



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

June 8, 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 Intellihartx, LLC (“ITx”), located at 7 Sheridan Square, Kingsport, TN 37660, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately two hundred eighty-one (281) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ITx 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 February 2, 2023, ITx discovered that its secure file transfer protocol provider, Fortra, was subject to a data privacy event that potentially impacted ITx’s clients’ patient information (“Fortra Event”). ITx promptly launched an investigation to determine the nature and scope of the Fortra Event. On March 24, 2023, ITx completed its initial review of the logs provided to it by Fortra. ITx began notifying potentially affected data owners on April 11, 2023. ITx completed a further review of the additional logs provided by Fortra, as well as correspondence with the unauthorized party, to determine the scope of impacted information on May 10, 2023. ITx then undertook a comprehensive review of the data to determine what information was affected and to whom that information related. This review was completed on May 19, 2023. ITx is unaware of misuse of information with regard to the Fortra Event.

The information that could have been subject to unauthorized access includes name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.

Notice to Maryland Residents

On or about June 8, 2023, ITx began providing written notice of this incident to approximately two hundred eighty-one (281) Maryland residents on behalf of and at the direction of its data owners. 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, ITx moved quickly to investigate and respond to the Fortra Event and identify potentially affected individuals. Further, ITx notified federal law enforcement regarding the event. ITx is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, ITx is providing impacted individuals with guidance on how to better protect against identity theft and fraud. ITx 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.

ITx is providing written notice of this incident to relevant state and federal regulators and to the three major credit reporting agencies, Equifax, Experian, and TransUnion, as necessary and at the direction of its impacted data owners. ITx is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA) at the direction of its impacted data owners.

Office of the Attorney General

June 8, 2023

Page 3

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,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/dtg
Enclosure

EXHIBIT A



P.O. Box 3404, Kingsport, TN 37664



First Last
123 Main St.
City, ST 31533

NOTICE OF SECURITY INCIDENT / DATA BREACH

Dear First Last:

Intellihartx, LLC ("ITx") is a leading Healthcare Revenue Cycle company focused on healthcare clients. [REDACTED] uses our services as part of its medical and/or clinic practices. ITx is writing to notify you of an incident that may affect the privacy of some of your information. We take this incident seriously, and this letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it is appropriate to do so.

What Happened? On February 2, 2023, ITx discovered that its secure file transfer protocol provider, Fortra, was subject to a data privacy event that potentially impacted certain medical providers' information, including [REDACTED] patient information ("Fortra Event"). We promptly launched an investigation to determine the nature and scope of the Fortra Event. On March 24, 2023, we completed our initial review of the logs provided to us by Fortra. We completed a further review of the additional logs provided by Fortra, as well as correspondence with the unauthorized party, to determine the scope of impacted information on May 10, 2023. We then undertook a comprehensive review of the data to determine what information was affected and to whom that information related. This review was completed on May 19, 2023.

We provided an initial notice to [REDACTED] on April 11, 2023. Although there is no evidence of misuse of your information, we are notifying all individuals with sensitive information stored in the affected systems and providing the protection identified below.

What Information Was Involved? Based on information provided by Fortra, it was determined that one or more of the following information may have been present in the affected systems at the time of the Fortra Event: your name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number. No individual's financial information was impacted by the Fortra Event.

What We Are Doing. ITx takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the Fortra Event, we promptly commenced an investigation to confirm the nature and scope of the Fortra Event. To protect against an incident like this from reoccurring, Fortra informed us that it has deleted the unauthorized party's accounts, rebuilt the secure file transfer platform with system limitations and restrictions, and produced a patch for the software. ITx has also implemented additional security measures, including immediate steps to implement measures to harden the security of ITx's use of the GoAnywhere platform. Both ITx and Fortra have notified federal law enforcement about the Fortra Event and are cooperating with law enforcement's investigation of the Fortra Event. Moreover, as an added precaution, we are offering complimentary access to two years of credit monitoring and identity restoration services to you. While this service is free to you, you must enroll on your own using the instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You can also review the enclosed Steps You Can Take to Help Protect Personal Information.

For More Information. If you have additional questions, please call our dedicated assistance line at 833-901-4622 (toll free), Monday through Friday, from 9 am - 9 pm Eastern Time (excluding U.S. holidays). You may write to ITx at P.O. Box 3404, Kingsport, TN 37664-3404 with any additional questions you may have.

Sincerely,

Michael S. Moss
Chief Strategy Officer
www.itxcompanies.com

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 24 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 24 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 24-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 9/30/23** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: [REDACTED]

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 833-901-4622 by 9/30/23. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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.

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
888-298-0045	1-888-397-3742	1 (800) 916-8800
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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>.

For 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 bureaus 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 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. We encourage you to 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 988 Rhode Island residents impacted by this incident.