



2049 Century Park East, Suite 2900, Los Angeles, CA 90067 • (310) 229-1335

June 26, 2023

Pasha Sternberg  
Principal  
310.229.1335  
psternberg@polsinelli.com

**VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)**

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

***Re: Notification of a Data Security Incident***

Dear Madam/Sir:

We represent Barrow County Board of Commissioners (“Barrow County”), located at 30 N. Broad Street Winder, Georgia 30680, in connection with an incident that may have involved the personal information of one (1) Maryland resident. VCC is reporting the incident pursuant to pursuant to MD. CODE ANN., COM. LAW § 14-3504(H). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Barrow County is notifying you of this Incident, Barrow County does not waive any rights or defenses relating to the incident or this notice, or the applicability of Maryland law on personal jurisdiction.

**NATURE OF THE INCIDENT**

Barrow County has discovered suspicious activity in its email environment. Upon discovering the incident, Barrow County began an internal investigation, and engaged, through counsel, a leading computer forensics cybersecurity firm to investigate the incident and confirm the security of its email environment and computer systems. Through that investigation, Barrow County determined that an unauthorized third party gained access to certain Barrow County email accounts between March 6, 2022, and August 2, 2022.

Following a review of the contents of the involved email accounts, Barrow County determined that the accounts contained the personal information of one (1) Maryland resident. The information included the individual’s name and their driver’s license or state identification number.

[polsinelli.com](http://polsinelli.com)

---

Atlanta    Boston    Chicago    Dallas    Denver    Houston    Kansas City    Los Angeles    Miami    Nashville    New York  
Phoenix    St. Louis    San Francisco    Seattle    Silicon Valley    Washington, D.C.    Wilmington

Polsinelli PC, Polsinelli LLP in California



June 26, 2023

Page 2

### **NOTIFICATION TO THE MARYLAND RESIDENT**

Barrow County determined that the emails accessed contained the personal information of one (1) Maryland resident. Barrow County mailed notification letters to these individuals via US First Class mail on June 26, 2023. Enclosed is a sample of the notice sent to the Maryland resident.

### **STEPS TAKEN RELATING TO THE INCIDENT**

Upon learning of the incident, Barrow County contained the incident by resetting the passwords for the involved email accounts and initiating an internal investigation. It also engaged a forensic cybersecurity firm, through counsel, to investigate the incident and confirm the security of its email environment and computer systems. In addition, Barrow County is reviewing its information security policies and evaluating additional trainings and controls it can implement to reduce the risk of a similar incident occurring in the future. Finally, as discussed above, Barrow County has notified the involved individuals, and has coordinated complimentary credit monitoring and identity theft protection services to individuals whose Social Security numbers or driver's license numbers may have been involved in the incident.

### **CONTACT INFORMATION**

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Pasha Sternberg  
Principal

Enclosure



BARROW COUNTY  
Georgia

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>>

RE: NOTICE OF DATA BREACH

Dear <<Name 1>>:

The Barrow County Board of Commissioners values and respects the privacy and security of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information stored in our systems. This letter provides additional information about the incident and guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

**What Happened?** We discovered suspicious activity that occurred in our email environment. Upon discovery, we promptly began an internal investigation and engaged a forensic security firm to investigate the incident and secure our computer and email systems. As part of our investigation, it was determined that the unauthorized person(s) accessed certain Barrow County Board of Commissioners email accounts between March 6, 2022 and August 2, 2022.

**What Information Was Involved?** We conducted a review of those email accounts' contents to determine if they contained any personal information. We recently determined that the accounts contained some personal information that included your name, together with your <<Breached elements>>.

**What We Are Doing.** We take the privacy and security of our customers' personal information very seriously. We have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft involving your information, we are also offering a complimentary one-year membership of Equifax Credit Watch Gold. 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. Equifax Credit Watch Gold is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Equifax Credit Watch Gold, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

**What You Can Do.** While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

**For More Information.** We value the trust you place in us to protect your information, take our responsibility to safeguard your information seriously, and apologize for any inconvenience or concern this incident might cause. If you have any questions or concerns, please contact us at 888-301-5191 between 9:00 am and 9:00 pm EST.

Sincerely,

Vickie Short  
Interim County Manager



<<Name1>>  
Enter your Activation Code: <<ACTIVATIONCODE>>  
Enrollment Deadline: <<ENROLLMENTDEADLINE>>

## **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<sup>1</sup> 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<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- 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<sup>4</sup>

### **Enrollment Instructions**

Go to [www.equifax.com/activate](http://www.equifax.com/activate)

Enter your unique Activation Code of <<ACTIVATIONCODE>>, 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.

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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](http://www.optoutprescreen.com).

<sup>4</sup> 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.

### Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**Credit Reports:** You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax  
1-866-349-5191  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
1-888-397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 2002  
Allen, TX 75013

TransUnion  
1-800-888-4213  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 2000  
Chester, PA 19016

**Fraud Alerts:** You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

**Credit and Security Freezes:** You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze  
1-888-298-0045  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 105788  
Atlanta, GA 30348

Experian Security Freeze  
1-888-397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 9554  
Allen, TX 75013

TransUnion Security Freeze  
1-888-909-8872  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 160  
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

**Maryland Residents:** Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

**New York State Residents:** New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

**North Carolina Residents:** North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; [www.ncdoj.gov](http://www.ncdoj.gov).