



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>> <<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Select Health Network (“Select Health”) is writing to inform you of a recent event that may impact the privacy of some of your information. Select Health provides the provider network to M-Plan, Advantage Health Solutions, or another current or former health plan that provided coverage to you. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** Select Health recently concluded its investigation into unusual activity related to an employee email account. Upon learning of the suspicious activity, we immediately took steps to secure the email account and began working with third-party forensic experts to determine the nature and scope of the incident. The investigation confirmed that the Select Health employee email account was accessed by an unknown actor from May 22, 2019 to June 13, 2019.

The investigation was unable to determine with forensic certainty what emails, if any, were accessed by the unauthorized actor. In an abundance of caution, we worked with experts to perform a comprehensive review of all information stored in the email account at the time of incident to confirm the identities of the individuals whose information may have been accessible to the unauthorized actor. On October 1, 2019, we received the results of the third-party audit. We immediately began reviewing the results of the audit to determine the identities and contact information for potentially impacted individuals.

**What Information Was Involved?** On November 1, 2019, we determined the following types of information relating to you were present in the email account and accessible to the unknown actor during this incident: name, <<insert variable field>>. There is no evidence this information was misused by the unknown actor and Select Health is providing this notice in an abundance of caution.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to secure the affected email account. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state and federal regulators, as required. While we are unaware of any misuse of your information as a result of this incident, we are offering you access to 12 months of credit monitoring and identity restoration services through TransUnion.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Prevent Fraud and Identity Theft*. We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit [www.annualcreditreport.com](http://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 their credit report.

**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 833-935-1364, Monday through Friday, during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to the Select Health Network at P.O. Box 6249, South Bend, IN 46660.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

A handwritten signature in cursive script that reads "Candace Jones".

Candace Jones  
Chief Executive Officer  
Select Health Network

## **STEPS YOU CAN TAKE TO PREVENT FRAUD AND IDENTITY THEFT**

### **Complimentary One-Year *myTrueIdentity* Credit Monitoring Service**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

#### **How to Enroll: You can sign up online or via U.S. mail delivery.**

- To enroll in this service, go to the *myTrueIdentity* website at [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

#### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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](http://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.

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**  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/  
center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/  
credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
[www.equifax.com/personal/  
credit-report-services](http://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**  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

To monitor for actual or attempted misuse of Social Security benefits, you can create an account at <https://www.socialsecurity.gov/myaccount>. If you see an error or attempted misuse of Social Security benefits, you can go to your local Social Security Office for assistance. Local offices can be found using the following office locator - <https://secure.ssa.gov/ICON/main.jsp>.

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](http://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 Maryland residents:** The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).

**For North Carolina residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**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/>.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Select Health Network (“Select Health”) is writing to inform you of a recent event that may impact the privacy of some of your information. Select Health provides the provider network to M-Plan, Advantage Health Solutions, or another current or former health plan that provided coverage to you. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** Select Health recently concluded its investigation into unusual activity related to an employee email account. Upon learning of the suspicious activity, we immediately took steps to secure the email account and began working with third-party forensic experts to determine the nature and scope of the incident. The investigation confirmed that the Select Health employee email account was accessed by an unknown actor from May 22, 2019 to June 13, 2019.

The investigation was unable to determine with forensic certainty what emails, if any, were accessed by the unauthorized actor. In an abundance of caution, we worked with experts to perform a comprehensive review of all information stored in the email account at the time of incident to confirm the identities of the individuals whose information may have been accessible to the unauthorized actor. On October 1, 2019, we received the results of the third-party audit. We immediately began reviewing the results of the audit to determine the identities and contact information for potentially impacted individuals.

**What Information Was Involved?** On November 1, 2019, we determined the following types of information relating to you were present in the email account and accessible to the unknown actor during this incident: <<insert variable field>>. There is no evidence this information was misused by the unknown actor and Select Health is providing this notice in an abundance of caution.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to secure the affected email account. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state and federal regulators, as required.

While we are unaware of any misuse of your information as a result of this incident, we have arranged for access to an identity restoration program for 1 year, at no cost to you, from TransUnion, which provides assistance in the event your identity is compromised to help you restore your identity. The identity restoration assistance is available to you through February 28, 2021, with no enrollment required. If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code **697984** to speak to a dedicated TransUnion representative about your identity theft issue.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Prevent Fraud and Identity Theft*. We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit [www.annualcreditreport.com](http://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 their credit report.

**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 833-935-1364, Monday through Friday, during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to the Select Health Network at P.O. Box 6249, South Bend, IN 46660.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

A handwritten signature in cursive script that reads "Candace Jones".

Candace Jones  
Chief Executive Officer  
Select Health Network

## **STEPS YOU CAN TAKE TO PREVENT FRAUD AND IDENTITY THEFT**

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](http://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.

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**  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/  
center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/  
credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
[www.equifax.com/personal/  
credit-report-services](http://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**  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/  
center.html](http://www.experian.com/fraud/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/  
fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/  
credit-report-services](http://www.equifax.com/personal/credit-report-services)

To monitor for actual or attempted misuse of Social Security benefits, you can create an account at <https://www.socialsecurity.gov/myaccount>. If you see an error or attempted misuse of Social Security benefits, you can go to your local Social Security Office for assistance. Local offices can be found using the following office locator - <https://secure.ssa.gov/ICON/main.jsp>.

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](http://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 Maryland residents:** The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).

**For North Carolina residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**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/>.