

Niagara County Department of Mental Health  
and Substance Abuse Services

Return to IDX  
P.O Box 989728  
West Sacramento, CA 95798-9728

**Notice of a Data Incident**

**To Enroll, Please Visit:**  
[https://app.idx.us/account-  
creation/protect](https://app.idx.us/account-creation/protect)  
Enrollment Code:

[Address]

[Date]

Dear [Name]:

We are sending this letter to you as part of Niagara County Department of Mental Health and Substance Abuse Services' ("Niagara") commitment to individuals' privacy. We take privacy very seriously and it is important to us that you are made fully aware of a potential privacy issue. We want to provide you with details about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information. Importantly, as of the date of this mailing, there has been no evidence of misuse of your information.

*What Happened?*

On or around May 4, 2022, we became aware of a business email compromise of a single account user of Niagara's email system. We learned of the issue when we were notified of potentially phishing emails being sent from the Niagara email account. We later discovered on June 6, 2022, that the compromise potentially involved patient information.

While we have no indication or evidence that the affected data has been or will be misused, we wanted to notify you of the issue.

*What Information Was Involved?*

The impacted data may have contained some of your health information, such as your name, diagnoses, treatment information, insurance information, and other demographic information.

*What Are We Doing?*

As soon as we learned of the potential issue, we immediately severed the threat actor's access to the email account, which resulted in the threat actor being in the compromised account for a minimal period of time. We then immediately commenced an internal investigation. While we were investigating, we also took steps to notify the public of this issue on August 5, 2022, by providing notice to the media and posting on our website.

We also began working closely with outside cybersecurity professionals and continue to do so to ensure that your information is protected. Niagara has implemented several changes that are designed to protect our data, including your personal data, from any subsequent issues including updated security measures and authentications.

Niagara County Department of Mental Health and Substance Abuse Services  
1001 11th St Suite 200,  
Niagara Falls, NY 14301

What You Can Do.

To protect you from any potential misuse of your information, and to demonstrate our commitment to the protection of your personal information, we are offering identity theft protection services through IDX. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

We encourage you to enroll in the free IDX identity protection services by going to <https://app.idx.us/account-creation/protect> or by calling 1-833-896-7940 and using the enrollment code provided above. IDX representatives are available Monday through Friday from 6 am to 6 pm Pacific Time. Please note that the deadline to enroll is March 1, 2023.

This letter also provides other precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

For More Information.

We understand that this may pose an inconvenience to you. We are committed to providing quality care, including protecting your personal information, and we want to assure you that we have policies and procedures to protect your privacy, which we have reinforced with our staff.

You will find detailed instructions for enrollment on the enclosed “Other Important Information” document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

If you have any further questions regarding this issue, please call 1-833-896-7940 for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read 'Laura J. Kelemen', with a long horizontal flourish extending to the right.

Laura J. Kelemen, LCSW-R  
Director, Niagara County

– OTHER IMPORTANT INFORMATION –

**1. Credit Monitoring Enrollment.**

- Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> or call 1-833-896-7940 and follow the instructions for enrollment using your Enrollment Code.
- 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.

**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

<b>Equifax</b> P.O. Box 105069 Atlanta, GA 30348 <a href="http://www.equifax.com">www.equifax.com</a> 1-800-525-6285	<b>Experian</b> P.O. Box 2002 Allen, TX 75013 <a href="http://www.experian.com">www.experian.com</a> 1-888-397-3742	<b>TransUnion LLC</b> P.O. Box 2000 Chester, PA 19016 <a href="http://www.transunion.com">www.transunion.com</a> 1-800-680-7289
--	---	---

**3. Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, *at no charge*. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 <a href="https://www.freeze.equifax.com">https://www.freeze.equifax.com</a> 1-800-685-1111	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 <a href="http://experian.com/freeze">http://experian.com/freeze</a> 1-888-397-3742	<b>TransUnion Security Freeze</b> P.O. Box 2000 Chester, PA 19016 <a href="http://www.transunion.com/securityfreeze">http://www.transunion.com/securityfreeze</a> 1-888-909-8872
---	--	--

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring 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.

**4. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at [www.annualcreditreport.com](http://www.annualcreditreport.com). Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

## 5. Additional Helpful Resources.

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 on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution(s) to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**Massachusetts Residents:** You have a right to obtain a police report concerning the data incident. To do so, please call your local police.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-775 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.