


RUSKIN MOSCOU FALTISCHEK P.C.
Counselors at Law

Writer's Direct Dial: (516) 663-6687
Writer's Direct Fax: (516) 663-6887
Writer's E-Mail: ndellaragione@rmfpc.com

January 27, 2020

VIA EMAIL AND FEDEX

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Data Breach Notification

Dear Attorney General MacDonald:

We are counsel to Personal Touch Holding Corp. and its direct and indirect subsidiaries Personal Touch Home-Aides, Inc., Personal Touch Home Care of Greater Portsmouth, Inc., and Personal Touch Home Care of Ohio, Inc. (the "Company"). Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, we are writing to notify you of a breach involving two thousand five hundred and seventy six (2,576) New Hampshire residents.

On December 1, 2019, the Company was notified by its cloud-hosting provider, Crossroads Technologies Inc., that there was a breach at its Pennsylvania data center, where the Company's electronic medical records and certain employee records relevant thereto are hosted. Crossroads Technologies, Inc. has reported to the Company that it was the victim of a ransomware attack and that it is investigating the extent of the breach. The electronic medical records that Crossroads Technologies, Inc. hosted for the Company contained patient information including medical treatment information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, and Social Security number. The electronic medical records also contained the following employee information, including first and last name, address, telephone numbers, date of birth, Social Security number, clinical licensing number, driver's license number, and basic financial information such as I-9s and tax codes.

Upon being notified of a security incident at Crossroads Technologies, Inc., the Company immediately began working with and corresponding with Crossroads Technologies, Inc. to stay updated regarding the investigation. During the course of the investigation, Crossroads Technologies, Inc. notified the Company that they were working with third-party forensic analysts and the Federal Bureau of Investigations to determine the origins and scope of the breach.

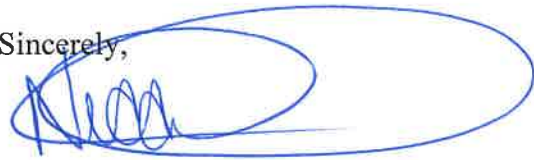
RMF
RUSKIN MOSCOU FALTISCHEK P.C.
Counselors at Law

January 27, 2020
Page 2

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, we intend to notify residents on or about January 28, 2020. We have attached copies of the notifications that will be provided to residents.

Please be assured that the Company is committed to its patients' and employees' privacy. Please feel free to contact me at 516-663-6687 with any questions or concerns.

Sincerely,



NICOLE E. DELLA RAGIONE
For the Firm

Encls.

Personal Touch Home-Aides, Inc.
C/O Personal Touch Holding Corp.
1985 Marcus Avenue, Suite 202
Lake Success, NY 111042
718-736-7233

January 28, 2020



F2790-L03-0000018 P001 T00002 *****MIXED AADC 159
SAMPLE A SAMPLE - L03_PTEMPLOYEES_MAJORITY
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A Sample:

Personal Touch Home-Aides, Inc. C/O Personal Touch Holding Corp., (the “Company”) is hereby providing you with a notification regarding a breach that may have affected your personally identifiable information.

WHAT HAPPENED:

On December 1, 2019, the Company was notified by its cloud-hosting provider, Crossroads Technologies Inc., that there was a breach at its Pennsylvania data center, where the Company’s electronic medical records are hosted. Crossroads Technologies, Inc. has reported to us that it was the victim of a ransomware attack and that it is investigating the extent of the breach. Although we cannot confirm the extent to which your data was compromised, we are notifying you that the breach occurred, in our efforts to comply with the applicable state data breach notification laws.

WHAT INFORMATION WAS INVOLVED:

Crossroads Technologies, Inc. hosts an electronic medical record system that contains personally identifiable information relating to your work as an employee of this Company. This information includes first and last name, address, telephone numbers, date of birth, Social Security number, clinical licensing number, driver’s license number, and basic financial information such as I-9s and tax codes. At this time, we cannot confirm to what extent your information was compromised.

WHAT WE ARE DOING:

Upon being notified of a security incident at Crossroads Technologies, Inc., we immediately began working with and corresponding with Crossroads Technologies to stay updated regarding the investigation. During the course of the investigation, Crossroads Technologies, Inc. notified us that they were working with third-party forensic analysts and the Federal Bureau of Investigations to determine the origins and scope of the breach. Pursuant to applicable law, we will be notifying state regulators as required.

