CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL
jloyal@c-wlaw.com

JORDAN MORGAN
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm
Visit us online at
www.C-WLAW.com

March 11, 2021

State of New Hampshire
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Incident Notification

To Whom It May Concern:

Please accept this Notification of Security Incident ("Notification") on behalf of our client, Signify Health, LLC ("Signify"). By way of background, Signify serves as a Business Associate to a number of Covered Entities under the Health Insurance Portability and Accountability Act ("HIPAA"). As a Business Associate, Signify is entrusted with certain personally identifiable and/or medical information ("Protected Data") on behalf of its Covered Entity clients ("Clients"). The details of this security incident ("Incident") follow.

Scope of Employee's Role and Misconduct

On October 12, 2020, Signify discovered that an employee inappropriately published his login credentials to a subscription-based job board. This employee published his credentials to secure a coding specialist to help him write a job-related script. According to the employee, they were unaware that they had published their login credentials on the job board at the time of the incident. Signify did not know, consent to, or condone this action; moreover, the employee violated Signify's established policy and Code of Conduct. Signify has since terminated this employee.

This employee was a low-level IT Support Specialist whose job was to receive, log, triage, and track IT support requests in ticketing software called "Jira". Jira is stand-alone software that is not connected to any of Signify's core technology assets. And, as an IT Support Specialist, Signify only provisioned this employee with access to Jira. In other words, the published credentials only permitted access to Jira – they did not and could not be used to access any other systems or technology environments maintained by Signify.

Protected Data is only present in Jira when it is manually uploaded into an IT support ticket to illustrate the reason for which IT support is being requested. To discover any Protected Data, a user must manually open each ticket to determine whether the ticket contains any attachments. If it does, the user must then click on the attachment to determine whether it contains Protected Data.

Scope of Signify's Investigation, Remediation and Notification

Signify learned of the published credentials on October 12, 2020, within approximately three (3) hours of being published by the offending employee. Upon discovery, Signify immediately revoked the published credentials, and suspended the employee. Signify also promptly engaged Kroll, a reputable team of third-party forensic experts, to perform a full and thorough investigation. Through their investigation, Kroll (1) could not establish that the published credentials were ever inappropriately used to access, view, or exfiltrate any Protected Data; (2) confirmed that no other Signify technology environments were touched in this Incident; (3) data-mined the Jira system to identify all Protected Data potentially implicated by this Incident; and (4) conducted a thirty (30) day dark-web search that did not detect any Protected Data.

In response to this Incident, Signify (1) terminated the offending employee, (2) retrained its workforce on the importance of protecting credentials, (3) implemented two-factor authentication for all employees who access Jira, and (4) is evaluating ongoing security improvements. Signify also notified impacted Clients of the Incident and met with many to discuss the scope and nature of the event. Finally, Signify is providing notice of the Incident and offering free credit monitoring to impacted individuals, as required by state law.

Specifically, on March 3, 2021, Signify identified one (1) New Hampshire resident with Protected Data in Jira who may have been affected by this Incident ("Individuals"). In accordance with New Hampshire law, on March 11, 2021, Signify will notify and offer one (1) year of free credit monitoring to each Individual. A sample copy of the notice and offer letter is enclosed. As Signify's investigation remains ongoing, we will of course supplement this Notification if we identify additional New Hampshire residents whose Protected Data was involved in this Incident.

Thank you for your attention to this Notification. Signify understands the paramount need to protect the security and integrity of all data entrusted to its custody and care. It is committed to taking appropriate steps to comply with all applicable data security and notification obligations, and to provide transparency into this Incident. Finally, Signify is looking forward to cooperatively resolving this Incident with you and – most importantly – the impacted Individuals.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal
John Loyal, Esq.

signifyhealth.

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

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

RE: NOTICE OF DATA BREACH
Important Security Notification. Please read this entire letter.

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

I am writing to inform you of a recent data security incident experienced by Signify Health ("Signify") that may have involved your protected health information ("PHI"), described below. After a thorough review of the incident, there is no evidence that your PHI was actually viewed or misused. However, out of an abundance of caution, Signify is notifying you of the event. This letter also details steps you can take to help protect your information, and offers you complimentary identity monitoring services paid for by Signify Health.

To begin, we understand that you may not have heard of Signify Health. Signify provides services to <<b2b_text_1(CoveredEntity)>>in support of its treatment, payment, and health care operations ("Services"). In order to provide these Services, Signify needs access to your PHI, and <<b2b_text_1(CoveredEntity)>> entrusts Signify with the required data. You may be affiliated with one or more of these healthcare organizations that Signify services. Signify takes the privacy and security of all information very seriously, including your information. Signify promptly undertook a thorough investigation of the event and is committed to providing you with ongoing protection of your information.

I sincerely apologize for any concern that this incident may cause you. Let me reassure you that Signify is fully committed to the privacy and protection of your personal information.

