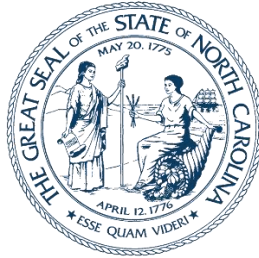




**JAMES WEAVER**  
*Secretary and State Chief Information Officer*



**ROY COOPER**  
*Governor*

NORTH CAROLINA Office of  
*State Human Resources*

**BARBARA GIBSON**  
*Director, State Human Resources*

August 12, 2021

**Re: Notice of Potential Security Problem Involving Personal Data**

Dear Colleague,

We are writing to inform you of a recent security concern involving your personal information. At this time, we have no evidence that any of your personal information has been accessed by anyone outside of those involved in the state identification and remediation efforts. However, from May 14, 2020 to July 30, 2021, a file containing your name and Social Security number was inadvertently accessible on a state intranet site to some state employees.

The file was not accessible to the general public, and we have no information indicating that the file was improperly accessed by anyone. The available data show no evidence that anyone accessed the information outside of those involved in the state identification and remediation efforts. However, at this time we cannot rule out the chance that the file was improperly accessed.

Since this file was discovered, we have worked hard to identify the root cause of the concern and take immediate steps to stop it from happening again. We are sending you this letter to make you aware of the concern and share information on steps you may take to protect yourself from potential online fraud.

**What Happened**

On May 14, 2020, a file containing personal information on 84,860 current or former state agency employees was uploaded by mistake to a state intranet portal. The intranet portal is accessible only if employees authenticate using the username and password that they use for work. Although we have no evidence that anyone accessed the information outside of those involved in the state identification and remediation efforts, the file was potentially accessible to the 65,000 state employees who had authenticated access to that intranet site.

On July 30, 2021, the file was discovered on the intranet site during a sweep for personally identifiable information on the network. The file was taken down immediately.

We have no evidence that the file was accessed or acquired by any unauthorized user. However, because we cannot prove this, we are taking the same efforts that we would take if there were a known data breach under the state's Identity Theft Protection Act.

### **What Information Was Involved**

The file contained the following data fields: name, Social Security number, employing agency, position classification, position work title, and a field which duplicated the Social Security number in certain cases. The file did not contain any other information.

### **What We Are Doing**

The North Carolina Department of Information Technology (DIT) and the Office of State Human Resources (OSHR) take this event very seriously. We took immediate steps to remove the file and look for any similar files. We have immediately implemented new security procedures to protect your personal data. State IT staff will conduct more comprehensive sweeps like the one that found the inappropriately uploaded file, leveraging the full complement of security tools and resources at the state's disposal. New training will be assigned to DIT and OSHR staff on properly managing access rights on the intranet site. Additionally, all staff will be reassigned training on safeguarding personal information.

### **What You Can Do**

Although at this time we have no information that a data breach occurred, as a courtesy we are working to make available to you 24 months of identity theft resolution services at no charge to you. We will share details on how to enroll as soon as a vendor is selected. Please note that you must enroll to use this free service. We encourage you to do so.

More broadly, it is always a good idea to take measures to protect yourself from cyberfraud. Even if no data were acquired in this instance involving the intranet site, data breaches in the private sector are common. In 2017, almost half of the U.S. population had its personal information exposed in a data breach at Equifax. We have worked with the North Carolina Department of Justice to suggest the following common-sense measures for anyone whose data may have been exposed:

-more-

### **Review Account Statements**

Check your credit, debit, and bank account statements for any activity that you did not authorize. If you see something you did not allow, contact the bank or company that services the account immediately to report the fraud.

### **Monitor Your Credit**

Review your credit reports on a regular schedule, looking for unauthorized entries. A credit monitoring service, which we will provide free for 24 months, can help. Also, anyone can request a free credit report each year by going to [www.annualcreditreport.com](http://www.annualcreditreport.com).

### **Request a Fraud Alert from Credit Bureaus**

You can request a fraud alert from the three credit bureaus (Equifax, Experian, and TransUnion). This tells banks and other creditors to take extra steps to verify your identity before issuing credit in your name. A fraud alert is free and will last one year. You'll also get a free copy of your credit report, which you should review carefully.

To request a fraud alert, you can contact Equifax at 1-800-525-6285, Experian at 1-888-397-3742, and TransUnion at 1-800-680-7289.

### **Consider a Security Freeze**

A security freeze stops access to new credit in your name. Placing a security freeze prohibits credit reporting agencies from releasing any information about you to new creditors without your approval. This makes it hard for an identity thief to use your information to open an account or obtain credit.

North Carolina residents can get free security freezes online, by mail, or phone. The Department of Justice has links, phone numbers, and addresses for how to start a free security freeze at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/free-security-freeze/>, and the Federal Trade Commission has more information at <https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here>.

### **Watch Out for Fake Credit Monitoring Services**

After a data breach, some scammers make calls claiming to be from credit monitoring services. Don't provide private information without making sure that the service is legitimate.

Here are the telephone numbers, websites, and addresses for the major consumer reporting agencies, the Federal Trade Commission, and the North Carolina Attorney General's Office. People can obtain information from these sources about preventing identity theft.

Equifax  
PO Box 105788  
Atlanta, GA 30348  
1-800-349-9960

<https://www.equifax.com/personal/>

Experian  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742

<https://www.experian.com/>

TransUnion  
PO Box 2000  
Chester, PA 19016  
1-888-909-8872

<https://www.transunion.com/>

U.S. Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
202-326-2222

<https://www.consumer.ftc.gov/features/feature-0014-identity-theft>

N.C. Attorney General's Office  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
919-716-6000

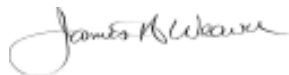
<https://ncdoj.gov/protecting-consumers/protecting-your-identity/>

### **What Comes Next**

Finally, we want to offer our deep and sincere apology that, in this instance, your personal information was not properly secured. As an employer and as your government, we must do better. We will continue to work to better safeguard your data and prevent future security issues. And, going forward, we will work to make this right by providing 24 months of free credit monitoring.

We understand that you may have questions. You can contact us by leaving a message at 984-236-0890 or by contacting us at [DataPrivacy@nc.gov](mailto:DataPrivacy@nc.gov).

Sincerely,



James Weaver, Secretary  
NC Department of Information Technology



Barbara Gibson, Director  
Office of State Human Resources