000001



F2790-L0:

To help protect your identity, we are offering a complimentary one- year membership of Experian's® IdentityWorksSM. 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: 5.31.2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: 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 **877-644-1116** by **5.31.2020**. Be prepared to provide engagement number **DB17313** as proof of eligibility for the identity restoration services by Experian.

WHAT YOU CAN DO:

As recommended by the Federal Trade Commission ("FTC"), we recommend that you remain vigilant and monitor your account statements and credit bureau reports closely. The FTC also recommends you place a fraud alert on your credit file. A fraud alert notifies creditors that they must contact you before they open any new accounts or make changes to your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You may renew it after 90 days. Additional information is available at <http://www.annualcreditreport.com>. For more information regarding what you can do, see the "Further Information and Steps You Should Take" guidance attached to this letter.

FOR MORE INFORMATION:

We value your privacy and deeply regret that this breach occurred. We value you as an employee and appreciate the trust you place in **Personal Touch Home-Aides, Inc. C/O Personal Touch Holding Corp.**. Please know that we remain committed to your privacy. For further information and assistance please contact us at our toll free number 877-644-1116 between the hours of 6:00 a.m. and 6:00 p.m. PST, Monday to Friday; 8:00 a.m. and 5:00 p.m. Saturday and Sunday or by e-mail to EmployeeQuestions@PTHomecare.com.

Sincerely,

Personal Touch Home-Aides, Inc. C/O Personal Touch Holding Corp.



By:

Name: Robert Caione

Title: Chief Executive Officer

FURTHER INFORMATION AND STEPS YOU CAN TAKE

We recommend that you remain vigilant for an incident of fraudulent activity and/or identify theft by monitoring your account statements and free credit monitoring reports closely. We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

You can also elect to purchase a copy of your credit report by contacting one of the three national credit-reporting agencies. Contact information for the three national credit-reporting agencies for requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

The FTC also suggests that you request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically.

In some states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

If you believe you are the victim of identity theft, you should contact your local law enforcement, Attorney General's Office and/or the Federal Trade Commission. You can file a report or obtain a report from your local law enforcement. You can also obtain from these sources more information about steps that you can take to avoid identify theft and information about fraud alerts and security freezes. Contact information for the Federal Trade Commission is Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT(1-877-438-4338), <https://www.ftc.gov/> or <http://www.ftc.gov/idtheft>.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.



Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400. You also have the right to file or obtain a police report regarding this incident. Approximately fifteen (15) Rhode Island residents were affected in this breach.

New Mexico residents, in addition to the rights set forth above, you have additional rights under the Fair Credit Reporting and Identity Security Act (NMSA 1978, § 56-3A-1).

Massachusetts residents have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

ADDITIONAL DETAILS REGARDING YOUR 12-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.

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 **877-644-1116**. 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 one year 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. You will also find self-help tips and information about identity protection at this site.

Personal Touch Home Care of Greater Portsmouth, Inc.
C/O Personal Touch Holding Corp.
1985 Marcus Avenue, Ste 202
Lake Success, NY 11042
718-736-7233

January 28, 2020



F2790-L01-0000010 P001 T00002 *****MIXED AADC 159
SAMPLE A SAMPLE - L01_PTPATIENTS_MAJORITY
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A Sample:

Personal Touch Home Care of Greater Portsmouth, Inc. C/O Personal Touch Holding Corp., (the “Covered Entity”) is hereby providing you with a notification regarding a breach that may have affected your protected health information and other personally identifiable information.

WHAT HAPPENED:

On December 1, 2019, the Covered Entity was notified by its cloud-hosting provider, Crossroads Technologies Inc., that there was a breach at its Pennsylvania data center, where the Covered Entity’s electronic medical records are hosted. Crossroads Technologies, Inc. has reported to us that it was the victim of a ransomware attack and that it is investigating the extent of the breach. Although we cannot confirm the extent to which your data was compromised, we are notifying you that the breach occurred, in our efforts to comply with the Health Information Portability and Accountability Act (“HIPAA”).

WHAT INFORMATION WAS INVOLVED:

Crossroads Technologies, Inc. hosts an electronic medical record system that contains your protected health information and personally identifiable information. This information includes medical treatment information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, and Social Security number. At this time, we cannot confirm to what extent your information was compromised.

