerely,

*John F. D'Aurizio*

John D'Aurizio, Esquire  
D'Aurizio Law Offices, PLLC

## ADDITIONAL STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Activate Identity Monitoring

Visit <<Membership Number s\_n>> to activate and take advantage of your identity monitoring services.

*You have until <<b2b\_text\_6(activation deadline)>> to activate your identity monitoring services.*

Membership Number: <<Membership Number s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.



### TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

#### 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.

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.

#### Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

|                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TransUnion</b><br>1-800-680-7289<br><a href="http://www.transunion.com">www.transunion.com</a><br><br><b>TransUnion Fraud Alert</b><br>P.O. Box 2000<br>Chester, PA 19016-2000<br><br><b>TransUnion Credit Freeze</b><br>P.O. Box 160<br>Woodlyn, PA 19094 | <b>Experian</b><br>1-888-397-3742<br><a href="http://www.experian.com">www.experian.com</a><br><br><b>Experian Fraud Alert</b><br>P.O. Box 9554<br>Allen, TX 75013<br><br><b>Experian Credit Freeze</b><br>P.O. Box 9554<br>Allen, TX 75013 | <b>Equifax</b><br>1-888-298-0045<br><a href="http://www.equifax.com">www.equifax.com</a><br><br><b>Equifax Fraud Alert</b><br>P.O. Box 105069<br>Atlanta, GA 30348-5069<br><br><b>Equifax Credit Freeze</b><br>P.O. Box 105788<br>Atlanta, GA 30348-5788 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to help protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

*For Maryland residents*, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us).

*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: (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 employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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, FTC, 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](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and [www.riag.ri.gov](http://www.riag.ri.gov). Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

*For Washington, D.C. residents*, the District of Columbia Attorney General may be contacted at 441 4<sup>th</sup> Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.