New Jersey Department of Human Services
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07483B 1-1

State of New Jersey
DEPARTMENT OF HUMAN SERVICES
DIVISION OF MEDICAL ASSISTANCE AND HEALTH SERVICES
PO BOX 712
TRENTON, NJ 08625-0712

[redacted]

July 10, 2023

Dear [redacted]:

We are writing to share important information regarding a data security incident that potentially involved your personal information and protected health information ("PHI"). The privacy and security of your information are important to us, and we are taking the appropriate steps to respond to the incident. At this time, we do not have any indication that your information has been misused. Out of an abundance of caution, we are providing you with information, as well as access to resources, so that you can better protect your personal information and PHI.

What Happened:

We recently discovered that the New Jersey Department of Human Services ("NJDHS"), Division of Medical Assistance and Health Services ("DMAHS" or "Medicaid"), experienced a data security incident, which resulted in the potential exposure of personal information and PHI. The incident was first discovered on March 17, 2023, when we received an alert that an applicant for Medicaid benefits was able to find personal information in search engine results for the individual's name. Specifically, the individual found their Asset Verification System report ("AVS report"), which is generated during the process of applying for Medicaid benefits. In response to this alert, DMAHS immediately cleared the document from the search engine, conducted an internal investigation, and patched the system error that allowed the information to be publicly available in search engine results. In addition, NJDHS engaged third-party experts, including forensic investigators, to investigate the scope of the incident and assist with response and remediation activities as appropriate. Through this investigation, NJDHS discovered that limited AVS reports, applications for Medicaid benefits, or confirmation of such applications (collectively, "Medicaid Application Documents") for certain other individuals applying for Medicaid benefits were publicly available through certain search engines. This information has since been cleared from these search engines.

You are receiving this notification because on or about June 12, 2023 at least one of your Medicaid Application Documents was identified as being among the information that was available on certain search engines. We do not have reason to believe that your information was used inappropriately. **However, because we are committed to protecting your personal information, we are providing you this notice, in an abundance of caution, so that you may diligently monitor your accounts.**

What Information was Involved:

The type of personal information and PHI contained on the Medicaid Application Documents may include your name and one or more of the following types of information:

- Address;
- Date of birth;
- Telephone number;

- Email address;
- Social Security number;
- Bank account information including account number(s) and balance(s);
- Health insurance information;
- Health history; and/or
- Medical record number.

What DMAHS is Doing:

The confidentiality of your personal information and PHI is one of DMAHS's top priorities. Immediately upon learning of the incident, we took steps to contain the incident and conduct a thorough investigation. The third-party information technology firm we retained also assisted in the remediation of our system, and implementation of additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While DMAHS is not aware of any identity fraud or improper use of any personal information or PHI directly resulting from this incident, we have arranged to have Cyberscout, a TransUnion company, provide you with twenty-four (24) months of complimentary credit monitoring services through Identity Force and identity theft insurance should you want such services. To activate your membership in these services, please follow the steps outlined at the end of this letter.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, including steps you can take to protect yourself against fraud and identity theft.

For More Information:

If you have any questions about this notice or the incident, please telephone the Cyberscout call center at 1-800-405-6108 from 8:00 am to 8:00 pm ET, Monday through Friday. The call center will be available for ninety (90) days from the date of this letter to assist you.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,

Charles B. Castillo

Charles B. Castillo
Privacy Officer, DMAHS

Credit Monitoring Services

In response to the network security incident, NJDHS has arranged for Cyberscout to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score*;
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

Representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm ET, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

How Do I Enroll for the Free Services?

To register your account and activate your services type the following URL into your browser: [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

Important – you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

* Services marked with an "*" require 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.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

Information on Obtaining a Free Credit Report:

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

Information on Implementing a Fraud Alert, Credit Freeze, or Credit Lock:

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

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, 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.); and

7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charge monthly fees.