WHAT WE ARE DOING:

Upon being notified of a security incident at Crossroads Technologies, Inc., we immediately began working with and corresponding with Crossroads Technologies, Inc. to stay updated regarding the investigation. During the course of the investigation, Crossroads Technologies, Inc. notified us that they were working with third-party forensic analysts and the Federal Bureau of Investigations to determine the origins and scope of the breach.

0000010



F2790-L01

Pursuant to applicable law, we will be notifying the U.S. Department of Health and Human Services, Office of Civil Rights ("OCR"), which is responsible for enforcing the HIPAA Privacy and Security Rules. We will fully comply with OCR to meet requirements of the HIPAA Breach Notification Rule, which requires that patients be notified and will cooperate with regard to any further inquiry they may have. We will also be notifying state regulators as required by law.

WHAT YOU CAN DO:

As recommended by the Federal Trade Commission ("FTC"), we recommend that you remain vigilant and monitor your account statements, explanation of benefits, and credit bureau reports closely. The FTC also recommends you place a fraud alert on your credit file. A fraud alert notifies creditors that they must contact you before they open any new accounts or make changes to your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You may renew it after 90 days. Additional information is available at <http://www.annualcreditreport.com>. For more information regarding what you can do, see the "Further Information and Steps You Should Take" guidance attached to this letter.

FOR MORE INFORMATION:

We value your privacy and deeply regret that this incident occurred. We value you as a patient and appreciate the trust you place in **Personal Touch Home Care of Greater Portsmouth, Inc. C/O Personal Touch Holding Corp.** Please know that we remain committed to your privacy. For further information and assistance please contact us at our toll free number 866-904-6220 between the hours of 6:00 a.m. and 6:00 p.m. PST, Monday to Friday; 8:00 a.m. and 5:00 p.m. Saturday and Sunday [engagement number: **DB17560**] or by e-mail to PatientQuestions@PTHomecare.com.

Sincerely,

Personal Touch Home Care of Greater Portsmouth, Inc. C/O Personal Touch Holding Corp.



By:

Name: Robert Caione

Title: Chief Executive Officer

FURTHER INFORMATION AND STEPS YOU CAN TAKE

We recommend that you remain vigilant for an incident of fraudulent activity and/or identify theft by monitoring your account statements, explanation of benefits, and free credit monitoring reports closely. We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

You can also elect to purchase a copy of your credit report by contacting one of the three national credit-reporting agencies. Contact information for the three national credit-reporting agencies for requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

The FTC also suggests that you request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically.

In some states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

If you believe you are the victim of identity theft, you should contact your local law enforcement, Attorney General's Office and/or the Federal Trade Commission. You can file a report or obtain a report from your local law enforcement. You can also obtain from these sources more information about steps that you can take to avoid identify theft and information about fraud alerts and security freezes. Contact information for the Federal Trade Commission is Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT(1-877-438-4338), <http://www.ftc.gov/> or <http://www.ftc.gov/idtheft>.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

0000010



North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400. You also have the right to file or obtain a police report regarding this incident. Approximately fifteen (15) Rhode Island residents were affected in this breach.

New Mexico residents, in addition to the rights set forth above, you have additional rights under the Fair Credit Reporting and Identity Security Act (NMSA 1978, § 56-3A-1).

Massachusetts residents have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Personal Touch Home Care of Greater Portsmouth, Inc.
C/O Personal Touch Holding Corp.
1985 Marcus Avenue, Suite 202
Lake Success, NY 111042
718-736-7233

January 28, 2020



F2790-L03-0000008 P001 T00002 *****MIXED AADC 159
SAMPLE A SAMPLE - L03_PTEMPLOYEES_MAJORITY
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A Sample:

Personal Touch Home Care of Greater Portsmouth, Inc. C/O Personal Touch Holding Corp., (the “Company”) is hereby providing you with a notification regarding a breach that may have affected your personally identifiable information.

WHAT HAPPENED:

On December 1, 2019, the Company was notified by its cloud-hosting provider, Crossroads Technologies Inc., that there was a breach at its Pennsylvania data center, where the Company’s electronic medical records are hosted. Crossroads Technologies, Inc. has reported to us that it was the victim of a ransomware attack and that it is investigating the extent of the breach. Although we cannot confirm the extent to which your data was compromised, we are notifying you that the breach occurred, in our efforts to comply with the applicable state data breach notification laws.

