Notice to Adult Patients/Guarantors

OH Muhlenberg, LLC

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

<<mail id>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>,

At OH Muhlenberg, LLC, the privacy and security of our patients' information is a top priority. On July 1, 2015, OH Muhlenberg, LLC acquired the hospital operations of Muhlenberg Community Hospital. Prior to that time, the Muhlenberg hospital had been owned and operated by Muhlenberg Community Hospital since 1938. As part of the acquisition, OH Muhlenberg, LLC acquired substantially all of the assets of Muhlenberg Community Hospital, including its computer systems, patient records and other records. Regrettably, we are writing to inform you of a security incident involving some of that information. As a result, we are providing this notice to you whether or not you were a patient prior to July 1, 2015, and whether or not particular data was transmitted prior to that date.

On September 16, 2015, the FBI notified the Hospital of suspicious network activity involving third parties. Upon learning this information, we took immediate action, including initiating an internal investigation, and we also engaged a leading forensic IT firm to investigate this matter. Based upon this review, we have confirmed that a limited number of computers were infected with a keystroke logger designed to capture and transmit data as it was entered onto the affected computers. The infection may have started as early as January 2012.

The affected computers were used to enter patient financial data and health information and information about persons responsible for a patient's bill, including potentially your name, address, telephone number(s), birthdate, Social Security number, driver's license/state identification number, medical and health plan information (such as your health insurance number, medical record number, diagnoses and treatment information, and payment information), financial account number, and payment card information (such as primary account number and expiration date).

The Hospital is committed to maintaining the privacy of its patients and takes precautions for the security of personal and medical information. Upon learning of the incident, the Hospital took prompt steps to address and contain it, including immediately blocking the external unauthorized IP addresses, as well as taking steps to disable the malware. The Hospital continues to enhance the security of its systems and is working with the FBI during its investigation.

While we have no indication that the data has been used inappropriately, out of an abundance of caution, we are providing this notice to individuals whose information was maintained in the Hospital's electronic patient records database, as well as to persons employed by or contracted for specific services by the Hospital on and after January 1, 2012. We want to make you aware of steps you can take to guard against possible identity theft or fraud:

- **Enroll in Experian's ProtectMyID® Alert.** We are offering you a complimentary one-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you, and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**
- **Explanation of Benefits Review.** We also recommend that you regularly review the explanation of benefits statements that you receive from your insurer or that you receive or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits forms that were not received, please immediately contact the insurer.

- **Check Credit Reports.** We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.
- **Review Payment Card Statements.** We also recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued your credit or debit card immediately.
- **Consult the Identity Theft Protection Guide.** Please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

Again, as of the date of this letter, we have no indication that any data has been used inappropriately. If you have questions or would like any additional information about this incident, we have established a call center to answer your questions. The call center is open 9 a.m.-9 p.m. EST and may be reached at 877-271-1568 from anywhere within the United States or at 503-520-4450 from outside the United States (tolls may apply). We sincerely regret any inconvenience this incident presents to you.

Sincerely,

DeAnn Tucker

DeAnn Tucker, RHIA, CHPS, CCS
Director of Privacy & Security
OH MUHLENBERG, LLC

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That **You Enroll By: February 18, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC97585.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARETM, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8057 to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. 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.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Credit Freezes for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
Fraud Alerts: P.O. Box 105069, Atlanta, GA 30348
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes: P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228
Fraud Alerts and Security Freezes: P.O. Box 2000, Chester, PA 19022
888-909-8872

OH Muhlenberg, LLC

Deceased Patient/Guarantor Notice

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

<<mail id>>
Next of Kin of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear Next of Kin of <<First Name>> <<Last Name>>,

At OH Muhlenberg, LLC, the privacy and security of our patients' information is a top priority. On July 1, 2015, OH Muhlenberg, LLC acquired the hospital operations of Muhlenberg Community Hospital. Prior to that time, the Muhlenberg hospital had been owned and operated by Muhlenberg Community Hospital since 1938. As part of the acquisition, OH Muhlenberg, LLC acquired substantially all of the assets of Muhlenberg Community Hospital, including its computer systems, patient records and other records. Regrettably, we are writing to inform you of a security incident involving some of that information. As a result, we are providing this notice whether or not the decedent was a patient prior to July 1, 2015, and whether or not particular data relating to the decedent was transmitted prior to that date.

