

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

17818

October 2, 2020

F8545-L04-0000004 T00001 *****OEL LINE
SAMPLE A SAMPLE - L04 DEC SSN ONLY MA
C/O NEXT OF KIN
APT #123
123 ANY ST
ANYTOWN, US 12345-6789



RE: Personal information

Dear next of kin of Sample A Sample:

We are writing to inform you that we were notified on July 16, 2020 by one of our third-party software vendors, Blackbaud, that it was the victim of a ransomware attack in May 2020. Blackbaud is a software vendor widely used by many non-profit organizations to support their fundraising and engagement efforts. Many Blackbaud clients, including Southcoast Hospitals Group, Inc. ("Southcoast"), were affected by this incident, in which hackers may have obtained some of our donors' and constituents' personal information, which may have included names, addresses, dates of birth and Social Security numbers.

Blackbaud informed us that the incident did not include credit card information, bank account information, usernames or passwords and we have independently confirmed this through a forensic analysis.

Southcoast takes the protection and proper use of our donors' and constituents' information very seriously, and our contractual agreement with Blackbaud required Blackbaud to keep our donors' and constituents' information confidential, including having security procedures in place to help prevent these types of incidents. Once we were informed of the incident by Blackbaud, we promptly started a comprehensive process of reviewing the affected data, in partnership with a forensic investigation firm, to determine the identity of the individuals potentially affected by this incident. This process took time to complete. We have determined that information about the individual listed above was included in the security incident.

A full description of the incident can be found on Blackbaud's website: <https://www.blackbaud.com/securityincident>. Blackbaud believes that the affected data was destroyed and not misused by the hackers, but as an added precaution, they have engaged experts to continuously monitor the dark web for an indefinite timeframe, in order to confirm that no stolen data is made publicly available in the future. In addition, as part of their efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect their systems from subsequent incidents.

0000004



Based on the nature of this incident, Blackbaud's research and a third-party investigation, including by law enforcement, Blackbaud has indicated to us that it has no reason to believe that any data will be misused or will be disseminated or otherwise made publicly available. However, we are taking precautionary measures to protect against fraudulent activities.

WHAT WE ARE DOING

We are committed to helping those who may have been impacted by this unfortunate situation. We have determined that this individual's Social Security number was included in the data that was accessed. That's why we are providing access to free credit monitoring for twenty-four (24) months through Experian's® IdentityWorksSM. This product offers identity detection and resolution of identity theft. To activate the membership please follow the steps below:

- Ensure enrollment by: **December 31, 2020** (the code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide the **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-855-896-4447 by **December 31, 2020**. Be prepared to provide engagement number **DB22970** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING THE EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

Please contact Experian **immediately** regarding any fraud issues. This product allows access to the following features once enrolled in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with this individual's credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** The same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of this individual's information and you would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-855-896-4447. If, after discussing the situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on this individual's credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore this individual's identity to its proper condition).

Please note that this Identity Restoration support is available for one year from the date of this letter and does not require any action at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

WHAT YOU CAN DO

If you choose not to use these services, **we strongly urge you to do the following:**

If you choose to place a fraud alert or security freeze on behalf of this individual, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests made for new loans, credit mortgages, employment, housing or other services. There is no charge to request a credit freeze.

In order to request a security freeze, you will need to provide the following information about the individual:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses over the prior five (5) years;
- Proof of most recent address; and,
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.) or some other proof of the individual's identity.

The credit reporting agencies have three (3) business days after receiving the request to place a security freeze on the credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to the credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive the credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving the request to lift the security freeze for those identified entities or for the specified period of time.



To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the security freeze.

Should you wish to obtain a credit report and monitor it on your own, you may obtain free copies of this individual's credit report by visiting www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.) Upon receipt of the credit report, we recommend that you review it carefully for any suspicious activity.

