Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<Variable Data 1>>

Dear <<Full Name>>:

The security of your information is important, and we are writing to notify you about a recent incident that may have impacted your information. We are sending you this letter to let you know what happened, what information may be involved, the response, and what steps you can take to protect your information. We sincerely regret any concern this incident may cause you.

What happened? On November 19, 2024, we became aware of a cybersecurity incident that led to unauthorized access to certain computer systems beginning on October 11, 2024. The impacted systems were being hosted by a third-party service provider and contained Allegheny Health Network ("AHN") Home Medical Equipment and Home Infusion patient information, and an unauthorized user was able to obtain some data from these systems, which may include your information. Once discovered, immediate steps were taken to begin an investigation, secure patient information, and stop the unauthorized access to the systems.

What information was involved? The information on the impacted systems that may have been involved includes your name, date of birth, address, Social Security number, financial account number provided to AHN on paper (but no access codes), health insurance identification number and other health insurance information, and treatment information including your diagnoses, provider's information, treatments/procedures, date(s) of service, prescription information, and medical device serial number, as applicable. We are not aware of any actual or attempted identity theft or fraud as a result of this incident.

What are we doing? Multiple corrective actions to respond to the incident and to help ensure an incident like this does not happen again have been taken. In addition to terminating the unauthorized access to the systems, including immediately taking the affected systems offline, connections to other systems were turned off to prevent additional unauthorized access. In addition, law enforcement was notified and we are notifying you so that you may take further steps to protect yourself, should you feel it appropriate to do so.

As an additional step, you are being offered complimentary credit monitoring and identity protection services.

What you can do. As a precaution, we encourage you to remain vigilant against the potential for identity theft and fraud and to monitor your accounts, medical bills, and credit reports for any suspicious activity. Please see the enclosed information on steps you can take to protect your information. You will also find instructions on how to enroll in the complimentary credit monitoring and identity protection services being made available to you.

For more information. If you have any questions or concerns regarding this or any matter relating to the privacy of your information, please do not hesitate to contact the dedicated assistance line toll-free at 888-753-5582 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time.

ADDITIONAL INFORMATION

Enroll in Monitoring Services

Identity Defense

<<Name 1>>
Enter your Activation Code: <<ActivationCode>>
Enrollment Deadline: <<Deadline>>
Service Term: <<CM Duration>>*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

1. **Enrollment Instructions**

To enroll in Identity Defense, visit <<URL>>

Enter your unique Activation Code <<Code>>

Enter your Activation Code and click 'Redeem Code'.

1. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
2. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
3. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Deadline>>. After <<Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and www.ncdoj.gov.

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
Parent or Guardian of
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<Variable Data 1>>

Dear Parent or Guardian of <<Full Name>>:

The security of your information is important, and we are writing to notify you about a recent incident that may have impacted your minor child's information. We are sending you this letter to let you know what happened, what information may be involved, the response, and what steps you can take to protect your minor child's information. We sincerely regret any concern this incident may cause you.

What happened? On November 19, 2024, we became aware of a cybersecurity incident that led to unauthorized access to certain computer systems beginning on October 11, 2024. The impacted systems were being hosted by a third-party service provider and contained Allegheny Health Network ("AHN") Home Medical Equipment and Home Infusion patient information, and an unauthorized user was able to obtain some data from these systems, which may include your information. Once discovered, immediate steps were taken to begin an investigation, secure patient information, and stop the unauthorized access to the systems.

What information was involved? The information on the impacted systems that may have been involved includes your minor child's name, date of birth, address, Social Security number, financial account number provided to AHN on paper (but no access codes), health insurance identification number and other health insurance information, and treatment information including your diagnoses, provider's information, treatments/procedures, date(s) of service, prescription information, and medical device serial number, as applicable. We are not aware of any actual or attempted identity theft or fraud as a result of this incident.

What are we doing? Multiple corrective actions to respond to the incident and to help ensure an incident like this does not happen again have been taken. In addition to terminating the unauthorized access to the systems, including immediately taking the affected systems offline, connections to other systems were turned off to prevent additional unauthorized access. In addition, law enforcement was notified and we are notifying you so that you may take further steps to protect yourself, should you feel it appropriate to do so.

As an additional step, your minor child is being offered complimentary identity protection services.

What you can do. As a precaution, we encourage you to remain vigilant against the potential for identity theft and fraud and to monitor your minor child's accounts and medical bills for any suspicious activity. Please see the enclosed information on steps you can take to protect your information. You will also find instructions on how to enroll your minor child in the complimentary identity protection services.

For more information. If you have any questions or concerns regarding this or any matter relating to the privacy of your information, please do not hesitate to contact the dedicated assistance line toll-free at 888-753-5582 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time.

ADDITIONAL INFORMATION

Enroll in Monitoring Services

Minor Defense

<<Name 1>>
Enter your Activation Code: **<<ActivationCode>>**
Enrollment Deadline: **<<Deadline>>**
Service Term: **<<CM Duration>>***

Key Features

- Synthetic Identity Monitoring
- Public Record Trace
- Dark Web Monitoring
- Parent/Custodial Adult Controls
- Victim Assistance

Enrollment Instructions

To enroll in Minor Defense, visit <<URL>>

1. Enter your unique Activation Code <<MinorDefenseID>>
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is **<<Deadline>>**. After **<<Deadline>>**, the enrollment process will close, and your Minor Defense code will no longer be active. If you do not enroll by **<<Deadline>>**, you will not be able to take advantage of Minor Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Minor Defense, please call Minor Defense directly at 866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

Monitor Minor Child Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established.

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

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above.

Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and www.ncdoj.gov.