BOND SCHOENECK & KING

One Lincoln Center | Syracuse, NY 13202-1355 | **bsk.com**

SHANNON A. KNAPP, ESQ.
sknapp@bsk.com
P: 315.218.8306

February 10, 2022

VIA ELECTRONIC MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 00301

Re: *Security Incident Notification*

To Whom It May Concern:

We represent The Bell Company, LLC (Bell Co.), located at 1340 Lexington Avenue, Rochester NY 14606. This letter serves as notice to the Office of the Attorney General pursuant to N.H. Rev. Stat. § 359-C:20(I)(b) of a data security incident that may have affected the personal information of one hundred thirty-four (134) New Hampshire residents.

On or around October 17, 2021, Bell Co. became aware of a computer security incident that was later determined to have resulted in the encryption of certain Bell Co. systems and information. Bell Co. immediately took steps to secure its network and launched an investigation into the nature and scope of the incident with the assistance of cybersecurity professionals. Upon further investigation, it was determined that the incident was due to an unknown actor, who may have accessed or acquired certain company data. After concluding its investigation, Bell Co. determined on or around January 3, 2022, that certain individuals residing in the state of New Hampshire may have been impacted by this incident, in that personal information of those residents may have been accessed or acquired.

As soon as Bell Co. learned of the incident, it commenced an investigation and reported the incident to law enforcement. Bell Co. immediately began working with cybersecurity professionals to contain and suspend the intrusion and to restore access to Bell Co.'s stored data. In addition, Bell Co. is reviewing tis cybersecurity policies and procedures to ensure ongoing compliance with applicable laws and has implemented additional security measures and other changes to protect its data in the future.

Bell. Co. will notify the New Hampshire residents on February 11, 2022, and the individuals will be offered twelve (12) months of complimentary credit monitoring. A sample copy of the notification letter to the affected individuals is included with this correspondence. Should you have any questions or need additional information, please contact me at 315-218-8306 or via email at sknapp@bsk.com.

Very truly yours,

BOND, SCHOENECK & KING, PLLC

s/ Shannon A. Knapp

Shannon A. Knapp

EMPLOYEE-OWNED
BELL
A DIVISION OF HB GLOBAL, LLC

P.O. Box 1907
Suwanee, GA 30024

Notification of Security Breach

To Enroll, Please Call:
1-833-676-2178
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 11, 2022

Dear <<First Name>> <<Last Name>>,

The privacy and security of the personal information we maintain is of the utmost importance to the Bell Company, LLC ("Bell"). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or around October 17, 2021, we became aware of a computer security incident that was later determined to have resulted in the encryption of certain Bell systems and information. We immediately took steps to secure our network and launched an investigation into the nature and scope of the incident with the assistance of cybersecurity professionals. Upon further investigation, it was determined that the incident was due to an unknown actor, who may have accessed or acquired certain company data.

After concluding our investigation, we determined on or around January 3, 2022, that certain individuals residing in the state of New Hampshire may have been impacted by this incident, in that personal information of those residents may have been accessed or acquired.

What Information Was Involved?

We are notifying you that the impacted data may have contained your name, social security number, retirement and employment information including dates of hire and termination dates where applicable, as well as other contact information.

What Are We Doing?

As soon as we were learned of the data incident, we commenced an investigation and reported the incident to law enforcement. We immediately began working with experienced cybersecurity professionals to contain and suspend the intrusion and to restore access to Bell's stored data.

We are continuing to work closely with our outside cybersecurity professionals to ensure that your personal information will be protected. Bell is reviewing its cybersecurity policies and procedures to ensure ongoing compliance with applicable laws. Bell has also implemented additional security measures and other changes intended to protect the privacy of individuals moving forward and to prevent any subsequent incidents in the future.

What You Can Do.

To protect you from any potential misuse of your information, and to demonstrate our commitment to the protection of your personal information, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

[XXXXXXXX]

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-676-2178 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is May 11, 2022.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely apologize and regret any inconvenience this incident may have caused you. You will find detailed instructions for enrollment in identity theft protection services on the enclosed "Other Important Information" document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

If you have any further questions regarding this incident, please call 1-833-676-2178 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Steven Ruether
President

– OTHER IMPORTANT INFORMATION –

1. Credit Monitoring Enrollment.

- Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- Telephone. Contact IDX at 1-833-676-2178 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, *at no charge*. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. 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.

5. Obtain a Police Report

You have the right to obtain a police report about the incident. To do so, please call your local police station.

6. 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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution(s) to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 1-800-771-775 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.