

BakerHostetler

RECEIVED

AUG 05 2019

CONSUMER PROTECTION
Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

August 1, 2019

VIA OVERNIGHT MAIL

Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: *Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, Covia Holdings Corporation (“Covia”), to notify your office of a security incident involving one New Hampshire resident.¹

On June 14, 2019, Covia determined that an email or an attachment that could have been viewed by an unauthorized person, due to a phishing email incident, contained personal information of a New Hampshire resident. Covia identified the underlying phishing incident involving certain Covia employee’s email accounts and immediately took steps to secure the email accounts involved and then began an investigation. A leading forensic firm was engaged to assist in the investigation. The investigation determined that unauthorized access to certain Covia employees’ accounts occurred at times that varied by account over the course of four days (April 12-15, 2019).

Covia undertook a review of the accounts to determine what personal information each contained. Since receiving the initial results of that review on June 14, 2019, Covia has been working to identify contact information for each of the individuals with personal information involved. Although those efforts remain ongoing, today, August 1, 2019, Covia is notifying one New Hampshire resident that their personal information, including their name and Social Security number, was found in one of the accounts that was accessed.

Covia is providing notice to these individuals via United States First Class Mail in accordance with N.H. Rev. Stat. § 359-C:20. A sample copy of the notification letter is attached. Covia is providing the New Hampshire resident with one year of complimentary credit monitoring

¹ This report is not a waiver of any objection that New Hampshire lacks personal jurisdiction over Covia.

Office of the Attorney General

August 1, 2019

Page 2

and identity theft protection services through Experian. Covia has also made a dedicated call center available to answer questions from the individuals with personal information involved.

As Covia identifies contact information for all of the individuals with personal information involved, Covia will promptly notify those individuals.

To help prevent something like this from happening in the future, Covia has taken, and continues to take, steps to further enhance its security measures, including further configuration changes for multi-factor authentication for remote email access that was previously implemented.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "Craig A. Hoffman", with a long horizontal flourish extending to the right.

Craig A. Hoffman
Partner

Enclosure



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

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

Covia Holdings Corporation (“Covia”) understands the importance of protecting the personal information that we maintain. We are writing to inform you that we recently identified and resolved an incident that may involve some of your information. This notice explains the incident, measures that we have taken and some steps that you can take in response.

We detected a phishing email incident in April 2019 that involved an unauthorized person gaining access to certain Covia employees’ email accounts. As soon as we learned about the incident, we immediately secured the employees’ email accounts and began an investigation. A leading forensic firm was engaged to assist our investigation. The investigation determined that unauthorized access to certain Covia employees’ accounts occurred at times that varied by account over the course of four days (April 12-15, 2019).

The investigation did not determine whether any specific emails or attachments may have been viewed by the unauthorized person. Therefore, we reviewed each account to determine what personal information each contained. On June 14, 2019, we determined that one of the accounts contained an email or an attachment with your << b2b_text_3>>. While we don’t know if your information was accessed or viewed by the unauthorized person, we wanted to make you aware of this incident and provide you with information on steps you can take in response.

We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. As a precaution, we are offering you a complimentary one-year membership with Experian’s® IdentityWorksSM. This product helps detect the possible misuse of your personal information and provides you with identity protection support. **For more information on IdentityWorksSM, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take, please see the additional information provided in this letter.**

We sincerely regret that this incident occurred and apologize for any inconvenience or concern. To help prevent something like this from happening in the future, we have taken, and continue to take, steps to further enhance our security measures, including further configuration changes for multi-factor authentication for remote email access that was previously implemented. If you have any questions about this matter, please call 1-833-389-2398, Monday through Friday between 9:00 am and 6:30 pm Eastern Time.

Sincerely,

Brian J. Richardson
Executive Vice President and
Chief Administrative Officer

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_1>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Member ID>>

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 877-288-8057. Be prepared to provide engagement number <<b2b_text_2>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS TO TAKE

Regardless of whether you choose to take advantage of this complementary credit monitoring, 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

If you are a resident of Maryland or North Carolina, 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
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of 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 below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 (1) 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

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). Here is a summary of your major rights under FCRA. 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.