You can also obtain more information about identity theft from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

OTHER IMPORTANT INFORMATION

For more information about identity theft and tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at <http://www.irs.gov>. You may want to consider notifying the IRS that this individual's tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. You will need to send Form 14039 to the IRS along with a copy of a valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including the identification, must be clear and legible;
- The identity theft marker will remain on file for a minimum of three tax cycles;
- Any returns containing this individual's Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

Please note that under Massachusetts law, there is a right to obtain any police report filed in regard to this incident. If this individual is the victim of identity theft, there is also the right to file a police report with local law enforcement or other enforcement agency and obtain a copy of it.

We apologize for any inconvenience this may cause. If you have any questions please do not hesitate to contact us at 1-855-896-4447.

Sincerely,



Kelly Breslin, CHC, CHPC | Privacy Officer
Corporate Compliance & Internal Audit

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 2, 2020

F8545-L05-0000005 T00001 *****OEL LINE
SAMPLE A SAMPLE - L05 DEC SSN/PHI MA
C/O NEXT OF KIN
APT #123
123 ANY ST
ANYTOWN, US 12345-6789

**RE: Protected health information and personal information**

Dear next of kin of Sample A Sample:

We are writing to inform you that we were notified on July 16, 2020 by one of our third-party software vendors, Blackbaud, that it was the victim of a ransomware attack in May 2020. Blackbaud is a software vendor widely used by many non-profit organizations to support their fundraising and engagement efforts. Many Blackbaud clients, including Southcoast Hospitals Group, Inc. ("Southcoast"), were affected by this incident, in which hackers may have obtained some of our donors' and constituents' protected health information and personal information, which may have included names, addresses, dates of birth, Social Security numbers, diagnosis and medical condition(s), dates of admission, dates of death (as applicable), treating provider(s) and provider name(s).

Blackbaud informed us that the incident did not include credit card information, bank account information, usernames or passwords and we have independently confirmed this through a forensic analysis.

Southcoast takes the protection and proper use of its donors' and constituents' information very seriously, and our contractual agreement with Blackbaud required Blackbaud to keep information confidential, including having security procedures in place to help prevent these types of incidents. Once we were informed of the incident by Blackbaud, we promptly started a comprehensive process of reviewing the affected data, in partnership with a forensic investigation firm, to determine the identity of the individuals potentially affected by this incident. This process took time to complete. We have determined that information about the individual listed above was included in the security incident.

A full description of the incident can be found on Blackbaud's website: <https://www.blackbaud.com/securityincident>. Blackbaud believes that the affected data was destroyed and not misused by the hackers, but as an added precaution, they have engaged experts to continuously monitor the dark web for an indefinite timeframe, in order to confirm that no stolen data is made publicly available in the future. In addition, as part of their efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect their systems from subsequent incidents.

0000005



Based on the nature of this incident, Blackbaud's research and a third-party investigation, including by law enforcement, Blackbaud has indicated to us that it has no reason to believe that any data will be misused or will be disseminated or otherwise made publicly available. However, we are taking precautionary measures to protect against fraudulent activities.

WHAT WE ARE DOING

We are committed to helping those who may have been impacted by this unfortunate situation. We have determined that this individual's Social Security number was included in the data that was accessed. That's why we are providing access to free credit monitoring for twenty-four (24) months through Experian's® IdentityWorksSM. This product offers identity detection and resolution of identity theft. To activate the membership please follow the steps below:

- Ensure enrollment by: **December 31, 2020** (the code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide the **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-855-896-4447 by **December 31, 2020**. Be prepared to provide engagement number **DB22970** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING THE EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

Please contact Experian **immediately** regarding any fraud issues. This product allows access to the following features once enrolled in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with this individual's credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** The same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of this individual's information and you would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-855-896-4447. If, after discussing the situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on this individual's credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore this individual's identity to its proper condition).

Please note that this Identity Restoration support is available for one year from the date of this letter and does not require any action at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

WHAT YOU CAN DO

If you choose not to use these services, **we strongly urge you to do the following:**

If you choose to place a fraud alert or security freeze on behalf of this individual, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests made for new loans, credit mortgages, employment, housing or other services. There is no charge to request a credit freeze.

