

BakerHostetler

Baker&Hostetler LLP

One North Wacker Drive
Suite 4500
Chicago, IL 60606-2841

T 312.416.6200
F 312.416.6201
www.bakerlaw.com

Aleksandra M. Vold
direct dial: 312.416.6249
avold@bakerlaw.com

April 10, 2020

VIA EMAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon MacDonald
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Confidio, LLC (“Confidio”), to notify you of a security incident involving two New Hampshire residents.¹ Confidio is a pharmacy benefits consulting firm hired by organizations to provide pharmacy solutions and consulting services. Confidio is located in Towson, Maryland and is a business associate as defined by the Health Insurance Portability and Accountability Act (“HIPAA”).

Confidio’s ongoing investigation into an email incident recently determined that an unauthorized person obtained access to a Confidio employee’s email account between November 29, 2019 and December 12, 2019, and during that time may have downloaded emails and attachments in the account. Upon first learning of the incident, Confidio immediately secured the employee’s email account, launched an investigation to determine the nature and scope of the incident, and a computer security firm was engaged to assist. The investigation was unable to determine which emails and/or attachments were viewed or acquired by the unauthorized person, if any. Confidio therefore reviewed the full contents of the account for personal information.

From that review, Confidio identified information relating to some of its clients’ current and/or former employees and their dependents. Confidio received this information in connection with the pharmacy solutions and consulting services it provides. Accordingly, on February 10, 2020 and March 31, 2020, pursuant to HIPAA and N.H. Rev. Stat. § 359-C:20(c), Confidio notified its clients of the incident. Beginning April 10, 2020, Confidio is providing notice to two

¹ This notice does not waive Confidio’s objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this incident.

Attorney General MacDonald

April 10, 2020

Page 2

New Hampshire residents² whose names and Social Security numbers were identified in the email account.

The New Hampshire residents are being notified in substantially the same form as the enclosed letter via U.S. First-Class mail in accordance with HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*) and N.H. Rev. Stat. § 359-C:20(a). Confidio is offering the individuals a complimentary, one-year membership to credit monitoring and identity theft protection services. Confidio has also established a dedicated, toll-free call center where individuals may obtain more information regarding the incident.

To help prevent a similar incident in the future, Confidio is implementing additional procedures to further expand and strengthen its security processes, and is providing additional education and training to its employees about how to identify and avoid suspicious emails.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read 'A. Vold', written in a cursive style.

Aleksandra M. Vold

Enclosure

² Confidio is notifying the New Hampshire residents on behalf of its client, Environmental Air Systems, LLC.



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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Confidio, LLC is a pharmacy benefits consulting firm hired by organizations to provide pharmacy solutions and consulting services. To accomplish this function, we receive necessary data about employees and dependents, including certain types of personal information. We place a high value on maintaining the integrity and security of the data we hold for our clients. Regrettably, we write to inform you that we recently identified and addressed a security incident that may have involved some of your information, which was provided to us in connection with the services we provide to <<ClientDef1(EntityName)>>. This notice describes the incident, outlines the measures we have taken in response, and provides steps you can take.

On February 10, 2020, we notified <<ClientDef1(EntityName)>> that we had identified suspicious activity within one of our employee's email accounts on December 12, 2019. We immediately secured the account, launched an investigation to determine the nature and scope of the incident, and a computer security firm was engaged to assist. On January 17, 2020, the investigation determined that an unauthorized person accessed the employee's account between November 29, 2019 and December 12, 2019, and during that time may have downloaded emails and attachments in the account. The investigation was unable to determine which emails and/or attachments were viewed or acquired by the unauthorized person, if any. We therefore reviewed the full contents of the account for personal information and determined that an email or an attachment contained your information, including your name, date of birth, Social Security number, prescription information, health insurance information, and/or clinical or treatment information, such as provider name or diagnosis.

To date, we have no indication that any of the information contained in the account was actually viewed or acquired by the unauthorized individual, or that it has been misused. However, we wanted to notify you of this incident to assure you we take this very seriously. As an added precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [https://\[IDMonitoringURL\]](https://[IDMonitoringURL]) to activate and take advantage of your identity monitoring services.

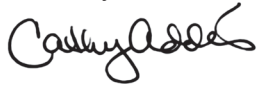
You have until *[Date]* to activate your identity monitoring services.

Membership Number: <<Member ID>>

For more information on safeguarding your identity, and on your complimentary services, please see the additional information provided in this letter. We also recommend that you review the billing statements or notifications of prescriptions ordered or filled that you receive from your mail and retail pharmacies or your healthcare providers. If you see charges for services or prescriptions you did not receive, please contact the provider or the Pharmacy Benefit Manager at the phone number on your prescription ID card immediately.

We regret any concern or inconvenience this incident may cause you. To help prevent a similar occurrence in the future, we are implementing additional procedures to further expand and strengthen our security processes, and are providing additional education and training to our employees about how to identify and avoid suspicious emails. If you have any questions, please call us at [1-800-833-3333](tel:1-800-833-3333), Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Cathy Addis". The signature is fluid and cursive, with a large initial "C" and a long, sweeping tail.

Cathy Addis
Vice President, Compliance

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because

¹ 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.

most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: Confidio, LLC is located at 502 Washington Avenue, Suite 450, Towson, MD 21204 and can be reached at 443-767-7200. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: 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>; *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: <<ClientDef2(RI Statement)>> Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.