

May 23, 2024

VIA E-MAIL (Idtheft@oag.state.md.us)

The Honorable Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Data Security Incident

Dear Attorney General Brown:

We are writing pursuant to Md. Code Ann., Com. Law § 14-3501 because Columbia Pipe & Supply Co. ("CPS") has learned of a data security incident that may have affected the personal information of two (2) Maryland residents. The information for these two individuals that was involved in the incident includes name, address, and social security number.

The incident occurred during the overnight period from February 29 to March 1, 2024, and certain files were copied from CPS's network by unauthorized actors. CPS immediately launched a comprehensive investigation into the nature and scope of the activity that included retaining an independent forensic investigation consulting team. All affected systems were disconnected and isolated and there is no indication of any continued unauthorized access or activity in our systems or any affiliated systems.

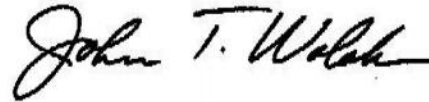
CPS also engaged a leading e-discovery firm to complete a thorough analysis and review of the files that were copied to determine the specific information that may have been impacted in the incident. That comprehensive review and analysis was recently completed and CPS moved promptly to inform these affected Maryland residents of this data security incident by sending a notification letter to each of these residents via the United States Postal Service on May 20, 2024. The letter included an offer of complementary credit monitoring services for 12 months.

GIBBONS P.C.

The Honorable Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
May 23, 2024
Page 2

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

Very truly,

A handwritten signature in black ink, reading "John T. Wolak". The signature is written in a cursive style with a large, stylized "J" and a long, sweeping underline.

John T. Wolak

DRAFT

GIBBONS P.C.

The Honorable Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
May 23, 2024
Page 3

[ATTACHMENT OF MD NOTICE]

DRAFT



COLUMBIA PIPE & SUPPLY CO.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

NOTICE OF DATA SECURITY INCIDENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing because Columbia Pipe & Supply Co. ("CPS") recently identified a data security incident that may involve some of your personal information. We are notifying you at this time to make you aware of this security incident so you can understand what happened, what we are doing to address it, and the steps you can take to remain vigilant and enhance the protection of your personal information, including activating complimentary identity monitoring services.

What Happened

On March 1, 2024, we identified unusual activity involving certain systems within CPS's network. Our IT Team immediately launched a comprehensive investigation into the nature and scope of the activity that included retaining an independent forensic investigation consulting team. All affected systems were disconnected and isolated and there is no indication of any continued unauthorized access or activity in our systems or any affiliated systems.

What Information Was Involved

As part of our investigation, we determined that during the overnight period from February 29 to March 1, 2024, certain files were copied from CPS's network as part of this incident by unauthorized actors. As a result, we have engaged a leading e-discovery firm to complete a thorough analysis and review of the files that were copied to determine the specific information that may have been impacted in the incident. That comprehensive review and analysis was recently completed and indicates that the files that were exposed contain the following types of personal information: t2b_text_1(Name, Impacted Data)>>

What We Are Doing

As noted above, there is no indication of any continued unauthorized access or activity in our systems or any affiliated systems. As part of our ongoing efforts to help prevent something like this from happening in the future, CPS has implemented several changes that will further harden our environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms to protect data from any subsequent incidents. In addition, we are working to identify vulnerabilities in our systems and implement appropriate remedial action.

What You Can Do, and For More Information

Because we take our obligation to safeguard your personal data very seriously and are sorry for any inconvenience or concern this has caused, CPS is offering you complimentary identity monitoring services. We encourage you to activate these complimentary services.

As an ongoing best practice, we recommend you remain vigilant, including carefully reviewing account statements and credit reports. Out of an abundance of caution, you may wish to change your username, password, and/or security questions relevant to your financial accounts and other personal accounts. Please also review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including

recommendations by the Federal Trade Commission regarding identity theft protection, details on how to place a fraud alert or a security freeze on your credit file, and other identity theft prevention and mitigation tools and services.

Identity Monitoring.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. 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, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

- Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.
- You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.
- Membership Number: <<Membership Number s_n>>

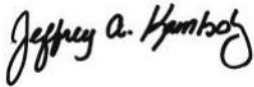
We recommend that you activate your complimentary identity monitoring services. Additional information describing your services is included with this letter.

Finally, in the event there is any suspicious activity in any of your accounts or you suspect you are the victim of identity theft, you should promptly notify the financial institution where the account is maintained and report the activity to the proper law enforcement authorities.

Your trust in CPS is of paramount importance to us. We deeply regret that this incident occurred.

If you have questions, please call 1-757-223-6197, Monday through Friday from 9:00 a.m. to 5:00: p.m. Eastern Time.

Very truly yours,



Jeffrey Kamholz
Area Manager



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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.