On September 16, 2015, the FBI notified the Hospital of suspicious network activity involving third parties. Upon learning this information, we took immediate action, including initiating an internal investigation, and we also engaged a leading forensic IT firm to investigate this matter. Based upon this review, we have confirmed that a limited number of computers were infected with a keystroke logger designed to capture and transmit data as it was entered onto the affected computers. The infection may have started as early as January 2012.

The affected computers were used to enter patient financial data and health information and information about persons responsible for a patient's bill, including potentially information about the decedent. The type of information affected could include name, address, telephone number(s), birthdate, Social Security number, driver's license/state identification number, medical and health plan information (such as health insurance number, medical record number, diagnoses and treatment information, and payment information), financial account number, and payment card information (such as primary account number and expiration date).

Please note that we have no indication that the data has been used inappropriately. However, out of an abundance of caution, we are providing this notice regarding individuals whose information was maintained in the Hospital's electronic patient records database.

The Hospital is committed to maintaining the privacy of its patients and takes precautions for the security of personal and medical information. Upon learning of the incident, the Hospital took prompt steps to address and contain it, including immediately blocking the external unauthorized IP addresses, as well as taking steps to disable the malware. The Hospital continues to enhance the security of its systems and is working with the FBI during its investigation.

We want to make you aware of steps you can take to guard against possible identity theft or fraud:

- **Check Credit Reports.** We recommend that you carefully check credit reports for accounts or inquiries you do not recognize. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on the credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up credit records. If you have not already done so, you can contact the National Credit Reporting Agencies to notify them of the decedent's passing and to request that a notation be added to the credit file.
- **Explanation of Benefits Review.** We also recommend that you regularly review the explanation of benefits statements that you receive or review for persons whose medical bills you assist with or pay. If you identify services listed on the explanation of benefits forms that were not received, please immediately contact the insurer.

- **Review Payment Card Statements.** We also recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.
- **Consult the Identity Theft Protection Guide.** Please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect against identity theft, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on credit files.

Again, as of the date of this letter, we have no indication that any data has been used inappropriately. If you have questions or would like any additional information about this incident, we have established a call center to answer your questions. The call center is open 9 a.m.-9 p.m. EST and may be reached at 877-271-1568 from anywhere within the United States or at 503-520-4450 from outside the United States (tolls may apply). We sincerely regret any inconvenience this incident presents to you.

Sincerely,

DeAnn Tucker

DeAnn Tucker, RHIA, CHPS, CCS
Director of Privacy & Security
OH MUHLENBERG, LLC

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Credit Freezes for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
Fraud Alerts: P.O. Box 105069, Atlanta, GA 30348
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes: P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228
Fraud Alerts and Security Freezes: P.O. Box 2000, Chester, PA 19022
888-909-8872

Adult Employee/Patient Notice

OH Muhlenberg, LLC

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

<<mail id>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>,

At OH Muhlenberg, LLC, the privacy and security of our patients' and employees' information is a top priority. On July 1, 2015, OH Muhlenberg, LLC acquired the hospital operations of Muhlenberg Community Hospital. Prior to that time, the Muhlenberg hospital had been owned and operated by Muhlenberg Community Hospital since 1938. As part of the acquisition, OH Muhlenberg, LLC acquired substantially all of the assets of Muhlenberg Community Hospital, including its computer systems, patient records and other records. Regrettably, we are writing to inform you of a security incident involving some of that information. As a result, we are providing this notice to you whether or not you were a patient or employee prior to July 1, 2015, and whether or not particular data was transmitted prior to that date.

