



P.O. Box 1907
Suwanee, GA 30024

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

Enrollment Deadline: August 1, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

May 1, 2026

NOTICE OF DATA <<Variable 2 - SECURITY INCIDENT/BREACH>>

Dear <<Full Name>>:

Mitchell County, North Carolina (the “County”), is writing to tell you about a ransomware attack involving personal information, including protected health information, maintained by the County. We take this matter very seriously because we are committed to the privacy and security of all information in our possession. We are providing this notice to tell you about the incident, offer complimentary identity monitoring services, and suggest ways that you can protect your information.

What Happened

On October 20, 2025, the County detected ransomware on our computer network. As soon as we learned this, we began working to investigate and determine the scope of the incident. We also reported this incident to federal law enforcement and worked with nationally recognized third-party cybersecurity and data forensics consultants, the North Carolina Joint Cybersecurity Task Force and other state resources to assist us. As part of the investigation, we determined that there was unauthorized access to the County network between October 16, 2025 and October 20, 2025. During that time, the cyber criminals took certain data from our network, which included personal information and protected health information. After taking the time to securely restore our network, we conducted a thorough review of the impacted data to determine: (1) what information was involved; (2) who may have been affected; and (3) where those people reside. On April 1, 2026, we completed that review and began working to provide written notice of this incident.

What Information Was Involved

The affected data included your <<variable 1 – data elements>>, and/or information related to services you may have received from the County.

What We Are Doing About It

As soon as we learned about this incident, we immediately worked with our team to secure our network and begin an investigation. To further enhance our security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Upgrading County email platform;
2. Deployed software to enhance detection and accelerate response to cyber incidents;
3. Updated password policies and strengthening restrictions for access to County systems; and
4. Continuing to take steps to further bolster our cyber defenses.

Additionally, the County notified the United States Department of Health and Human Services and will be providing notice to all appropriate state regulators.

What You Can Do

We recommend that you take the following preventative measures to help protect your information:

1. Enroll in complimentary identity theft protection services through IDX. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To enroll, scan the QR code at the top of this letter or follow the instructions included at the end of this letter.
2. Remain alert for incidents of fraud and identity theft by regularly reviewing any account statements and free credit reports for unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.
3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General, and the major credit bureaus.

For More Information

Please accept our apologies that this incident occurred. The privacy and security of information is important to us, and we remain committed to protecting it. If you have any questions or concerns about this incident, you may call our dedicated assistance line at 1-844-635-8378, between 9:00 am and 9:00 pm Eastern Time, Monday through Friday, excluding U.S. holidays.

Sincerely,



Allen Cook
Mitchell County Manager

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit <https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/> for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at <https://consumer.ftc.gov/features/identity-theft>. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-833-799-5355 www.transunion.com
--	---	---

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf> and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report. You may be able to obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one 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. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting 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.

Additional Helpful Information

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 at the information provided above. This notice was not delayed as a result of a law enforcement investigation.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

DISTRICT OF COLUMBIA residents: You may also obtain information about preventing and avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of the Attorney General of the District of Columbia
Office of Consumer Protection
400 6th Street NW
Washington, D.C. 20001
www.oag.dc.gov
1-202-727-3400

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
<https://oag.maryland.gov>
Toll-free: 1-888-743-0023

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
<http://www.dos.ny.gov/consumerprotection>

New York Attorney General
1-800-771-7755
<https://ag.ny.gov/>

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.gov
1-877-566-7226 (Toll-free in North Carolina)
919-716-6000



Credit Monitoring Enrollment Instructions

1. Website and Enrollment. Scan the QR image or 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. Please note the deadline to enroll is August 1, 2026.

2. 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.

3. Telephone. Contact IDX at 1-844-635-8378 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items in your credit report and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.