



Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

October 25, 2022

VIA E-MAIL: IDTheft@oag.state.md.us

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

Re: Notice of Data Breach

Dear Attorney General Frosh:

This notice is provided on behalf of my client, Gordon County, Georgia (the “County”) following a ransomware attack that involved the name, date of birth, address, and Social Security number of one (1) Maryland resident. The County will provide written notice to this individual later today, via U.S. Mail. The notice letter includes general advice on how to protect one’s identity, obtain free credit reports, and place security freezes, as well as instructions for enrolling in a one-year, complimentary membership for credit monitoring and identity theft services with Experian. A sample notice letter is enclosed and additional information about the incident is below.

On March 28, 2022, the County detected and responded to a ransomware attack on its computer network. As soon as the County discovered this, the County engaged legal counsel with expertise in cybersecurity. Legal counsel also hired a nationally recognized cybersecurity and digital forensics firm to assist with the investigation, contain the malware, mitigate any harm, and restore operations. With assistance from its cybersecurity experts, the County also alerted the Federal Bureau of Investigation. The investigation revealed that the cybercriminals had accessed the County’s computer network and removed some County data before deploying the ransomware. The County extensively reviewed this data with assistance from legal counsel in order to determine what information was involved, who may have been affected, and where those people reside so that it could provide proper notice.

On July 20, 2022, the County mailed notice letters to all impacted individuals. In the weeks thereafter, the County received certain individual notice letters that were returned in the mail as “undeliverable”, at which time the County worked with outside counsel to locate updated addresses for these individuals. In an effort to ensure written notice is provided to all impacted individuals, the County is re-mailing the returned letters to individuals for whom updated address information is available. Therefore, although no Maryland residents were included in the initial mailing, on October 6, 2022, the County discovered that one (1) intended recipient of the original notification letter now resides in Maryland.

Because cyber threats are always evolving, the County works to identify and mitigate threats and evaluates its IT security protocols to ensure that sensitive data is protected. In addition, to further improve

its network security and help prevent similar occurrences in the future, the County has taken, or will be taking, the following steps:

1. Closely monitoring and restricting outside access to its computer network;
2. Requiring multi-factor authentication for remote access;
3. Enhancing network intrusion detection and response; and
4. Enhancing its cyber training and providing regular communications in order to increase cyber awareness.

In addition, consistent with its compliance obligations and responsibilities, the County provided notice of this incident to appropriate state regulators.

The County is committed to protecting the security and confidentiality of sensitive information and will continue to invest in the internal resources and tools necessary to help prevent something like this from happening again. Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure



Gordon County Board of Commissioners

Board of Commissioners

Becky Hood, Chairman
Chad Steward, Vice-Chairman
Kevin Cunningham, Commissioner
M.L. Bud Owens, Commissioner
Bruce Potts, Commissioner

James F. Ledbetter, Administrator
jledbetter@gordoncounty.org

Annette Berry, County Clerk
aberry@gordoncounty.org



i4989-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 ADULT PII SSN DL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

October 25, 2022

Dear Sample A. Sample:

The privacy and security of your personal information is of the utmost importance to Gordon County (the “County”). On July 20, 2022, Gordon County provided written notice to you at your last known address in our records regarding a recent data security incident that involved your personal information. Your notice was returned to the County as being “undeliverable,” at which time the County worked to locate your updated address to provide you with this notice.

We are providing this notice as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering, and let you know that we continue to take significant measures to protect your information.

What Happened

On March 28, 2022, we detected and responded to a suspected ransomware attack on our computer network. We began working with cybersecurity experts, including legal counsel and a nationally recognized digital forensics firm, to investigate the incident, contain the attack, mitigate any harm, and restore operations.

The investigation revealed that the cybercriminals had accessed our computer network and removed some County data before deploying the ransomware. Once we learned this, we started thoroughly reviewing this data to determine what information may have been involved and who may have been affected. We completed our review of the impacted data on June 27, 2022. We then worked to locate current contact information for affected individuals so that we could provide proper notice.

What Information Was Involved

The impacted data included your name, date of birth, address, and Social Security number or driver’s license number.

What We Are Doing

We are committed to making this right and are investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. Because cyber threats are always evolving, we work to identify and mitigate threats as they arise and evaluate our IT security protocols to make sure that sensitive data is protected. In addition, to further improve our network security and help prevent similar occurrences in the future, we have taken, or will be taking, the following steps:

1. Closely monitoring and restricting outside access to our computer network;
2. Requiring multi-factor authentication for remote access;
3. Enhancing network intrusion detection and response; and
4. Enhancing our cyber training and providing regular communications in order to increase cyber awareness.



We also alerted law enforcement and have provided them with information about this incident.

What You Can Do

In an abundance of caution, we recommend that you take the following preventative measures to help detect and mitigate any potential misuse of your personal information:

1. Enroll in a complimentary, one-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized 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. We remain fully committed to maintaining the privacy of personal information in our possession and will continue to take many precautions to safeguard it.

If you have any further questions regarding this incident, please contact us, toll-free, at **(833) 420-2843**, Monday through Friday 9 am – 11 pm EST, and Saturday and Sunday 11 am – 8 pm EST. Be prepared to provide your engagement number: **B055894**.

Sincerely,



Becky Hood
Chair-Person,
Gordon County Board of Commissioners

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 www.consumer.ftc.gov/features/feature-0014-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 160 Woodlyn, PA 19094 1-888-909-8872 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.

For Colorado, Georgia, Maryland, and New Jersey residents: You may obtain one or more (depending on 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 at least 90 days. 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

0000001



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.

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

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
www.oag.state.md.us/Consumer
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
<http://www.ag.ny.gov/home.html>

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 Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
Toll-free: 1-877-566-7226

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN
IDENTITYWORKS MEMBERSHIP:**

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: January 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: ABCDEFGHI**

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 **(833) 420-2843** by **January 31, 2023**. Be prepared to provide engagement number **B055894** as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 (833) 420-2843. 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 one year 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.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000001



