Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and

reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and

reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and

reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training

specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols.

This includes a recent town hall meeting where LCH employees were informed of the recent attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent

attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent

attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

747083.1

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear ,

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent

attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear ,

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent

attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Lynn Community
Health Center
269 Union Street
Lynn, Mass 01901

February 8, 2023

Dear ,

We are sending this letter to you as part of Lynn Community Health Inc's ("LCH") commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident potentially involving your personal information.

On December 12, 2022, we learned that an unauthorized user gained access to the email accounts of three employees. The unauthorized access occurred as a result of a phishing scheme sent to numerous LCH email users. Phishing is when an outside party replicates an email from a trusted source and directs it to a third party prompting the third-party recipient to respond as a means to gain unauthorized access to the email account of the recipient.

In this instance, LCH had robust monitoring software in place that enabled LCH to immediately detect, and respond to, unusual use consistent with phishing. LCH promptly secured the impacted email accounts to prevent further access. LCH launched an internal investigation to learn more about the incident immediately, and soon thereafter, LCH engaged independent digital forensics experts to determine the scope and extent of the potential unauthorized access to LCH's email system. LCH quickly confirmed that the phishing effort was limited to three email accounts and was effectively thwarted the same day.

During our investigation, we learned that the personal information of current and former patients, including the names and one or more of the following identifiers, was contained in the email account or other accessed information and, therefore, potentially accessible to the unauthorized user: date of birth, mailing address, phone number, insurance information, medical record number, diagnoses and other clinical information.

At this time, we have no indication that your personal information has been collected or misused. LCH is committed to further strengthening the existing security protocols to better protect patient records and patient information and takes cybersecurity incidents like these very seriously. To date, LCH has taken steps to further heighten security of personal information, retrain and reinforce existing information security procedures with employees, including training specifically on safeguarding personal password and credentials, and revise information protocols. This includes a recent town hall meeting where LCH employees were informed of the recent

attack and provided with renewed training/education on the dangers of phishing and ways to prevent attacks. These efforts are ongoing and will be increased as new threats emerge.

We sincerely regret any concern or inconvenience that this matter may cause you. For further assistance, please call 781-586-6652 and provide your contact information, and we will return the call as soon as possible during the week (Monday-Friday 8am-4pm).

Sincerely,
LCHC Compliance Team
Elena Freydin, DNO, Chief Compliance Officer
Brian D'Arcangelo Information Security Officer
Melanie Mendonca, CHCO HIPAA Privacy Officer

747083.1

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based on the method of your request. 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 between one (1) hour (for requests made online) three (3) business days (for requests made by mail) 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 or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.coom	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.