



Suite 2800, 1100 Peachtree Street NE
Atlanta, GA 30309-4528
t 404 815 6500 f 404 815 6555

September 13, 2023

direct dial 404 685 6713
direct fax 404 541 3205
VZeltser@kilpatricktownsend.com

Via U.S. Mail

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

Re: Notice of Breach of Security and Unauthorized Access of Taxpayer Information

Dear Attorney General Brown:

We represent Viventium Software, Inc. (“Viventium”), a payroll processor, which recently learned of a breach of security affecting four (4) Maryland residents. The incident occurred when either the Maryland residents or their employers’ payroll administrators inadvertently disclosed their Viventium account login credentials to unauthorized third parties online.

Cyber criminals set up a series of websites impersonating a Viventium login page but entirely unrelated to Viventium, and purchased search engine advertisement services that were linked to these impersonated websites. As a result, some Internet search results for the term “Viventium” presented advertisements directing individuals to the malicious websites at the top of the search results, and individuals who clicked on the link presented in the advertisements were directed to a website impersonating Viventium. Individuals who entered their login credentials in such a website were, in fact, providing their Viventium login credentials to unknown third parties.

Through this scheme, between approximately June 8 and June 14, 2023, cyber criminals may have had access to information that included the affected Maryland residents’ first and last names, dates of birth, addresses, email addresses, Social Security Numbers, banking information associated with their direct deposit, and payroll information. The cyber criminals may have changed direct deposit information to redirect one or more of the affected Maryland residents’ pay to an account the cyber criminals controlled.

Viventium took immediate steps to secure affected accounts by forcing a change of password, reviewing for any fraudulent activity associated with the account, mandating multi-factor authentication, if it was not already enabled, and taking other technical measures to secure the account and the Viventium systems. Viventium investigated and reversed known or suspected fraudulent direct deposit account changes. Viventium reported this incident to the FBI and

September 13, 2023

Page 2

consulted with them to confirm that Viventium has taken the recommended steps to protect consumer data against evolving cyber criminal activity.

Viventium is offering affected consumers free credit monitoring and related services, as more fully explained in the enclosed template consumer notice. The consumer notice is to be distributed to recipients in the days following the dispatch of this letter.

An independent forensics firm assisted Viventium with its investigation and confirmed Viventium's findings and conclusions in connection with this incident.

Please contact the undersigned at the above address, telephone number, or e-mail should you require any additional information regarding this incident.

Best regards,



Vita E. Zeltser

Enclosure

cc: Julieann Esper Rainville, CEO, Viventium Software, Inc.



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 13, 2023



K0013-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 EMPLOYEES - ALL STATES
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to alert you that your Viventium account information may have been accessed by unauthorized individuals when you or your employer's payroll administrator inadvertently provided Viventium account access to malicious actors online. We have taken steps to secure your account and information as detailed below and are notifying you out of an abundance of caution.

What Happened?

Cyber criminals set up a series of websites impersonating a Viventium login page but entirely unrelated to Viventium. This activity is a part of a vast sophisticated scam involving cyber criminals impersonating numerous brands and financial institutions, as discussed in the public service announcement from the FBI referenced in the For More Information section below. The cyber criminals purchased search engine advertisement services that were linked to these impersonated websites. As a result, some Internet search results for the term "Viventium" presented advertisements directing individuals to the malicious websites at the top of the search results, and individuals who clicked on the link presented in the advertisements were directed to a website impersonating Viventium. Individuals who entered their login credentials in such a website were, in fact, providing their Viventium login credentials to unknown third parties.

We suspect that you or your employer's payroll administrator may have inadvertently provided a Viventium account username and password to cyber criminals in this manner around June 8-14, and the cyber criminals then used your or your employer's payroll administrator's credentials to access your Viventium account information.

What Information Was Involved?

The cyber criminals obtained your or your employer's payroll administrator's Viventium account username and password that you or the payroll administrator may have inadvertently entered into a website impersonating Viventium.

The cyber criminals may have had access to information that included your first and last name, date of birth, address, email address, Social Security Number, banking information associated with your direct deposit, and payroll information, although we have no direct evidence that such data was actually viewed. The cyber criminals may have changed your direct deposit information to redirect your pay to an account they controlled.

What We Are Doing.

