Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Cincinnati Bell Inc. ("Cincinnati Bell") recognizes the importance of protecting our employees' personal information. A vendor recently notified us of an incident that involved your information. This letter explains the incident, measures we have taken, and steps you can take in response.

Cincinnati Bell was notified on April 11, 2019 by an accounting firm that audits our 401(k) benefit plans that an unauthorized person(s) was able to log-in to an employee's email account. The audit firm subsequently identified emails (including attachments) in the compromised mailbox that contained some of your information, including your name and Social Security number. The audit firm reported the employee changed the email account password and disabled the account's web access to its email system.

As a precaution, we have arranged for you to receive a complimentary one-year membership of Experian's® IdentityWorks℠. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks℠ is completely free to you and enrolling in this program will not hurt your credit score. Please see the enclosed materials for more information on identity theft prevention and IdentityWorks℠, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect your information and safeguard your 401(k) account.

We take the security of your personal information very seriously and require that our vendors implement appropriate training and security measures. We regret that this occurred and apologize for any inconvenience. If you have any questions, please call 877-253-3702, Monday through Friday, from 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,

Leo Cronin
VP and Chief Security Officer
Cincinnati Bell, Inc.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **<<Activation Code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **<<Enrollment Deadline>>**. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Steps You Can Take

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023 / (410) 576-6300 (for calls originating outside Maryland), www.oag.state.md.us

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, 919-716-6400 / 1-877-566-7226, www.ncdoj.gov

Fraud Alerts: There are two types of fraud alerts 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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

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 years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

NetBenefits® Customer Protection

How 2-Factor Authentication Works

To help prevent unauthorized access to your Fidelity NetBenefits® account, we use an enhanced security feature to verify your identity.

HOW IT WORKS

1. GET A CODE

2. ENTER THE CODE

3. ON YOUR WAY

WHAT IS 2-FACTOR AUTHENTICATION?

With 2-factor authentication, an extra layer of security is added to your NetBenefits account to prevent someone from accessing your account or performing certain transactions within your account, even if they have your password. This extra security measure requires you to verify your identity using a randomized 6-digit code. You can choose to have this security code sent to your mobile phone (or an alternate phone number) via text or voice call. Each security code is used only once. It is *not* a password that you need to create and remember.

While 2-factor authentication for key NetBenefits transactions is automatically enabled, we recommend that you turn on 2-factor authentication at login (find out how below).

NEXT STEPS

Please take a moment to log in to NetBenefits.com. Navigate to *Profile*, and under *Personal & Contact Information*, verify that your mobile phone number and other contact details are current. To turn on 2-factor authentication at login, visit the *Security Center* in *Profile* and select the *2-Factor Authentication* link. Please note that to take advantage of this feature, you must have at least one phone number on file in NetBenefits.

Fidelity INVESTMENTS

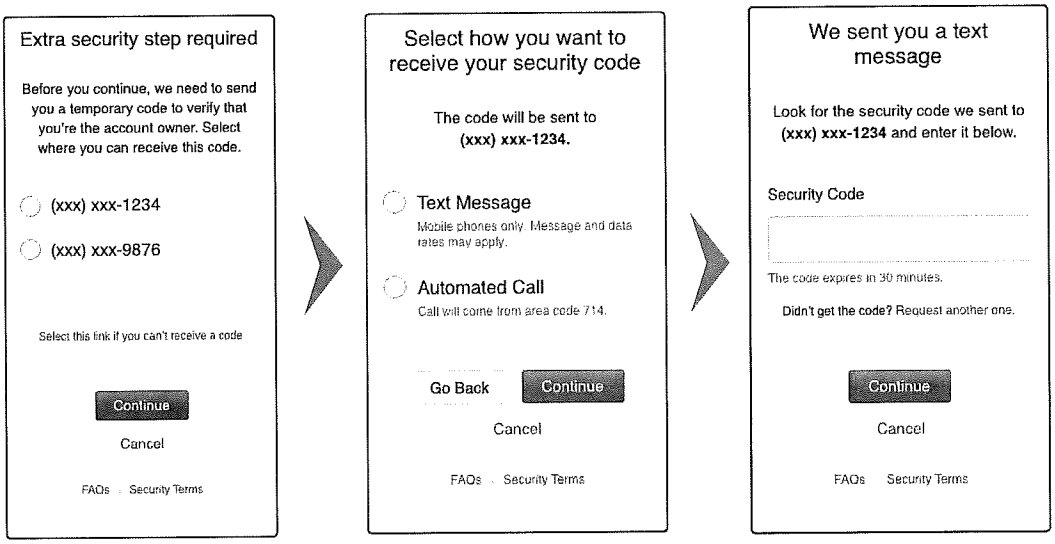
Frequently Asked Questions

Q: Why is this extra step required?

