Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 25, 2022

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent Scott County, Iowa ("Scott County") located at 600 W. 4th Street Davenport, Iowa 52801, and are writing to supplement our June 24, 2022 notice to your office (the June 24 Notice"). The June 24 Notice is attached hereto as ***Exhibit A.*** Since the submission of the June 24 Notice, Scott County began providing notice on behalf of the entities listed in ***Exhibit B***. This incident may have impacted the security of personal information relating to an additional nine (9) Iowa residents. By providing this notice, Scott County does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 30, 2021, Scott County became aware of suspicious activity relating to an employee email account that was sending unauthorized messages to internal and external users. Scott County immediately launched an investigation to determine the cause of the activity and to secure the account. Working with an outside computer forensics specialist, the investigation determined that an unauthorized actor had accessed three (3) employee email accounts between October 27, 2021 and December 1, 2021. Because Scott County was unable to determine which email messages in the accounts were viewed by the unauthorized actor, Scott County began to review the entire contents of the affected email accounts to identify what information was accessible to the unauthorized actor. Scott County received the initial results of the comprehensive data review on February 22, 2022. Scott County then undertook further analysis of the results of the data review, and as of April 26, 2022, identified that information related to certain clients, employees of Scott County, and other individuals who received healthcare treatment or services facilitated by Scott County or local healthcare providers

may have been impacted by this event. Scott County has been working since this time to verify the information at issue, communicate with the relevant data owners, and locate address information for impacted individuals in order to notify them of this event.

The information that could have been subject to unauthorized access includes name, date of birth and medical information. However, Scott County has no evidence that any specific individuals' information was accessed or viewed in connection with the event, and has no evidence of any identity theft or fraud occurring as a result of the event.

Notice to Iowa Residents

On or about July 25, 2022, Scott County continued providing written notice of this incident to an additional nine (9) Iowa residents on behalf of the entities listed in *Exhibit B*. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, Scott County moved quickly to investigate and respond to the incident, locked down the affected accounts, assessed the security of its systems, and worked to identify potentially affected individuals. Scott County is also working to implement additional safeguards and training to its employees. Scott County is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Scott County is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Scott County is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Scott County is providing written notice of this incident to relevant state and federal regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jpc
Enclosure

EXHIBIT B

Entity Name	**Number of Impacted Iowa Residents**
University of Iowa State Hygienic Lab	2
Compassion Counseling, Inc.	1
Hammond-Henry Hospital	6

EXHIBIT A

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 24, 2022

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Scott County, Iowa ("Scott County") located at 600 W. 4th Street Davenport, Iowa 52801, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seven hundred one (701) Iowa residents. By providing this notice, Scott County does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 30, 2021, Scott County became aware of suspicious activity relating to an employee email account that was sending unauthorized messages to internal and external users. Scott County immediately launched an investigation to determine the cause of the activity and to secure the account. Working with an outside computer forensics specialist, the investigation determined that an unauthorized actor had accessed three (3) employee email accounts between October 27, 2021 and December 1, 2021. Because Scott County was unable to determine which email messages in the accounts were viewed by the unauthorized actor, Scott County began to review the entire contents of the affected email accounts to identify what information was accessible to the unauthorized actor. Scott County received the initial results of the comprehensive data review on February 22, 2022. Scott County then undertook further analysis of the results of the data review, and as of April 26, 2022, identified that information related to certain clients, employees of Scott County, and other individuals who received healthcare treatment or services facilitated by Scott County or local healthcare providers may have been impacted by this event. Scott County has been working since this time to verify the information at issue, communicate with the relevant data owners, and locate address information for impacted individuals in order to notify them of this event.

The information that could have been subject to unauthorized access varies for each person but includes one or more of the following types of information in addition to the individual's name: Social Security

number, driver's license number, state identification number, and/or financial account information. However, Scott County has no evidence that any specific individuals' information was accessed or viewed in connection with the event, and has no evidence of any identity theft or fraud occurring as a result of the event.

Notice to Iowa Residents

On June 24, 2022, Scott County began providing written notice of this incident to seven hundred one (701) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Scott County moved quickly to investigate and respond to the incident, locked down the affected accounts, assessed the security of its systems, and worked to identify potentially affected individuals. Scott County is also working to implement additional safeguards and training to its employees. Scott County is providing access to credit monitoring services for twelve (12) months, through Kroll, Inc., to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Scott County is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Scott County is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Scott County is providing written notice of this incident to relevant state and federal regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jpc
Enclosure

EXHIBIT B

Return Mail Processing
PO Box 999
Suwanee, GA 30024

July 25, 2022

7 1 1546 **********AUTO**5-DIGIT 52806
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF [DATA EVENT] / [DATA BREACH]

Dear Sample A. Sample:

Scott County, Iowa ("Scott County") is writing to notify you of an incident that may impact the privacy of some of your personal information. Scott County received your information from [Extra1] in connection with the provision of health care to you, or pursuant to State reporting requirements. This incident may have affected some of your laboratory testing information that was transmitted via fax to Scott County by local healthcare providers in connection with required state reporting procedures. While we are unaware of any actual or attempted misuse of your information, we take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible, misuse, should you feel it appropriate to do so.

What Happened? On November 30, 2021, Scott County became aware of suspicious activity relating to an employee email account that was sending unauthorized messages to internal and external users. We immediately launched an investigation to determine the cause of the activity and to secure the account. Working with an outside computer forensics specialist, our investigation determined that an unauthorized actor had accessed three (3) employee email accounts between October 27, 2021 and December 1, 2021. Because we were unable to determine which email messages in the accounts were viewed by the unauthorized actor, we began to review the entire contents of the affected email accounts, with the assistance of an outside vendor, to identify what information was accessible to the unauthorized actor. We received the initial results of the comprehensive review by February 22, 2022. Scott County then undertook further analysis of the results of the data review, and as of April 26, 2022, identified that information related to certain clients, employees of Scott County, and other individuals who received healthcare treatment or services facilitated by Scott County or local healthcare providers may have been impacted by this event. As a result of the investigation, we have identified that information related to you may have been impacted by this event. We have been working since this time to verify the information at issue and locate address information for impacted individuals in order to notify them of this event.

What Information Was Involved? Although we have no evidence that your personal information was actually accessed, viewed or acquired without permission, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The following types of your information were located in an email or attachment that may have been accessed or acquired by an unauthorized actor: your name and [Extra2].

What We Are Doing. Upon discovery of this incident, we promptly began an investigation with the assistance of third-party cyber security specialists to confirm the nature and scope of this incident. We have also taken steps to secure the impacted email accounts. While we have no evidence of misuse of your information, we are offering you complimentary access to twelve (12) months of credit monitoring and identity theft restoration services, through Kroll, Inc. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Personal Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact (833) 430-2163, toll free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Lori Elam
Mental Health Region CEO
Community Services

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for twelve (12) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for twelve (12) months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twelve (12) month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by October 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 430-2163 by **October 31, 2022.** Be prepared to provide engagement number **B058160** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWELVE (12) MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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 file 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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.