Additional Resources

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

New Jersey Department of Human Services
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07483B 1-1

State of New Jersey
DEPARTMENT OF HUMAN SERVICES
DIVISION OF MEDICAL ASSISTANCE AND HEALTH SERVICES
PO BOX 712
TRENTON, NJ 08625-0712

[redacted]

July 10, 2023

Dear [redacted]:

We are writing to share important information regarding a data security incident that potentially involved your personal information and protected health information ("PHI"). The privacy and security of your information are important to us, and we are taking the appropriate steps to respond to the incident. At this time, we do not have any indication that your information has been misused. Out of an abundance of caution, we are providing you with information, as well as access to resources, so that you can better protect your personal information and PHI.

What Happened:

We recently discovered that the New Jersey Department of Human Services ("NJDHS"), Division of Medical Assistance and Health Services ("DMAHS" or "Medicaid"), experienced a data security incident, which resulted in the potential exposure of personal information and PHI. The incident was first discovered on March 17, 2023, when we received an alert that an applicant for Medicaid benefits was able to find personal information in search engine results for the individual's name. Specifically, the individual found their Asset Verification System report ("AVS report"), which is generated during the process of applying for Medicaid benefits. In response to this alert, DMAHS immediately cleared the document from the search engine, conducted an internal investigation, and patched the system error that allowed the information to be publicly available in search engine results. In addition, NJDHS engaged third-party experts, including forensic investigators, to investigate the scope of the incident and assist with response and remediation activities as appropriate. Through this investigation, NJDHS discovered that limited AVS reports, applications for Medicaid benefits, or confirmation of such applications (collectively, "Medicaid Application Documents") for certain other individuals applying for Medicaid benefits were publicly available through certain search engines. This information has since been cleared from these search engines.

You are receiving this notification because on or about June 12, 2023 at least one of your Medicaid Application Documents was identified as being among the information that was available on certain search engines. We do not have reason to believe that your information was used inappropriately. **However, because we are committed to protecting your personal information, we are providing you this notice, in an abundance of caution, so that you may diligently monitor your accounts.**

What Information was Involved:

The type of personal information and PHI contained on the Medicaid Application Documents may include your name and one or more of the following types of information:

- Address;
- Date of birth;
- Telephone number;

- Email address;
- Social Security number;
- Bank account information including account number(s) and balance(s);
- Health insurance information;
- Health history; and/or
- Medical record number.

What DMAHS is Doing:

The confidentiality of your personal information and PHI is one of DMAHS's top priorities. Immediately upon learning of the incident, we took steps to contain the incident and conduct a thorough investigation. The third-party information technology firm we retained also assisted in the remediation of our system, and implementation of additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While DMAHS is not aware of any identity fraud or improper use of any personal information or PHI directly resulting from this incident, we have arranged to have Cyberscout, a TransUnion company, provide you with twenty-four (24) months of complimentary credit monitoring services through Identity Force and identity theft insurance should you want such services. To activate your membership in these services, please follow the steps outlined at the end of this letter.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, including steps you can take to protect yourself against fraud and identity theft.

For More Information:

If you have any questions about this notice or the incident, please telephone the Cyberscout call center at 1-800-405-6108 from 8:00 am to 8:00 pm ET, Monday through Friday. The call center will be available for ninety (90) days from the date of this letter to assist you.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,

Charles B. Castillo

Charles B. Castillo
Privacy Officer, DMAHS

Credit Monitoring Services

In response to the network security incident, NJDHS has arranged for Cyberscout to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score*;
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

Representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm ET, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

How Do I Enroll for the Free Services?

To register your account and activate your services type the following URL into your browser: [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted].

Important – you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

* Services marked with an "*" require 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.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

Information on Obtaining a Free Credit Report:

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

Information on Implementing a Fraud Alert, Credit Freeze, or Credit Lock:

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

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, 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.); and

7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charge monthly fees.

Additional Resources

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.