NATIONAL CENTER
FOR CONSTRUCTION
EDUCATION AND RESEARCH

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

[redacted]

[redacted]

Dear [redacted]:

The privacy and security of our employees' personal information is of the utmost importance to National Center for Construction Education and Research ("NCCER"). We are writing to follow up on a recent incident involving the disclosure of your personal information. We want to provide you with additional 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 personal information.

As we recently informed you, we discovered that an email phishing attack resulted in the inadvertent disclosure of employee W2 information to an unauthorized individual. We became aware of this incident on March 2, 2023, after a small number of employees reported that their tax returns were rejected by the IRS as they had already been filed. Upon becoming aware of this incident, we immediately commenced an internal investigation to determine the nature and scope of the incident. Based on our investigation, we confirmed that this was an isolated disclosure resulting from a phishing attack that occurred on January 26, 2023.

The information disclosed included your 2022 W2 information, such as your name, address, Social Security number, 2022 earnings, and other tax-related information. Our systems were not breached, and no other information was accessed or acquired.

Upon learning of this issue, we commenced a comprehensive internal investigation and are working with cybersecurity professionals to prevent an incident like this from happening in the future. We are committed to protecting your information and have arranged for you to receive 12 months of identity theft protection services provided by Equifax, at no cost. These services include comprehensive credit monitoring and identity restoration services by Equifax, one of the nationwide credit reporting companies. For more information on identity theft prevention and instructions on how to activate your one-year membership, please refer to the additional information provided in this letter.

We strongly encourage you to enroll in the free service from Equifax. In addition to enrolling in credit monitoring services, this letter provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. Additionally, as the information exposed by this incident could be used to file a fraudulent tax return, we are also including steps you can take to protect yourself from tax fraud. We strongly recommend that all employees follow the steps listed under "Taxes" below.

We are committed to maintaining the privacy of our employee 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 888-401-6661. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 AM – 9:00 PM Eastern Time, except major U.S. holidays.

Sincerely,

Ryan Wilder
Director of Legal & Compliance
National Center for Construction Education and Research

OTHER IMPORTANT INFORMATION

Enter your Activation Code: [redacted]
Enrollment Deadline: [redacted]

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may want to consider placing a fraud alert on your credit report by contacting any of the three nationwide credit reporting agencies identified above. An initial fraud alert is free and will stay on your credit file for at least 90 days. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three (3) major consumer reporting agencies listed above. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-349-9960	1-888-397-3742	1-888-909-8872
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/freeze/center.html	https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to 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 (5) years;
5. Proof of current address, such as 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. 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.

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or up to three (3) 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 (5) 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove 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 (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) 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 (3) 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 (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. 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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes.You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-FTC-HELP (382-4357).

- **For New York Residents**: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

Taxes. Some of the information affected by this incident could be used to file a fraudulent tax return. If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. *See* additional information at http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

If you have an IRS account, visit https://www.irs.gov/payments/your-online-account to check whether your 2022 return has been processed. If you have not yet filed your taxes for 2022, we strongly recommend that you do so as early as possible to determine whether your tax return has been compromised.

Even if you have not had your return filed or been contacted by the IRS, we recommend that you request an identity protection PIN (IP PIN) from the IRS to add an extra layer of security to prevent anyone else from filing a tax return in your name (https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)

For Federal Taxes: If you have or are contacted by the IRS via mail, respond immediately to the IRS notice by calling the number provided on the letter. When you contact the IRS, you (and your authorized representative or third party designee, if any) should have the letter you received, your prior year tax return (if you filed one), your current year tax return (if you filed one) and any supporting documents for each year's return (such as W-2's, 1099's, Schedule C, Schedule F, etc.). Please note: **The IRS will not contact you by telephone or email** to request personal or financial information.

The IRS requires that each individual report the problem to them. The IRS will not financially penalize you even if they paid a fraudulent refund. Accordingly, as an additional measure of precaution, we recommend that you (and, if applicable, your spouse or domestic partner) complete IRS Form 14039 and then mail or fax that form to the IRS. A copy of that form can be obtained by going to https://www.irs.gov/pub/irs-pdf/f14039.pdf. You may also call the IRS Identity Theft Hotline at 800-908-4490 to learn whether you are a victim of a fraudulent scheme or have any further questions. For additional information from the IRS about identity theft, consult https://www.irs.gov/uac/newsroom/identity-theft-information-for-taxpayers-and-victims.

For State Taxes: There may be similar resources and forms for each state, so we recommend that you contact your state department of revenue directly for more information. Additional information on how to contact your state department of revenue may be found by going to http://www.taxadmin.org/state-tax-agencies.