We took immediate steps to secure your or your employer's payroll administrator's account by forcing a change of password, reviewing for any fraudulent activity associated with the account, mandating multi-factor authentication, if it was not already enabled, and taking other technical measures to secure the account and our systems. We investigated and reversed known or suspected fraudulent direct deposit account changes. We have

0000001



reported this incident to the FBI and have consulted with them to confirm that we are taking the recommended steps to protect your data against evolving cyber criminal activity. Law enforcement did not request that our notifications of this incident be delayed.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9297 by November 30, 2023. Be prepared to provide engagement number B103175 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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.

What You Can Do.

Please immediately report any suspicious activity in your payroll account to your payroll administrator.

Please ensure that you only access the Viventium website by typing in our official URL, www.viventium.com, into your web browser address bar, or by using your previously bookmarked link to our official website. We also strongly encourage you to take the steps recommended by the FBI in the public service announcement referenced below to protect yourself online:

- Before clicking on an advertisement, check the URL to make sure the site is authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.

- Rather than search for a business or financial institution, type the business's URL into an internet browser's address bar to access the official website directly.
- Use an ad blocking extension when performing internet searches. Most internet browsers allow a user to add extensions, including extensions that block advertisements. These ad blockers can be turned on and off within a browser to permit advertisements on certain websites while blocking advertisements on others.

For More Information

You can learn more about how to protect yourself from the FBI's December 21, 2022 Public Service Announcement, *Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users*, <https://www.ic3.gov/Media/Y2022/PSA221221>. Please also review the enclosed Information About Identity Theft Prevention.

We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 877-890-9297 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B103175.

Thank you for partnering with us to keep your data secure.

Sincerely,



Julieann Esper Rainville, CEO
Viventium Software, Inc.
400 Connell Drive, Suite 1000
Berkeley Heights, NJ 07922

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Information About Identity Theft Prevention

We recommend that you regularly review statements from your credit card accounts and other accounts and periodically obtain your credit reports from the national consumer credit reporting agencies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national consumer credit reporting agencies listed below:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com

Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com

When you receive your credit reports from the above consumer credit reporting agencies, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information such as a home address or Social Security Number that is not accurate. If you see anything you do not understand, call the consumer credit reporting agency at the telephone number on the report.

We recommend you remain vigilant in reviewing your account statements and monitoring your free credit reports to detect errors which may result from this incident and for instances of fraud and identity theft, and promptly report any fraud, suspicious activity or suspected identity theft to your credit card company/bank, the proper law enforcement authorities, including local law enforcement, your state's Attorney General and/or the Federal Trade Commission ("FTC"). You may contact the FTC and your state's regulatory authority to obtain additional information about the steps you can take to avoid identity theft. To contact the FTC, write to the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, call 1-877-IDTHEFT (438-4338), or visit their website, www.ftc.gov/idtheft.

For Maryland residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx>.

For North Carolina residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For Oregon residents: You may report suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Fraud Alerts: There are two types of fraud alerts that 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 at least one year. You may have an extended alert placed on your credit report with the appropriate documentary proof if you have previously been a victim of identity theft. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national consumer credit reporting agencies listed above. You can obtain additional information about fraud alerts from the consumer credit reporting agencies and the FTC at the contact information listed above.

Credit Freezes / Security Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file by registering with each of the three consumer credit reporting agencies listed above. A credit freeze is a free tool that lets you restrict access to your credit report, which make it more difficult for identity thieves to open a new account in your name. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each consumer credit reporting agency. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password which you will need to lift the freeze. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. It is free to lift the freeze and free to place it again when you're done accessing your credit. You can obtain additional information about credit freezes from the consumer credit reporting agencies and the FTC at the contact information listed above. To request a credit freeze, you will need to provide the following information (note, some requirements differ for each of the three credit bureaus): your full name, including middle initial and any suffix; current address; former address; telephone numbers; Social Security Number; and date of birth. Additionally, some credit bureaus may require your maiden name or other last name, and driver's license number, and specify that former addresses are required for the past two years. Credit bureaus may also request copies of supporting documents, such as those proving your identity, Social Security Number and address. These documents may include, for example, a copy of a government-issued identification card, such as a driver's license or state identification card, a copy of a utility bill or bank statement showing your address, and a copy of your Social Security card, pay stub with your Social Security Number, or IRS form W2 that includes your Social Security Number.