On September 16, 2015, the FBI notified the Hospital of suspicious network activity involving third parties. Upon learning this information, we took immediate action, including initiating an internal investigation, and we also engaged a leading forensic IT firm to investigate this matter. Based upon this review, we have confirmed that a limited number of computers were infected with a keystroke logger designed to capture and transmit data as it was entered onto the affected computers. The infection may have started as early as January 2012.

The affected computers were used to enter patient financial data and health information; information about persons responsible for a patient's bill; and employee/contractor data, including potentially your name, address, telephone number(s), birthdate, Social Security number, driver's license/state identification number, medical and health plan information (such as your health insurance number, medical record number, diagnoses and treatment information, and payment information), financial account number, payment card information (such as primary account number and expiration date) and employment-related information. We also believe that the malware could have captured username and password information for accounts or websites that were accessed using the affected terminals.

The Hospital is committed to maintaining the privacy of its patients and employees, and takes precautions for the security of personal and medical information. Upon learning of the incident, the Hospital took prompt steps to address and contain it, including immediately blocking the external unauthorized IP addresses, as well as taking steps to disable the malware. The Hospital continues to enhance the security of its systems and is working with the FBI during its investigation.

While we have no indication that the data has been used inappropriately, out of an abundance of caution, we are providing this notice to individuals whose information was maintained in the Hospital's electronic patient records database, as well as to persons employed by or contracted for specific services by the Hospital on and after January 1, 2012. We want to make you aware of steps you can take to guard against possible identity theft or fraud:

- **Enroll in Experian's ProtectMyID® Alert.** We are offering you a complimentary one-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you, and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

- **Explanation of Benefits Review.** We also recommend that you regularly review the explanation of benefits statements that you receive from your insurer or that you receive or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits forms that were not received, please immediately contact the insurer.
- **Check Credit Reports.** We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.
- **Review Payment Card Statements.** We also recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued your credit or debit card immediately.
- **Change Your Passwords.** We recommend that you change your passwords for any accounts or websites you may have accessed using a Hospital terminal or the Hospital's Wi-Fi system as soon as possible. In addition, if you use the same password for other online accounts/websites, we recommend that you change your password for those accounts/websites as well. You should use different and "strong" password for all accounts/websites. Tips on creating a strong password are available at http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password and http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/.
- **Consult the Identity Theft Protection Guide.** Please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

Again, as of the date of this letter, we have no indication that any data has been used inappropriately. If you have questions or would like any additional information about this incident, we have established a call center to answer your questions. The call center is open 9 a.m.-9 p.m. EST and may be reached at 877-271-1568 from anywhere within the United States or at 503-520-4450 from outside the United States (tolls may apply). We sincerely regret any inconvenience this incident presents to you.

Sincerely,

DeAnn Tucker

DeAnn Tucker, RHIA, CHPS, CCS
Director of Privacy & Security
OH MUHLENBERG, LLC

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: February 18, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code:** [code]

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC97585.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- Free copy of your Experian credit report
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARETM, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8057 to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. 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.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Credit Freezes for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
Fraud Alerts: P.O. Box 105069, Atlanta, GA 30348
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes: P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228
Fraud Alerts and Security Freezes: P.O. Box 2000, Chester, PA 19022
888-909-8872

OH Muhlenberg, LLC

Deceased Employee/Patient Notice

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

<<mail id>>
Next of Kin of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear Next of Kin of <<First Name>> <<Last Name>>,

At OH Muhlenberg, LLC, the privacy and security of our patients' and employees' information is a top priority. On July 1, 2015, OH Muhlenberg, LLC acquired the hospital operations of Muhlenberg Community Hospital. Prior to that time, the Muhlenberg hospital had been owned and operated by Muhlenberg Community Hospital since 1938. As part of the acquisition, OH Muhlenberg, LLC acquired substantially all of the assets of Muhlenberg Community Hospital, including its computer systems, patient records and other records. Regrettably, we are writing to inform you of a security incident involving some of that information. As a result, we are providing this notice whether or not the decedent was a patient or employee prior to July 1, 2015, and whether or not particular data relating to the decedent was transmitted prior to that date.

