



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

January 31, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Prestige Care, Inc. ("Prestige Care") located at 7700 NE Parkway Drive, Suite 300, Vancouver, Washington 98662, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) 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, Prestige Care 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 around September 7, 2023, Prestige Care became aware of suspicious activity on its computer network. Prestige Care launched an investigation and determined that its network had been infected with malware, which prevented access to certain files on the system. Through the investigation, Prestige Care determined that an unauthorized actor may have had access to certain systems that stored personal and health information on September 7, 2023. Prestige Care is undertaking an extensive and time intensive review of what information was potentially impacted and to whom that information relates. On December 18, 2023, Prestige Care determined that information related to certain current former employees and residents was present in its systems. Although Prestige Care has no evidence of any identity theft or fraud in connection with this incident, Prestige Care began providing notice to those individuals whose information was present in its systems.

The information that could have been subject to unauthorized access includes

Notice to New Hampshire Residents

On or about January 31, 2024, Prestige Care began providing written notice of this incident to two (2) 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, Prestige Care moved quickly to investigate and respond to the incident, assess the security of Prestige Care systems, and identify potentially affected individuals. Further, Prestige Care notified law enforcement regarding the event. Prestige Care is providing access to credit monitoring services for _____, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Prestige Care 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. Prestige Care 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.

Prestige Care is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Prestige Care also notified the U.S. Department of Health and Human Services, as well as federal law enforcement.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at _____.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/kld
Enclosure

EXHIBIT A



January 31, 2024

NOTICE OF SECURITY INCIDENT

Dear

Prestige Care, Inc. ("Prestige Care") is writing to notify you of an incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around September 7, 2023, Prestige Care became aware of suspicious activity on our computer network. Prestige Care launched an investigation and determined that our network had been infected with malware, which prevented access to certain files on the system. Through our investigation, we determined that, an unauthorized actor may have had access to certain systems that stored personal and health information on September 7, 2023. Prestige Care is undertaking an extensive and time intensive review of what information was potentially impacted and to whom that information relates. On December 18, 2023, Prestige Care determined that information related to certain current former employees and residents was present in its systems. Although we have no evidence of any identity theft or fraud in connection with this incident, Prestige Care began providing notice to those individuals whose information was present in its systems.

What Information Was Involved? Our investigation determined the following types of your information may have been impacted by this incident:

At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. Data privacy and security are among Prestige Care's highest priorities, and there are extensive measures in place to protect information in Prestige Care's systems. Upon discovery, Prestige Care promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities, as required by law.

As an added precaution, we are also offering of complimentary access to credit monitoring services through Cyberscout, a TransUnion company. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

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 may also review the

information contained in the attached *Steps You Can Take to Help Protect Your Personal Information*. There you will also find more information regarding the complimentary credit monitoring services we are making available to you. While Prestige Care will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

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 call our dedicated assistance line at 1-844-711-0795 between the hours of 8:00 a.m. and 8:00 p.m. ET, Monday - Friday, excluding holidays. You may also write to Prestige Care at 7700 NE Parkway Drive, Suite 300, Vancouver, Washington 98662-6654.

Sincerely,

Prestige Care

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/prestigecare>** and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.