



Frantz Ward LLP | 200 Public Square, Suite 3000 | Cleveland, OH 44114
Phone (216) 515-1660 | Fax (216) 515-1650 | FrantzWard.com

Bradley D. Reed | Direct: (216) 515-1662 | breed@frantzward.com

May 5, 2023

VIA EMAIL ldtheft@oag.state.md.us

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

RE: 7Signal Security Breach Incident

To whom it may concern,

Please be advised that the undersigned and this firm represent 7SIGNAL, Inc. ("7Signal") in connection with a security incident that occurred on April 5, 2023.

On behalf of 7Signal, we are writing to inform you of a data breach that occurred on April 5, 2023. The target of the unauthorized access was the company's Zenefits payroll and human resources system. The threat actor accessed the accounts of three employees and altered bank account information. 7Signal took immediate steps to disable access to the system and restore the account information of the affected individuals before any money could be sent to the redirected accounts. Additional information regarding the categories of personal information potentially exposed and steps the company is taking to restore the integrity of the system can be found in the attached notification letter.

One Maryland resident was potentially affected by this unauthorized access. 7Signal is in the process of preparing to notify that resident in compliance with the applicable Maryland laws and regulations. Please find attached a copy of the notification letter that will be sent via mail to the Maryland resident on May 8, 2023.

If you have any further questions or requests related to this incident, please do not hesitate to contact me. 7Signal remains committed to responding as appropriate and consistent with its legal obligations to this incident.

Sincerely,

Bradley D. Reed

Bradley D. Reed

BDR/slr
Enclosure



7SIGNAL, Inc.
6155 Rockside Road, Suite 110
Independence, Ohio 44131

May 2, 2023

Dear 7SIGNAL Community,

We want to make you aware of a recent security incident at 7SIGNAL.

What Happened

On Wednesday, April 5, 2023, 7SIGNAL became aware that an employee's bank information had been changed in Zenefits, 7SIGNAL's payroll and human resources information System, without the employee's authorization.

7SIGNAL promptly contacted Zenefits and determined that a 7SIGNAL Zenefits account login had been compromised, thus allowing an unauthorized third-party access into the 7SIGNAL Zenefits system. Upon further investigation by 7SIGNAL, we determined that an unidentified third-party threat actor did in fact access our Zenefits system. and as a result, three employees had their bank account information changed in the system. Fortunately, we learned of the incident prior to any funds being sent to the modified bank accounts. We immediately took steps to disable access to the Zenefits system through the compromised account and to prevent further access by updating and changing the compromised credentials.

While only three employees had their bank account information changed, you are receiving this notice because your personal identifying information as described in detail below was included in the compromised system and potentially accessed by an unauthorized third-party. If your bank account information was modified, you would have already been contacted by us.

What Information Was Involved

The personal identifying information in the Zenefits system included: first and last name, date of birth, social security number, current and previous addresses, email addresses, and banking and financial information., including account numbers. We have no indication that any data or information was removed from the Zenefits system, however, it is possible that the unauthorized third-party had access to view and copy this information.

We take the security of our employees' personal information very seriously. While we have been assured through our investigation and correspondence with Zenefits that only three employees' financial information was changed and that the unauthorized third party no longer has access to our system, we understand the significance of this issue to you.

What We Are Doing

We thank you for your understanding as we work to ensure that the appropriate steps are being taken to further safeguard your information and ensure that it used only in accordance with 7SIGNAL's privacy and security practices. Upon learning of the incident, we took immediate steps to resolve the incident and prevent access through the compromised user's account. We also contacted the three employees who



7SIGNAL, Inc.
6155 Rockside Road, Suite 110
Independence, Ohio 44131

were directly involved and notified all current employees that they needed to change their Zenefits passwords, update their MFA credentials, and confirm their bank account information was corrected.

7SIGNAL also initiated a review of its other systems and IT infrastructure to help ensure that there was no continuing risk of unauthorized access to the Zenefits system. 7SIGNAL is also reviewing its security procedures and policies as part of its ongoing efforts to seek to prevent similar incidents going forward.

We are in the process of notifying the appropriate and required authorities in accordance with applicable state laws. But at this time, law enforcement is not engaged in any active investigation.

What You Can Do

While we have no current indication that your personal information has been misused, we encourage you to remain vigilant by monitoring your personal accounts and statements. For more information about how to access a free credit report, you can visit <https://www.usa.gov/credit-reports>.

To the extent you have not changed your Zenefits password or confirmed your bank account information is accurate, we encourage you to do so. We also recommend updating your banking and financial account logins and passwords, and monitoring those accounts for any suspicious activity.

You may obtain additional information about fraud alerts, security freezes, and preventing identity theft from the Federal Trade Commission by calling its identity theft hotline: 1-877-438-4338 or reporting identity theft online at www.IdentityTheft.gov. The FTC also provides information online at <https://www.usa.gov/identity-theft>. The FTC can also be reached at: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also contact the national consumer reporting agencies regarding your credit reports and identify theft using the following information:

National Consumer Reporting Agencies Contact Information		
TransUnion	Experian	Equifax
P.O. Box 2000	P.O. Box 9554	P.O. Box 105788
Chester, PA 19022	Allen, TX 75013	Atlanta, GA 30348
1-888-909-8872	1-888-397-3742	1-800-685-1111
www.transunion.com	www.experian.com	www.equifax.com

You can obtain further information about fraud alerts and security freezes from the FTC and the Consumer Reporting Agencies.

Allstate Identity Protection Monitoring

Finally, as courtesy for this inconvenience, we would like to offer you a 12-month Allstate Identity Protection membership. Please see the attached flyer for a description of the coverage we are offering. To receive this coverage, please contact our management office below. We deeply regret any concern or inconvenience that this may have caused you.



7SIGNAL, Inc.
6155 Rockside Road, Suite 110
Independence, Ohio 44131

If you have any questions about this incident or require further information or assistance, please contact the Security Advisory Team at security@7SIGNAL.com.

Sincerely,
7SIGNAL, Inc.

For MARYLAND Residents	You can get additional information regarding steps you can take to prevent identity theft from the Maryland Office of the Attorney General by calling its toll-free consumer hotline: 1-888-743-0023. The AG also provides information online at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/databreach.aspx . The AG can also be reached at: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202.
For NEW YORK Residents	You can get additional information regarding steps you can take to prevent identity theft from the NYS Department of State Division of Consumer Protection by calling its toll-free number at 800-697-1220 or visiting its website at dos.ny.gov/identity-theft-prevention-and-mitigation-program . Information is also available from the NYS Attorney General, which you can obtain by calling its toll-free Consumer Helpline at 800-771-7755 or visiting its website at ag.ny.gov/consumer-frauds-bureau/identity-theft .
For NORTH CAROLINA Residents	You can get additional information regarding steps you can take to prevent identity theft from the North Carolina Attorney General Consumer Protection Division, located at 9001 Mail Service Center, Raleigh, North Carolina, 27699. You can also reach the Division at its toll-free number at 919-716-6000 or by visiting http://www.ncdoj.com .
For RHODE ISLAND Residents	You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office at 150 South Main Street, Providence, Rhode Island 02903. You can also reach the Office at 401-274-4400 or http://www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. 93 total individuals were impacted by the security incident.
For FLORIDA Residents	Three Florida residents were impacted by the security incident.
For TEXAS Residents	Six Texas residents were impacted by the security incident.