On September 16, 2015, the FBI notified the Hospital of suspicious network activity involving third parties. Upon learning this information, we took immediate action, including initiating an internal investigation, and we also engaged a leading forensic IT firm to investigate this matter. Based upon this review, we have confirmed that a limited number of computers were infected with a keystroke logger designed to capture and transmit data as it was entered onto the affected computers. The infection may have started as early as January 2012.

The affected computers were used to enter patient financial data and health information; information about persons responsible for a patient's bill; and employee/contractor data, including potentially information about the decedent. The type of information affected could include name, address, telephone number(s), birthdate, Social Security number, driver's license/state identification number, medical and health plan information (such as health insurance number, medical record number, diagnoses and treatment information, and payment information), financial account number, payment card information (such as primary account number and expiration date) and employment-related information. We also believe that the malware could have captured username and password information for accounts or websites that were accessed using the affected terminals.

Please note that we have no indication that the data has been used inappropriately. However, out of an abundance of caution, we are providing this notice regarding individuals whose information was maintained in the Hospital's electronic patient records database, as well as regarding persons employed by or contracted for specific services by the Hospital on and after January 1, 2012.

The Hospital is committed to maintaining the privacy of its patients and employees, and takes precautions for the security of personal and medical information. Upon learning of the incident, the Hospital took prompt steps to address and contain it, including immediately blocking the external unauthorized IP addresses, as well as taking steps to disable the malware. The Hospital continues to enhance the security of its systems and is working with the FBI during its investigation.

We want to make you aware of steps you can take to guard against possible identity theft or fraud:

- **Check Credit Reports.** We recommend that you carefully check credit reports for accounts or inquiries you do not recognize. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on the credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up credit records. If you have not already done so, you can contact the National Credit Reporting Agencies to notify them of the decedent's passing and to request that a notation be added to the credit file.

- **Explanation of Benefits Review.** We also recommend that you regularly review the explanation of benefits statements that you receive or review for persons whose medical bills you assist with or pay. If you identify services listed on the explanation of benefits forms that were not received, please immediately contact the insurer.
- **Review Payment Card Statements.** We also recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.
- **Change Account Passwords.** We recommend that you change your passwords for any accounts or websites that may have been accessed using a Hospital terminal or the Hospital's Wi-Fi system as soon as possible. In addition, if the same password is used for other online accounts/websites, we recommend that you change the password for those accounts/websites as well. Different and "strong" passwords should be used for all accounts/websites. Tips on creating a strong password are available at http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password and http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/.
- **Consult the Identity Theft Protection Guide.** Please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect against identity theft, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on credit files.

Again, as of the date of this letter, we have no indication that any data has been used inappropriately. If you have questions or would like any additional information about this incident, we have established a call center to answer your questions. The call center is open 9 a.m.-9 p.m. EST and may be reached at 877-271-1568 from anywhere within the United States or at 503-520-4450 from outside the United States (tolls may apply). We sincerely regret any inconvenience this incident presents to you.

Sincerely,

DeAnn Tucker

DeAnn Tucker, RHIA, CHPS, CCS
Director of Privacy & Security
OH MUHLENBERG, LLC

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Credit Freezes for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
Fraud Alerts: P.O. Box 105069, Atlanta, GA 30348
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes: P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228
Fraud Alerts and Security Freezes: P.O. Box 2000, Chester, PA 19022
888-909-8872

Patient/Guarantor (Minor) Notice

OH Muhlenberg, LLC

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

<<mail id>>
Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>.

At OH Muhlenberg, LLC, the privacy and security of our patients' information is a top priority. On July 1, 2015, OH Muhlenberg, LLC acquired the hospital operations of Muhlenberg Community Hospital. Prior to that time, the Muhlenberg hospital had been owned and operated by Muhlenberg Community Hospital since 1938. As part of the acquisition, OH Muhlenberg, LLC acquired substantially all of the assets of Muhlenberg Community Hospital, including its computer systems, patient records and other records. Regrettably, we are writing to inform you of a security incident involving some of that information. As a result, we are providing this notice whether or not the minor was a patient prior to July 1, 2015, and whether or not particular data relating to the minor was transmitted prior to that date.