WHAT INFORMATION WAS INVOLVED:

Crossroads Technologies, Inc. hosts an electronic medical record system that contains personally identifiable information relating to your work as an employee of this Company. This information includes first and last name, address, telephone numbers, date of birth, Social Security number, clinical licensing number, driver’s license number, and basic financial information such as I-9s and tax codes. At this time, we cannot confirm to what extent your information was compromised.

WHAT WE ARE DOING:

Upon being notified of a security incident at Crossroads Technologies, Inc., we immediately began working with and corresponding with Crossroads Technologies to stay updated regarding the investigation. During the course of the investigation, Crossroads Technologies, Inc. notified us that they were working with third-party forensic analysts and the Federal Bureau of Investigations to determine the origins and scope of the breach. Pursuant to applicable law, we will be notifying state regulators as required.



To help protect your identity, we are offering a complimentary one- year membership of Experian's® IdentityWorksSM. 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: 5.31.2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: 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 **877-644-1116** by **5.31.2020**. Be prepared to provide engagement number **DB17313** as proof of eligibility for the identity restoration services by Experian.

WHAT YOU CAN DO:

As recommended by the Federal Trade Commission ("FTC"), we recommend that you remain vigilant and monitor your account statements and credit bureau reports closely. The FTC also recommends you place a fraud alert on your credit file. A fraud alert notifies creditors that they must contact you before they open any new accounts or make changes to your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You may renew it after 90 days. Additional information is available at <http://www.annualcreditreport.com>. For more information regarding what you can do, see the "Further Information and Steps You Should Take" guidance attached to this letter.

FOR MORE INFORMATION:

We value your privacy and deeply regret that this breach occurred. We value you as an employee and appreciate the trust you place in **Personal Touch Home Care of Greater Portsmouth, Inc. C/O Personal Touch Holding Corp.** Please know that we remain committed to your privacy. For further information and assistance please contact us at our toll free number 877-644-1116 between the hours of 6:00 a.m. and 6:00 p.m. PST, Monday to Friday; 8:00 a.m. and 5:00 p.m. Saturday and Sunday or by e-mail to EmployeeQuestions@PTHomecare.com.

Sincerely,

Personal Touch Home Care of Greater Portsmouth, Inc. C/O Personal Touch Holding Corp.



By:

Name: Robert Caione

Title: Chief Executive Officer

FURTHER INFORMATION AND STEPS YOU CAN TAKE

We recommend that you remain vigilant for an incident of fraudulent activity and/or identify theft by monitoring your account statements and free credit monitoring reports closely. We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

You can also elect to purchase a copy of your credit report by contacting one of the three national credit-reporting agencies. Contact information for the three national credit-reporting agencies for requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

The FTC also suggests that you request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically.

In some states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

If you believe you are the victim of identity theft, you should contact your local law enforcement, Attorney General's Office and/or the Federal Trade Commission. You can file a report or obtain a report from your local law enforcement. You can also obtain from these sources more information about steps that you can take to avoid identity theft and information about fraud alerts and security freezes. Contact information for the Federal Trade Commission is Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT(1-877-438-4338), <https://www.ftc.gov/> or <http://www.ftc.gov/idtheft>.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.



Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400. You also have the right to file or obtain a police report regarding this incident. Approximately fifteen (15) Rhode Island residents were affected in this breach.

New Mexico residents, in addition to the rights set forth above, you have additional rights under the Fair Credit Reporting and Identity Security Act (NMSA 1978, § 56-3A-1).

Massachusetts residents have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

ADDITIONAL DETAILS REGARDING YOUR 12-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.

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 **877-644-1116**. 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 one year 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. You will also find self-help tips and information about identity protection at this site.

Personal Touch Home Care of Ohio, Inc.
C/O Personal Touch Holding Corp.
1985 Marcus Avenue, Ste 202
Lake Success, NY 11042
718-736-7233

January 28, 2020



F2790-L01-0000015 P001 T00002 *****MIXED AADC 159
SAMPLE A SAMPLE - L01_PTPATIENTS_MAJORITY
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A Sample:

Personal Touch Home Care of Ohio, Inc. C/O Personal Touch Holding Corp., (the “Covered Entity”) is hereby providing you with a notification regarding a breach that may have affected your protected health information and other personally identifiable information.

