MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

July 2, 2020

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 MelroseWakefield Healthcare, Inc. ("Melrose"), located at 170 Governors Avenue, Medford, MA 02155, and are writing to notify your office of an incident that may affect the security of some personal information relating to two hundred fifty-nine (259) New Hampshire residents. Melrose will supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, Melrose 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 March 20, 2020, Melrose was notified by PaperlessPay Corporation ("PaperlessPay") regarding potential unauthorized access to PaperlessPay's client database. PaperlessPay is a third-party vendor who provides online distribution services for pay stubs and W2 forms for Melrose employees. In this notification PaperlessPay reported that with the help of a third-party forensic investigator and law enforcement, PaperlessPay completed an investigation into unauthorized access of their system. Paperless Pay's investigation was not able to determine what data may have been accessed when the system was accessed on February 18, 2020.

Melrose worked to obtain additional information from Paperless Pay on their investigation, findings and the individuals whose information may have been in their database at the time of this event. Melrose received a list of those individuals with information within the database at the time of the event on May 6, 2020. To date, there is no definitive evidence that any information was accessed or misused, but because the information was present in the data base, Melrose provided notice to all potentially affected individuals out of an abundance of caution.

The information that could have been subject to unauthorized access includes name, address and Social Security numbers.

Notice to New Hampshire Residents

On or about July 2, 2020, Melrose provided written notice of this incident to all potentially affected individuals, which includes two hundred fifty-nine (259) 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, Melrose quickly took steps to investigate and are working to remove all W2 data from PaperlessPay's systems. Melrose is currently working with PaperlessPay to ensure all data related to its employees is returned to Melrose and removed from PaperlessPay's system.

Although a third-party (PaperlessPay) was in possession of the information that was exposed, and Melrose is not aware of any identity theft or fraud occurring as a result of this event, to illustrate its commitment to the protection of personal information, Melrose is providing access to credit monitoring services for twenty-four (24) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Melrose 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. Melrose 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) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/acl

EXHIBIT A

MW MelroseWakefield Healthcare

Proudly wellforce

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

July 2, 2020

F6245-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - INDIVIDUAL
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Breach

Dear Sample A Sample:

MelroseWakefield Healthcare, Inc. ("Melrose") is writing to notify you of an incident that occurred at PaperlessPay Corporation ("PaperlessPay") which may affect the security of some of your personal information. We take this incident very seriously, and 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? As you may be aware, PaperlessPay provides online distribution services for pay stubs and W2 forms for our employees. On March 20, 2020, we were notified by PaperlessPay regarding unauthorized access to PaperlessPay's client database. In this notification they reported that with the help of a third-party forensic investigator and law enforcement, PaperlessPay completed an investigation into unauthorized access of their system. Their investigation determined the unauthorized actor gained access to a database containing employee information, including your W2 records. Paperless Pay's investigation was not able to determine what data may have been accessed when the system was accessed on February 18, 2020.

Since learning of this incident, we have been working to obtain additional information from Paperless Pay on their investigation, findings and the individual whose information may have been in their database at the time of this event. We received a list of those individuals with information within the database at the time of the event on May 6, 2020. To date, there is no definitive evidence that any of your information was accessed or misused, but because your information was present in the data base, we are notifying you out of an abundance of caution.

What Information Was Involved? PaperlessPay confirmed the database containing your information included your name and Social Security number. Please note that while the investigation did not reveal evidence that your information was actually viewed by the unauthorized actor, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. Information privacy and security are among our highest priorities. Melrose has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to investigate and are working to remove all W2 data from PaperlessPay's systems. We are currently working with PaperlessPay to ensure all data related to our employees is returned to Melrose and removed from PaperlessPay's system.

While Paperless Pay is not able to say if your information was accessed, we have arranged to have Experian protect your identity for 24 months at no cost to you as an added precaution.

What You Can Do. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also enroll to receive the identity protection services we are making available to you. Melrose will cover the cost of this service. Because the enrollment process does not allow us to enroll on your behalf, you will need to enroll yourself by following the instructions outlined in this letter.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact (833) 704-9386.

Sincerely,

Kelley McCue, Esq., CHC, CHPC
Director of Corporate Compliance/Chief Privacy Officer | Compliance

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. 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: September 30, 2020 (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 or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 704-9386 by September 30, 2020. 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 agents 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.
- Up to $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

Monitor Accounts

We 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. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

* 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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	https://www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us. Melrose may be contacted by mail at 170 Governors Avenue, Medford, MA 02155.

For 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/.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 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 13 Rhode Island residents impacted by this incident.

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 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 violators. 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.