In order to request a security freeze, you will need to provide the following information about the individual:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses over the prior five (5) years;
- Proof of most recent address; and,
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.) or some other proof of the individual's identity.

The credit reporting agencies have three (3) business days after receiving the request to place a security freeze on the credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to the credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive the credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving the request to lift the security freeze for those identified entities or for the specified period of time.



To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the security freeze.

Should you wish to obtain a credit report and monitor it on your own, you may obtain free copies of this individual's credit report by visiting www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.) Upon receipt of the credit report, we recommend that you review it carefully for any suspicious activity.

You can also obtain more information about identity theft from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

OTHER IMPORTANT INFORMATION

For more information about identity theft and tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at <http://www.irs.gov>. You may want to consider notifying the IRS that this individual's tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. You will need to send Form 14039 to the IRS along with a copy of a valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including the identification, must be clear and legible;
- The identity theft marker will remain on file for a minimum of three tax cycles;
- Any returns containing this individual's Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

Please note that under Massachusetts law, there is a right to obtain any police report filed in regard to this incident. If this individual is the victim of identity theft, there is also the right to file a police report with local law enforcement or other enforcement agency and obtain a copy of it.

We apologize for any inconvenience this may cause. If you have any questions please do not hesitate to contact us at 1-855-896-4447.

Sincerely,



Kelly Breslin, CHC, CHPC | Privacy Officer
Corporate Compliance & Internal Audit

October 2, 2020

F8545-L09-0000009 T00001 *****OEL LINE

SAMPLE A SAMPLE - L09 SSN ONLY MA

APT #123

123 ANY ST

ANYTOWN, US 12345-6789

**RE: Your personal information**

Dear Sample A Sample:

We are writing to inform you that we were notified on July 16, 2020 by one of our third-party software vendors, Blackbaud, that it was the victim of a ransomware attack in May 2020. Blackbaud is a software vendor widely used by many non-profit organizations to support their fundraising and engagement efforts. Many Blackbaud clients, including Southcoast Hospitals Group, Inc. ("Southcoast"), were affected by this incident, in which hackers may have obtained some of our donors' and constituents' personal information, which may have included names, addresses, dates of birth and Social Security numbers.

Blackbaud informed us that the incident did not include credit card information, bank account information, usernames or passwords and we have independently confirmed this through a forensic analysis.

Southcoast takes the protection and proper use of your information very seriously, and our contractual agreement with Blackbaud required Blackbaud to keep our donors' and constituents' information confidential, including having security procedures in place to help prevent these types of incidents. Once we were informed of the incident by Blackbaud, we promptly started a comprehensive process of reviewing the affected data, in partnership with a forensic investigation firm, to determine the identity of the individuals potentially affected by this incident. This process took time to complete. We have determined that your information was included in the security incident.

A full description of the incident can be found on Blackbaud's website: <https://www.blackbaud.com/securityincident>. Blackbaud believes that the affected data was destroyed and not misused by the hackers, but as an added precaution, they have engaged experts to continuously monitor the dark web for an indefinite timeframe, in order to confirm that no stolen data is made publicly available in the future. In addition, as part of their efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect their systems from subsequent incidents.

0000009



Based on the nature of this incident, Blackbaud's research and a third-party investigation, including by law enforcement, Blackbaud has indicated to us that it has no reason to believe that any data will be misused or will be disseminated or otherwise made publicly available. However, we are taking precautionary measures to protect your financial security and help to alleviate any concerns you may have.

We are committed to helping those who may have been impacted by this unfortunate situation. We have determined that your Social Security number was included in the data that was accessed. That's why we are providing you with access to free credit monitoring for twenty-four (24) months through Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: December 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-855-896-4447 by **December 31, 2020**. Be prepared to provide engagement number **DB22970** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-855-896-4447. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

If you choose not to use these services, **we strongly urge you to do the following:**

If you choose to place a fraud alert or security freeze on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no charge to request a credit freeze.