On September 16, 2015, the FBI notified the Hospital of suspicious network activity involving third parties. Upon learning this information, we took immediate action, including initiating an internal investigation, and we also engaged a leading forensic IT firm to investigate this matter. Based upon this review, we have confirmed that a limited number of computers were infected with a keystroke logger designed to capture and transmit data as it was entered onto the affected computers. The infection may have started as early as January 2012.

The affected computers were used to enter patient financial data and health information and information about persons responsible for a patient's bill, including potentially information about the minor. The type of information affected could include name, address, telephone number(s), birthdate, Social Security number, driver's license/ state identification number, medical and health plan information (such as health insurance number, medical record number, diagnoses and treatment information, and payment information), financial account number, and payment card information (such as primary account number and expiration date).

The Hospital is committed to maintaining the privacy of its patients and takes precautions for the security of personal and medical information. Upon learning of the incident, the Hospital took prompt steps to address and contain it, including immediately blocking the external unauthorized IP addresses, as well as taking steps to disable the malware. The Hospital continues to enhance the security of its systems and is working with the FBI during its investigation.

While we have no indication that the data has been used inappropriately, out of an abundance of caution, we are providing this notice to individuals whose information was maintained in the Hospital's electronic patient records database, as well as to persons employed by or contracted for specific services by the Hospital on and after January 1, 2012. We want to make you aware of steps you can take to guard against possible identity theft or fraud:

- **Enroll in Experian's Family Secure.** We are offering a complimentary one-year membership in Family Secure® from Experian®. This product monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if the minor has a credit report, a potential sign that his or her identity has been stolen. **To receive the complimentary Family Secure product, you, as the parent, must enroll at the web site with your activation code listed on the next page.**
- **Explanation of Benefits Review.** We also recommend that you regularly review the explanation of benefits statement that you receive from the minor's health insurer. If you identify services listed on the explanation of benefits forms that were not received, please immediately contact the insurer.
- **Check Credit Reports.** We recommend that you carefully check credit reports for accounts or inquiries you do not recognize. If you see anything you do not understand, call the credit agency immediately. If you find

any suspicious activity on the credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up credit records.

- **Review Payment Card Statements.** We also recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.
- **Consult the Identity Theft Protection Guide.** Please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect against identity theft, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on credit files.

Again, as of the date of this letter, we have no indication that any data has been used inappropriately. If you have questions or would like any additional information about this incident, we have established a call center to answer your questions. The call center is open 9 a.m.-9 p.m. EST and may be reached at 877-271-1568 from anywhere within the United States or at 503-520-4450 from outside the United States (tolls may apply). We sincerely regret any inconvenience this incident presents to you.

Sincerely,

DeAnn Tucker

DeAnn Tucker, RHIA, CHPS, CCS
Director of Privacy & Security
OH MUHLENBERG, LLC

To receive the complimentary Family Secure product, you as the parent must enroll at the web site with your activation code listed below. This activation code can only be used by the parent or guardian of the minor. Please keep in mind that once activated, the code cannot be re-used for another enrollment.

Activate Family Secure Now in Three Easy Steps

1. ENSURE **That You Enroll By: February 18, 2016** (Your code will not work after this date.)
2. VISIT the **Family Secure Web Site to enroll: http://www.familysecure.com/enroll**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call (877) 288-8057 and provide engagement #: **PC97586.**

Your complimentary one-year Family Secure membership includes:

Parent or Legal Guardian:
- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis.

Children:
- Monthly monitoring to determine whether enrolled minors in your household have an Experian credit report
- Alerts of key changes to your children's Experian credit report

All Members:
- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee*

Once your enrollment in Family Secure is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Credit Freezes for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
Fraud Alerts: P.O. Box 105069, Atlanta, GA 30348
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes: P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228
Fraud Alerts and Security Freezes: P.O. Box 2000, Chester, PA 19022
888-909-8872