[redacted]

[redacted]

[redacted]

NOTICE OF DATA BREACH

[redacted]

Dear Sample A. Sample

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to SafetyCall, which provides adverse event reporting services related to consumer products for various companies, including [redacted]. We wanted to provide you with information about an incident at a third-party vendor, Netgain, potentially involving some of your information and let you know that we continue to take significant measures to protect your information.

What Happened?

Netgain provides data hosting services to SafetyCall. Netgain informed us that it experienced a network intrusion resulting in unauthorized access to certain portions of its network. Netgain indicated to SafetyCall that it first became aware of a potential security incident beginning on November 24, 2020, which ultimately culminated in the launch of ransomware on December 3, 2020. Netgain reported that the last day of unauthorized access on its network was December 3, 2020. Netgain also indicated that its environment is secure. On January 14, 2021, Netgain informed us that certain of SafetyCall's customer's data may have been taken from its network as part of the attack.

What We Are Doing.

Upon learning of the issue, we immediately obtained the records that may have been compromised and began a comprehensive review with outside data privacy professionals to determine whether any sensitive data was located within them. Our investigation concluded on [redacted] that the records did contain a limited amount of personal information.

What Information Was Involved?

The impacted data sets contained some of your personal information, including your name and any information you provided in relation to the product incident you reported when you called to report an issue with a [redacted] product. The information does not include your extensive health record.

What You Can Do.

We have no information to date indicating that your information involved in this incident was or will be used for any unintended purposes. To the extent it is helpful, this letter provides precautionary measures you can take to protect your personal information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do if you are concerned about potential misuse of your information. The response line is available Monday through Friday from 9 am – 11 pm Eastern Time, or Saturday and Sunday from 11 am – 8 pm Eastern Time (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted].

Sincerely,

SafetyCall

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File

You may place a fraud alert on your credit reports. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified below. Additional information is available at https://www.annualcreditreport.com/index.action.

As soon as one credit reporting company confirms your fraud alert, the others are notified to place fraud alerts. After your fraud alert request, all three credit reporting companies will send you one free credit report for your review.

Equifax	*Experian*	*TransUnion*
(800) 525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ P. O. Box 105788 Atlanta, GA 30348	(888) 397-3742 https://www.experian.com/fraud/center.html P. O. Box 9554 Allen, TX 75013	(800) 680-7289 https://www.transunion.com/fraud-alerts P. O. Box 6790 Fullerton, CA 92834-6790

2. Placing a Security Freeze on Your Credit File.

You also have the right to place a security freeze on your credit file. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit file, you need to separately contact each of the three nationwide credit reporting companies. A security freeze can be placed on your credit file at no cost to you. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. We recommend that you contact the credit reporting companies, identified below, by phone or online to find out their specific requirements and expedite this process.

You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

3. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit https://www.consumer.ftc.gov/topics/identity-theft.

4. Protecting Your Medical Information.

We have no information to date indicating that your information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your Explanation of Benefits (EOB) which is a statement you receive from your health insurance company after you have a medical visit. Follow up with your insurance company or care provider's billing office for any items you do not recognize. If necessary, contact the care provider on the EOB statement and ask for copies of medical records from the date of the potential access (noted above) to current date at no expense to you.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.