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years;
- Proof of current address such as a current utility bill or telephone bill; and,
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

0000009



Should you wish to obtain a credit report and monitor it on your own, you may obtain free copies of your credit report by visiting www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.) Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity.

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at <http://www.irs.gov>. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

Please note that under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report with your local law enforcement or other enforcement agency and obtain a copy of it.

We apologize for any inconvenience this may cause you. If you have any questions please do not hesitate to contact us at 1-855-896-4447.

Sincerely,



Kelly Breslin, CHC, CHPC | Privacy Officer
Corporate Compliance & Internal Audit

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 2, 2020



F8545-L10-0000010 T00001 *****OEL LINE
SAMPLE A SAMPLE - L10 SSN/PHI MA
APT #123
123 ANY ST
ANYTOWN, US 12345-6789

**RE: Your protected health information and personal information**

Dear Sample A Sample:

We are writing to inform you that we were notified on July 16, 2020 by one of our third-party software vendors, Blackbaud, that it was the victim of a ransomware attack in May 2020. Blackbaud is a software vendor widely used by many non-profit organizations to support their fundraising and engagement efforts. Many Blackbaud clients, including Southcoast Hospitals Group, Inc. ("Southcoast"), were affected by this incident, in which hackers may have obtained some of our donors' and constituents' protected health information and personal information, which may have included names, addresses, dates of birth, Social Security numbers, diagnosis and medical condition(s), dates of admission, dates of death (as applicable), treating provider(s) and provider name(s).

Blackbaud informed us that the incident did not include credit card information, bank account information, usernames or passwords and we have independently confirmed this through a forensic analysis.

Southcoast takes the protection and proper use of your information very seriously, and our contractual agreement with Blackbaud required Blackbaud to keep our donors' and constituents' information confidential, including having security procedures in place to help prevent these types of incidents. Once we were informed of the incident by Blackbaud, we promptly started a comprehensive process of reviewing the affected data, in partnership with a forensic investigation firm, to determine the identity of the individuals potentially affected by this incident. This process took time to complete. We have determined that your information was included in the security incident.

A full description of the incident can be found on Blackbaud's website: <https://www.blackbaud.com/securityincident>. Blackbaud believes that the affected data was destroyed and not misused by the hackers, but as an added precaution, they have engaged experts to continuously monitor the dark web for an indefinite timeframe, in order to confirm that no stolen data is made publicly available in the future. In addition, as part of their efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect their systems from subsequent incidents.

Based on the nature of this incident, Blackbaud's research and a third-party investigation, including by law enforcement, Blackbaud has indicated to us that it has no reason to believe that any data will be misused or will be disseminated or otherwise made publicly available. However, we are taking precautionary measures to protect your financial security and help to alleviate any concerns you may have.

We are committed to helping those who may have been impacted by this unfortunate situation. We have determined that your Social Security number was included in the data that was accessed. That's why we are providing you with access to free credit monitoring for twenty-four (24) months through Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: December 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-855-896-4447 by **December 31, 2020**. Be prepared to provide engagement number **DB22970** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-855-896-4447. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

If you choose not to use these services, **we strongly urge you to do the following:**

If you choose to place a fraud alert or security freeze on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no charge to request a credit freeze.

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years;
- Proof of current address such as a current utility bill or telephone bill; and,
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.



To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Should you wish to obtain a credit report and monitor it on your own, you may obtain free copies of your credit report by visiting www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.) Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity.

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at <http://www.irs.gov>. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

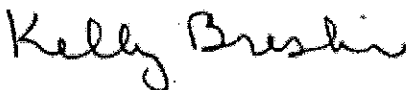
Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

Please note that under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report with your local law enforcement or other enforcement agency and obtain a copy of it.

We apologize for any inconvenience this may cause you. If you have any questions please do not hesitate to contact us at 1-855-896-4447.

Sincerely,



Kelly Breslin, CHC, CHPC | Privacy Officer
Corporate Compliance & Internal Audit