



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

November 9, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent McLaren Health Care (“McLaren”), located at One McLaren Parkway, Grand Blanc, MI, 48439, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately four hundred seventy-three (473) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, McLaren does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about August 22, 2023, McLaren became aware of suspicious activity related to its computer systems. McLaren immediately launched an investigation with the assistance of third-party forensic specialists to secure its network and to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to McLaren’s network between July 28, 2023, and August 23, 2023. On August 31, 2023, McLaren learned the unauthorized actor had the ability to acquire certain information stored on the network during the period of access. As part of an ongoing investigation, McLaren undertook a thorough review of the potentially impacted files to determine whether any sensitive information was present. It was through this process, which concluded on October 10, 2023, that McLaren determined that information pertaining to certain individuals may have been included in the potentially impacted files.

The information that could have been subject to unauthorized access includes name, Social Security number, health information, and health insurance policy or subscription identification number.

Notice to Maryland Residents

On or about October 20, 2023, McLaren provided substitute via website and media notice. On or about November 9, 2023, McLaren provided written notice of this incident to approximately four hundred seventy-three (473) Maryland 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, McLaren moved quickly to investigate and respond to the incident, assess the security of McLaren systems, and identify potentially affected individuals. Further, McLaren notified federal law enforcement regarding the event. McLaren is also working to implement additional safeguards and training to its employees. McLaren is providing access to credit monitoring services for twelve (12) months through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, McLaren is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. McLaren 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,

A handwritten signature in blue ink that reads "Matthew V. Toldero".

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/ajl
Enclosure

EXHIBIT A



HEALTH CARE

P.O. Box 989728

West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/mlhc>

November 9, 2023

Notice of Data Security <<Incident/Breach>>

Dear <<FIRST NAME>> <<LAST NAME>>,

McLaren Health Care values our relationship with every patient and family we serve, and maintaining your trust and confidence is important to us. We are writing to inform you that our organization recently experienced a cybersecurity event. We are writing today to inform you about what happened, what information was involved, what we have done to address the situation and what you can do to help protect yourself against possible misuse of information.

What Happened? On or about August 22, 2023, we became aware of suspicious activity related to certain McLaren computer systems. We immediately launched an investigation with the assistance of third-party forensic specialists to secure our network and to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to McLaren's network between July 28, 2023, and August 23, 2023. On August 31, 2023, we learned the unauthorized actor had the ability to acquire certain information stored on the network during the period of access.

As part of our ongoing investigation, we undertook a thorough review of the potentially impacted files to determine whether any sensitive information was present. It was through this process, which concluded on October 10, 2023, that we determined that information pertaining to you may have been included in the potentially impacted files.

What Information Was Involved? The information impacted varied by individual and not all information was available for every individual. The information that may have been impacted includes some combination of certain individuals' names and the following: Social Security number, health insurance information, date of birth, and medical information including billing or claims information, diagnosis, physician information, medical record number, Medicare/Medicaid information, prescription/medication information, diagnostic and treatment information.

What We Are Doing. McLaren takes the security of your information seriously. Upon learning of this incident, we immediately took steps to secure our network and maintain operations in a safe and secure fashion. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on our systems. We remain committed to fully complying with all state and federal requirements and maintaining timely and transparent communication with our patients and the community.

What You Can Do. While there is currently no evidence that your information has been misused, we recommend that you remain vigilant, monitor and review all of your financial and account statements and explanations of benefits, and

report any unusual activity to the institution of record and to law enforcement. You may also review the guidance contained in *Recommended Steps to help Protect Your Information*.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services offered by McLaren 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. You will find detailed instructions for enrollment on the enclosed Recommended Steps 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. Please note the deadline to enroll is February 9, 2024.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

For More Information For assistance with questions regarding this incident, please call IDX at (888) 867-1630, scan the QR code above, or go to <https://response.idx.us/mlhc>. Representatives are available Monday through Friday from 9am - 9pm Eastern Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

McLaren Health Care

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/mlhc> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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 (888) 867-1630 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items 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 our ID Care team who will help you determine the cause of the suspicious items. In the unlikely 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.