WHAT HAPPENED:

On December 1, 2019, the Covered Entity was notified by its cloud-hosting provider, Crossroads Technologies Inc., that there was a breach at its Pennsylvania data center, where the Covered Entity’s electronic medical records are hosted. Crossroads Technologies, Inc. has reported to us that it was the victim of a ransomware attack and that it is investigating the extent of the breach. Although we cannot confirm the extent to which your data was compromised, we are notifying you that the breach occurred, in our efforts to comply with the Health Information Portability and Accountability Act (“HIPAA”).

WHAT INFORMATION WAS INVOLVED:

Crossroads Technologies, Inc. hosts an electronic medical record system that contains your protected health information and personally identifiable information. This information includes medical treatment information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, and Social Security number. At this time, we cannot confirm to what extent your information was compromised.

WHAT WE ARE DOING:

Upon being notified of a security incident at Crossroads Technologies, Inc., we immediately began working with and corresponding with Crossroads Technologies, Inc. to stay updated regarding the investigation. During the course of the investigation, Crossroads Technologies, Inc. notified us that they were working with third-party forensic analysts and the Federal Bureau of Investigations to determine the origins and scope of the breach.

0000015



F2790-L01

Pursuant to applicable law, we will be notifying the U.S. Department of Health and Human Services, Office of Civil Rights ("OCR"), which is responsible for enforcing the HIPAA Privacy and Security Rules. We will fully comply with OCR to meet requirements of the HIPAA Breach Notification Rule, which requires that patients be notified and will cooperate with regard to any further inquiry they may have. We will also be notifying state regulators as required by law.

WHAT YOU CAN DO:

As recommended by the Federal Trade Commission ("FTC"), we recommend that you remain vigilant and monitor your account statements, explanation of benefits, and credit bureau reports closely. The FTC also recommends you place a fraud alert on your credit file. A fraud alert notifies creditors that they must contact you before they open any new accounts or make changes to your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You may renew it after 90 days. Additional information is available at <http://www.annualcreditreport.com>. For more information regarding what you can do, see the "Further Information and Steps You Should Take" guidance attached to this letter.

FOR MORE INFORMATION:

We value your privacy and deeply regret that this incident occurred. We value you as a patient and appreciate the trust you place in **Personal Touch Home Care of Ohio, Inc. C/O Personal Touch Holding Corp.** Please know that we remain committed to your privacy. For further information and assistance please contact us at our toll free number 866-904-6220 between the hours of 6:00 a.m. and 6:00 p.m. PST, Monday to Friday; 8:00 a.m. and 5:00 p.m. Saturday and Sunday [engagement number: **DB17560**] or by e-mail to PatientQuestions@PTHomecare.com.

Sincerely,

Personal Touch Home Care of Ohio, Inc. C/O Personal Touch Holding Corp.



By:

Name: Robert Caione

Title: Chief Executive Officer

FURTHER INFORMATION AND STEPS YOU CAN TAKE

We recommend that you remain vigilant for an incident of fraudulent activity and/or identify theft by monitoring your account statements, explanation of benefits, and free credit monitoring reports closely. We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

You can also elect to purchase a copy of your credit report by contacting one of the three national credit-reporting agencies. Contact information for the three national credit-reporting agencies for requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

The FTC also suggests that you request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically.

In some states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

If you believe you are the victim of identity theft, you should contact your local law enforcement, Attorney General's Office and/or the Federal Trade Commission. You can file a report or obtain a report from your local law enforcement. You can also obtain from these sources more information about steps that you can take to avoid identify theft and information about fraud alerts and security freezes. Contact information for the Federal Trade Commission is Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT(1-877-438-4338), <https://www.ftc.gov/> or <http://www.ftc.gov/idtheft>.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.



North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400. You also have the right to file or obtain a police report regarding this incident. Approximately fifteen (15) Rhode Island residents were affected in this breach.

New Mexico residents, in addition to the rights set forth above, you have additional rights under the Fair Credit Reporting and Identity Security Act (NMSA 1978, § 56-3A-1).

Massachusetts residents have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.