What Happened:

On October 12, 2020, Signify became aware of an incident involving the unauthorized use of credentials to our IT support ticket system. Specifically, Signify discovered that an employee, without our prior knowledge or consent, published his log in credentials to the IT support ticket system on a subscription-based job board. This employee was trying to recruit individuals to help him automate certain functions of our IT ticket system. This employee was not permitted to hire any outside individuals or publish his credentials – both actions were direct violations of Signify policy – and the employee has been terminated. However, because he published his credentials on the job board, individuals who saw the post could have used those credentials to gain access to our IT support ticket system. The shared credentials did not permit access to any other Signify systems or technology environments.

As soon as Signify discovered this incident, we immediately terminated the employee's credentials and engaged a team of third-party forensic experts to perform a full and thorough investigation. On January 12, 2021, after a thorough investigation, we could neither prove nor rule out unauthorized access to your PHI.

To date, there is no indication that any of your information was actually viewed, disclosed or exfiltrated by any third-party. We are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources. We take great care in the protection of your information and regret that this incident has occurred.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been viewed or misused. The personal information that could have been viewed may have included your first and last name, in combination with your protected health information, including treatment/diagnosis information, prescription information, provider name, patient ID number, Medicare/Medicaid number, Social Security number, and health insurance information.

Importantly, the information potentially impacted as it relates to you may be limited to only one of the above-listed types of information.

What We Are Doing:

Signify has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately secured the affected account and subsequently terminated the employee who published his credentials. Additionally, Signify is undertaking a comprehensive security training program for all employees, which includes behavior-based learning on the imperative to protect log in credentials. Moreover, Signify has implemented two-factor authentication for all of its technology systems. We retained a third-party forensic firm to conduct a thorough investigation and are offering you complimentary identity monitoring services.

Credit Monitoring:

In an abundance of caution and to help relieve concerns, we have secured the services of Kroll to provide identity monitoring at no cost to you for one (1) 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.

Additional information regarding how to activate your complimentary identity monitoring service is enclosed.

What You Can Do:

- Sign up for Identity Monitoring Services – We encourage you to activate your free identity monitoring services at **https://enroll.idheadquarters.com**, use your membership number, <<Member ID>>, and follow the steps to receive your identity monitoring service online within minutes. Please note the deadline to activate is <<DATE>>.
- Review credit reports –We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not recognize or understand, consult with Kroll or contact the credit agencies directly. You may also wish to place a fraud alert or credit freeze on your credit files. Please review the "Information about Identity Theft Protection", which can be found in the reference guide included with this letter for additional information about these options.
- Review your credit and debit card accounts – Although credit card information was NOT compromised it is always good practice to monitor your account activity regularly to reduce your risk of becoming a victim. If you see something you do not recognize, immediately notify the financial institution as well as the proper law enforcement authorities.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to call 1-855-774-0642, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Signify has no relationship more important or more meaningful than the one we share with you. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,

Lisa E. Davis, J.D.
Chief Privacy Officer

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An initial 1-year fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 2000	P.O. Box 9554	P.O. Box 740256
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30374
1-800-680-7289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. In order to request a security freeze,you will need to provide some or all of the following informationto the credit reporting agency, depending on whether you do so online, by phone, or by mail: 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 (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address,suchas a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W-2;8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements.

Be proactive and create alerts on credit cards and bank accounts to notify you of activity.

If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents,** the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
- **For New York residents,** 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/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov
- **For North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.
- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.

Kroll | A Division of DUFF & PHELPS

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 will 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.

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.

Frequently Asked Questions

1. **What happened?**

   An employee accidentally published his login ID and password to a software system called "Jira" on a public website. Jira contained some information about you. The login ID and password were revoked approximately three hours after they were published.

2. **Was information about me "hacked"?**

   No. This event was caused by an employee who unknowingly and without a bad motive published his login ID and password to Jira.

3. **Did anybody use the employee's login ID and password?**

   Not that we know of. However, someone could have used it. For this reason we are providing you with this notice and the opportunity to enroll in free Identity Monitoring Services.

4. **Was information about me disclosed?**

   Not that we know of. However, for a very brief period of time (3 hours), information about you contained in Jira could have been seen by someone without permission to see it. For this reason, we are offering you Identity Monitoring Services at no charge.

5. **What kind of information could have been disclosed about me?**

   It depends. For some people, only their names and medical record numbers could have been disclosed. For other people, information that *could have been* disclosed included their names, addresses, telephone numbers, Social Security numbers, and diagnoses.

6. **When did this happen?**

   On October 12, 2020.

7. **Why am I just now learning about this?**

   Between October 12, 2020 and today, we have been investigating this event. Our investigation included monitoring the internet for your data. None was found.

8. **Who is Signify Health?**

   Signify Health works with us to help us find ways to provide you with better care at lower costs.

9. **Why did Signify Health have information about me?**

   Signify Health needs to know information about the care you receive so it can help us find ways to improve the care we provide to you.

We sincerely regret that this event happened, and are committed to securing the information we possess about you. We understand that you trust your health care providers and, by extension, us to keep that information safe. We encourage you to sign up for the free Identity Monitoring Services, and wish you more happy, health days at home.

Sincerely,

Lisa Davis, VP, Chief Privacy Officer