A: Common online activities, such as downloading apps or using the same password on multiple sites, can put your information at risk. Phishing emails and data breaches at companies where you have previously done business can also pose a threat. We use the 2-factor security code as a second level of verification to help prevent unauthorized access to your account (for example, in situations where your username and/or password may have been compromised).

Q: What will the 2-factor authentication experience look like?

A: Review the sample screens below:



Q: How do I update my phone numbers?

A: You can update your phone numbers on NetBenefits by visiting *Profile* after logging in.

Q: What if I don't have my phone with me?

A: Don't worry—you can still receive your security code. Simply log in to your account and request that the code be sent to your alternate phone number. If you don't have an alternate number listed, please call a customer service representative at 800-544-4637. We're available Monday through Friday, 8:30 a.m. to midnight Eastern time.

Q: I did not receive a code. What should I do?

A:
- If you choose to receive the code via text message, ensure that your phone is capable of receiving texts.
- If you still do not receive a code, consider having the code sent via an alternate method, such as a voice call.

Q: My code doesn't work. What should I do?

A: First, make sure to enter the security code that is in the message itself and not the hyphenated six-digit incoming number. If this doesn't solve the problem, do the following:

1. Select *Request a new code*.
2. If you receive multiple codes, enter the most recent one.

Q: You asked for my security code. Does this mean someone tried to access my account?

A: No, it's just a security best practice we implement to help prevent unauthorized access. We take security very seriously and employ the latest measures to help protect your information.

Q: Can I access my account from different devices?

A: Yes, though you may be asked for a security code if you're accessing your accounts from a device we do not recognize. To register your device, select *Remember this device* after entering your code.

Q: How does *Remember this device* work?

A: When you select *Remember this device*, we mark that device as a trusted resource. We may still request a security code periodically. To help maintain security, we recommend that you register only devices that you use frequently. You can register multiple personal devices, but please do not register public devices.

Q: I previously selected *Remember this device*. Why did I have to request a security code?

A: Device recognition is just one of several factors we use to verify your identity. For example, if you are using a different browser or if you registered multiple devices, we may request a security code to confirm your identity.

Q: What if I lose or give away a device I registered?

A: If this happens, please call a customer service representative at 800-544-4637. We're available Monday through Friday, 8:30 a.m. to midnight Eastern time.

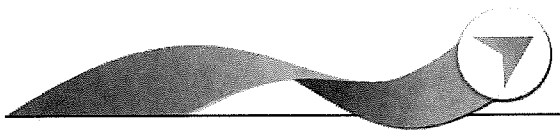
Q: Why am I going through 2-factor authentication every time I log in to the site?

A: You signed up for 2-factor authentication at login. When entering the one-time passcode, remember to select *Remember this device*. Periodically, you may still be challenged if we detect changes to your device.

Screenshots are for illustrative purposes only.

765241.4.0

37219_03



THE TOP 5 THINGS YOU CAN DO TO PROTECT YOUR ACCOUNT

Keep your Fidelity workplace savings account safe and secure, and help reduce the possibility of identity theft.

To Do	WHY?	HOW?
1. Set up online access for your Fidelity NetBenefits® account.	The most effective thing you can do to protect your account is to register online to establish your online access. Cybercriminals frequently attempt to target unregistered online accounts.	**From the NetBenefits.com login page, select *Register as a new user*.**
2. Create a UNIQUE username and password for your Fidelity NetBenefits account that is not used for other online accounts. Don't share this information with any third parties.	Reusing a single username or password for multiple websites, or sharing your login credentials with third-party sites, puts your account at risk if these other sites are compromised. Cybercriminals frequently try to log in with stolen credentials. Avoid using your Social Security number (SSN) as your username, as many SSNs have been disclosed during various high-profile data breaches. Using your SSN makes it easier for cybercriminals to compromise your account.	**If you are new to NetBenefits, create a UNIQUE username and password during the *Register as a new user* process.** **If you're already registered, visit NetBenefits.com > Profile > Login & Security to change your username and password.**
3. Add or update your mobile phone number and email address.	Providing this information ensures that you will receive real-time alerts for sensitive online transactions in your account, such as changes to personal information. It also allows you to confirm these transactions through the delivery of a one-time verification code, known as two-factor authentication.	**Visit NetBenefits.com > Profile > Personal & Contact Information.**
4. Monitor your Fidelity NetBenefits account monthly.	You would know better than anyone if something has gone missing from your account or if changes have been made that you didn't initiate. Log in at least monthly, and contact us if you detect any unusual or unauthorized activity. To make this easy, sign up for eDelivery to receive account statements via email.	**Visit NetBenefits.com > Profile > Preferences.** Choose to receive your documents via email instead of U.S. Mail.
5. Enable Fidelity MyVoice℠.	Our voice verification confirms your identity when you call us, so you can skip entering PINs and passwords and get things done right away.	**The next time you call, a Fidelity Representative will offer to enroll you**—you just need to give Fidelity consent to create your unique voiceprint.

815109.2.0