LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Donna Maddux
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Donna.Maddux@lewisbrisbois.com
Direct: 971.334.7001

April 22, 2022

VIA EMAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General Formella:

Lewis Brisbois represents Community Bridges in conjunction with a recent data security incident described in greater detail below. Community Bridges is a non-profit agency headquartered in Concord, New Hampshire with a mission to advance the integration, growth, and interdependence of individuals with developmental disabilities. The purpose of this letter is to notify you of the incident in accordance with N.H. Rev. Stat. §§ 359-C:19, C:20, C:21.

1. Nature of the Security Incident

On March 1, 2022, Community Bridges experienced a network disruption. Upon discovering this activity, Community Bridges immediately took steps to secure its environment and engaged cybersecurity experts to assist with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the Community Bridges network without authorization. On March 27, 2022, Community Bridges determined that certain personal information was involved in the incident. Community Bridges has worked diligently to notify impacted consumers.

2. Type of Information and Number of New Hampshire Residents Affected

Community Bridges notified nine (9) residents of New Hampshire of this data security incident via first class U.S. mail on April 22, 2022. The name and Social Security number of the impacted residents were potentially involved. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Community Bridges has implemented additional security features in an effort to prevent similar incidents from occurring in the future. Further, Community Bridges reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrator(s) of this incident responsible, if possible. In addition, Community Bridges has offered the affected individuals twelve (12) months of credit monitoring, identity remediation, and identity theft insurance services through notification services vendor, IDX.

Community Bridges has also launched a comprehensive data review project to identify other files that may have been accessed or acquired without authorization to determine if they contain personal information. This project remains ongoing, and we will provide you with supplemental notice should notification be provided to additional New Hampshire residents.

4. Contact Information

Community Bridges remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (971) 334-7001 or by email at Donna.Maddux@lewisbrisbois.com. Please let me know if you have any questions.

Regards,

Donna Maddux of
LEWIS BRISBOIS BISGAARD & SMITH LLP

DM
Attachment: Consumer Notification Letter Templates

COMMUNITY BRIDGES

Connecting Individuals with Disabilities to Their Community

April 22, 2022

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXX>>

Re: Notice of Data Security Incident for Individual Served

Dear Individual Served,

Community Bridges is writing to inform you of a recent data security incident that involved your personal information. At Community Bridges, we take the privacy and security of all of the information within our possession very seriously. We want to notify you of the incident, provide you with steps you can take to help protect your personal information, and offer you complimentary credit monitoring and identity protection services.

What Happened? On March 1, 2022, Community Bridges discovered it was the victim of a sophisticated cybersecurity attack affecting the digital network. Upon discovering this activity, we took steps to secure our digital environment. We also engaged a leading cybersecurity firm to assist with an investigation to determine whether personal information may have been accessed or acquired without authorization in conjunction with the attack. The investigation revealed that an unknown actor gained access to and obtained certain data from the Community Bridges network. On March 27, 2022, we learned that some of your personal information of your was involved in this incident.

What Information Was Involved? The information potentially impacted is any information may include your name, Social Security number, health insurance information, medical information, and other information.

What Are We Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible. We are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary credit monitoring and identity protection services for 12 months through IDX, a national leader in identity theft protection.

IDX's services include 12 months of credit monitoring and identity protection services, including CyberScan dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help resolve issues if their identity is compromised. As noted below, minors are ineligible for credit monitoring but are eligible for identity protection services.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect you information. You can also enroll in the IDX identity protection services, which are offered to you at no cost.

To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in their name, and have a U.S. residential address associated with their credit file. You can enroll in the complimentary IDX identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above.

Please note, the deadline to enroll is December 1, 2022. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

For More Information. If you have any questions about this letter, please call 1-800-225-4779 ext. 233 Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time.

On behalf of Community Bridges, thank you for your understanding about this incident. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience this matter may cause you.

Sincerely,

Ann P. Potoczak
President and CEO

Community Bridges

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving

your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

COMMUNITY BRIDGES

Connecting Individuals with Disabilities to Their Community

April 22, 2022

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXX>>

Re: Notice of Data Security Incident for Parent or Guardian of Individual Served

Dear Parent or Guardian,

Community Bridges is writing to inform you of a recent data security incident that involved the personal information of your family member or protected person. At Community Bridges, we take the privacy and security of all of the information within our possession very seriously. We want to notify you of the incident, provide you with steps you can take to help protect their personal information, and offer them complimentary credit monitoring and identity protection services.

What Happened? On March 1, 2022, Community Bridges discovered it was the victim of a sophisticated cybersecurity attack affecting the digital network. Upon discovering this activity, we took steps to secure our digital environment. We also engaged a leading cybersecurity firm to assist with an investigation to determine whether personal information may have been accessed or acquired without authorization in conjunction with the attack. The investigation revealed that an unknown actor gained access to and obtained certain data from the Community Bridges network. On March 27, 2022, we learned that some of your personal information of your was involved in this incident.

What Information Was Involved? The information potentially impacted is any information may include your name, Social Security number, health insurance information, medical information, and other information.

What Are We Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible. We are further notifying you of this event and advising you about steps you can take to help protect their information. In addition, out of an abundance of caution, we are offering them complimentary credit monitoring and identity protection services for 12 months through IDX, a national leader in identity theft protection.

IDX's services include 12 months of credit monitoring and identity protection services, including CyberScan dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help resolve issues if their identity is compromised. As noted below, minors are ineligible for credit monitoring but are eligible for identity protection services.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect you information. You can also enroll in the IDX identity protection services, which are offered to you at no cost.

To receive credit monitoring services, they must be over the age of 18 and have established credit in the U.S., have a Social Security number in their name, and have a U.S. residential address associated with their credit file. You can enroll them in the complimentary IDX identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above.

Please note, the deadline to enroll is December 1, 2022. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

For More Information. If you have any questions about this letter, please call 1-800-225-4779 ext. 233 Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time.

On behalf of Community Bridges, thank you for your understanding about this incident. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience this matter may cause you.

Sincerely,

Ann P. Potoczak
President and CEO

Community Bridges

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR WARD'S/ FAMILY MEMBER'S INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving

your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.