



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED

MAR 29 2022

CONSUMER

Kevin Dolan  
Office: (267) 930-4861  
Fax: (267) 930-4771  
Email: kdolan@mullen.law

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

March 25, 2022

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Christie Business Holdings Company, P.C. (“Christie Clinic”) located at 101 West University Avenue, Champaign, IL 61820, and are writing to notify your office of an incident that may affect the security of some personal information relating to eighty-two (82) New Hampshire 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, Christie Clinic does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On or about August 10, 2021, Christie Clinic became aware of suspicious activity related to one of its business email accounts. **This event did not impact Christie Clinic’s computer systems, electronic medical record, MyChristie patient portal, or patient care.** The suspicious activity was occurring with respect to only a single user email account. Christie Clinic promptly launched an internal investigation to determine the nature and scope of this incident, and contacted federal law enforcement and worked with them to mitigate the impact of the unauthorized access. Christie Clinic also engaged a leading data forensics firm, and on January 27, 2022, Christie Clinic’s investigation confirmed that there was unauthorized access to the affected email account from July 14, 2021 to August 19, 2021. The investigation indicated that the purpose of the unauthorized access was to intercept a business transaction between Christie Clinic and a third-party vendor. This investigation was unable to determine the extent to which email messages in the account were actually viewed or accessed by an unauthorized actor. As a result, Christie Clinic undertook a review to identify the full scope of information that could have been contained in the affected

Mullen.law

email account to determine whether protected information was potentially impacted. On March 10, 2022, Christie Clinic's review determined that the account contained information related to certain individuals.

The information that could have been subject to unauthorized access includes name, address, Social Security number, medical information, and health insurance information.

### **Notice to New Hampshire Residents**

On or about March 25, 2022, Christie Clinic provided written notice of this incident to all affected individuals, which includes eighty-two (82) New Hampshire 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, Christie Clinic moved quickly to investigate and respond to the incident, assess the security of Christie Clinic systems, and notify potentially affected individuals. Christie Clinic is also working to implement additional safeguards and training to its employees. Christie Clinic 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.

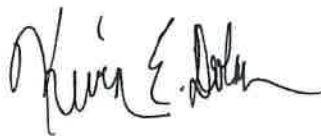
Additionally, Christie Clinic is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Christie Clinic is providing individuals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

Office of the New Hampshire Attorney General  
March 25, 2022  
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) 930-4861.

Very truly yours,

A handwritten signature in black ink, appearing to read "Kevin E. Dolan". The signature is fluid and cursive, with a long horizontal stroke at the end.

Kevin Dolan of  
MULLEN COUGHLIN LLC

KED:bwt  
Enclosure

# Exhibit A



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

March 25, 2022

H7003-L01-0000001 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL  
APT ABC  
123 ANY STREET  
ANYTOWN, ST 12345-6789



**RE: Notice of Data [Variable Header]**

Dear Sample A. Sample:

Christie Business Holdings Company, P.C. (“Christie Clinic”) writes to notify you of an incident that may affect the privacy of some of your information. In an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take additional steps to better protect your personal information, should you feel it is appropriate to do so. **We do not have any evidence of identity theft or misuse of your personal information as a result of this incident, however 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 information, should you feel it appropriate to do so.**

**What Happened?** Christie Clinic recently discovered suspicious activity related to one of its business email accounts. **This event did not impact Christie Clinic’s computer systems, electronic medical record, MyChristie patient portal, or patient care.** The suspicious activity was occurring with respect to only a single user email account. Christie Clinic promptly launched an internal investigation to determine the nature and scope of this incident, and contacted federal law enforcement and worked with them to mitigate the impact of the unauthorized access. We also engaged a leading data forensics firm, and on January 27, 2022, Christie Clinic’s investigation confirmed that there was unauthorized access to the affected email account from July 14, 2021 to August 19, 2021. The investigation indicated that the purpose of the unauthorized access was to intercept a business transaction between Christie Clinic and a third party vendor. This investigation was unable to determine to what extent email messages in the account were actually viewed or accessed by an unauthorized actor. As a result, Christie Clinic undertook a review to identify the full scope of information that could have been contained in the affected email account to determine whether protected information was potentially impacted. On March 10, 2022, Christie Clinic’s review determined that the impacted account *MAY* have contained certain information related to you. We are notifying you of the incident as it *MAY* potentially affect the privacy of some of your information.

**What Information Was Involved?** Christie Clinic’s analysis revealed that the types of information held by Christie Clinic and potentially in the affected email account *MAY* include your name and: address, Social Security number, medical information, and health insurance information. **The unauthorized actor did not have access to the electronic medical record, MyChristie patient portal, or Christie Clinic’s network.**

**What We Are Doing.** Christie Clinic takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we notified federal law enforcement, steps were taken to secure the impacted account and we immediately commenced an investigation to confirm the nature and scope of the incident. We have taken steps to implement additional safeguards for Christie Clinic and its patients. We already employ industry-leading network security solutions and perform regular and ongoing data security and privacy training.

0000001



H7003-L01

Christie Clinic is providing you with ## months of comprehensive credit monitoring and identity protection services through Experian at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

***What You Can Do.*** You can review the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*. You can also enroll to receive the complimentary credit monitoring and identity protection services through Experian. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

***For More Information.*** We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please contact our dedicated assistance line at (866) 915-5006 Monday through Friday from 8 a.m. to 10 p.m. Central, and Saturday and Sunday from 10 a.m. to 7 p.m. Central, or visit our website at [www.christieclinic.com](http://www.christieclinic.com).

Christie Clinic takes the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Scott Segerstrom, Director of Information Systems & Services  
Christie Business Holdings Company, P.C.

## STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

### Enroll in Credit Monitoring

#### What we are doing to protect your information:

To help protect your identity, we are offering a complimentary ##-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: June 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://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 (866) 915-5006 by **June 30, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR ##-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, 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<sup>TM</sup>:** 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<sup>\*\*</sup>:** 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.

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 (866) 915-5006. 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 ## 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

000001



## **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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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](mailto: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 [www.oag.state.md.us](http://www.oag.state.md.us). Christie Clinic is located at 101 West University Avenue, Champaign, IL 61820.

*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](http://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](http://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](http://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 60 Rhode Island residents impacted by this incident.

