MULLEN COUGHLIN LLC

Paul McGurkin
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 15, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Community Solutions, Inc. ("CSI"), 340 West Newberry Road Suite B, Bloomfield, CT 06002, and write to provide your Office with notice of an incident that may affect the security of personal information relating to certain New Hampshire residents. This notice may be supplemented if significant facts are learned subsequent to its submission. By providing this notice, CSI does not waive any rights or defenses regarding the applicability of New Hampshire law, the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

Earlier this year, CSI determined that several employee email accounts were subject to unauthorized access between November 11, 2019 to December 5, 2019. CSI was unable to determine what, if any, emails and attachments within the account were subject to unauthorized access. CSI was only able to confirm that the email accounts were subject to unauthorized access. CSI enlisted the services of a third-party firm to review the contents of the email account in order to determine whether it contained any sensitive information.

CSI is unaware of any actual or attempted misuse of personal information as a result of this incident. CSI undertook a review to confirm what data may have been present in the impacted email accounts and to whom that information relates. The investigation has been ongoing and has included a diligent review of the impacted employee accounts to confirm the nature and scope of the incident.

The time-intensive review of the email contents concluded on March 25, 2020. However, for a significant number of individuals, the initial review was unable to identify an address for the individuals. As the impacted population impacted both current and former employees as well as individuals to whom CSI provides services, this review was essential in order to provide affected individuals with the appropriate notice. CSI immediately began a second review of its internal records to match the individuals to the address

in their file, if necessary, so that CSI could provide them with notice. The review determined that the following data elements for New Hampshire residents were impacted: name, Social Security number and driver's license. This review concluded on May 12, 2020.

Notice to New Hampshire Residents

On June 15, 2020, CSI began mailing written notice of this incident to two (2) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and to Be Taken

Upon discovering this incident, CSI began an investigation to determine the nature and scope of the event, including identifying the individuals who may be affected, putting in place resources to assist them, and providing them with notice of this incident. CSI took immediate steps to respond to the incident and protect the impacted accounts by resetting the users' passwords.

CSI is also providing individuals with potentially affected Social Security numbers access to 12 months of credit monitoring and identity restoration services. Additionally, CSI is providing all potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4788.

Very truly yours,

Paul McGurkin of
MULLEN COUGHLIN LLC

Enclosure
PTM/hfh

EXHIBIT A

community solutions, inc.
creating conditions for change
www.csi-online.org

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

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

[First Name] [Last Name]
[Address 1] [Address 2]
[City] [State] [Zip]

June 15, 2020

Re: Notice of Data Event

Dear [First Name] [Middle Name] [Last Name] [Suffix],

Community Solutions, Inc. ("CSI") is writing to notify you of a recent event that may impact the privacy of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the incident, our response, and the steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? Earlier this year, CSI determined that several employee email accounts were subject to unauthorized access between November 11, 2019 to December 5, 2019. CSI was unable to determine what, if any, emails and attachments within the account were subject to unauthorized access. We were only able to confirm that the email accounts were subject to unauthorized access. CSI then enlisted the services of a third-party firm to review the contents of the email accounts in order to determine whether they contained any sensitive information. The time-intensive review of the email contents concluded on March 25, 2020. However, for a significant number of individuals, the initial review was unable to identify an address for the individuals. We immediately began a second review of our internal records to match the individuals to the address in our file, if necessary, so that we could provide them with notice. This review was completed on May 12, 2020.

What Information Was Involved? After a thorough and exhaustive review process, CSI determined that the impacted email accounts contained the following types of information: your name and [data elements]. At this time, we are unaware of any actual misuse of personal information relating to this event, and we are providing this notice in an abundance of caution.

What We Are Doing. The security, privacy, and confidentiality of your personal information are among our highest priorities. Upon learning of this incident, CSI immediately took steps to secure the email account and launched an in-depth investigation to determine the nature and scope of the incident. CSI is also reporting this incident to certain regulatory authorities, as required. While we are unaware of any misuse of your information as a result of this incident, we are offering you access to [XX] months of credit monitoring and identity restoration services through ID Experts at no cost to you.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information," which contain information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We recognize that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-800-939-4170. This toll-free line is available Monday - Friday from 6:00 am to 6:00 pm PST

We sincerely regret the inconvenience this event may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Fernando Muñiz
Chief Executive Officer
Community Solutions, Inc.

Steps You Can Take to Protect Your Information

Complimentary One-Year of Credit Monitoring Service

As an added precaution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect_and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. The deadline to enroll in free MyIDCare services is September 15, 2020.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

Monitor Your Accounts/Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will 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. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

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

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 56 approximately Rhode Island residents impacted by this incident.

community solutions, inc.
creating conditions for change
www.csi-online.org

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

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

[First Name] [Last Name]
[Address 1] [Address 2]
[City] [State] [Zip]

June 15, 2020

Re: Notice of Data Event

Dear [First Name] [Middle Name] [Last Name] [Suffix]

Community Solutions, Inc. ("CSI"), the organization that provides services to [PROGRAM NAME], is writing to notify you of a recent event that may impact the privacy of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the incident, our response, and the steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? Earlier this year, CSI determined that an unknown party may have gained access to several employee email accounts between November 11, 2019 to December 5, 2019. CSI was unable to determine what, if any, emails and attachments within the account were viewed by the unknown party. We only know that the email accounts were accessed by the unknown party. CSI then hired a third-party firm to review the contents of the email accounts in order to determine whether they contained any sensitive information. The review of the email contents concluded on March 25, 2020. However, for a significant number of individuals, the first review was unable to link them to the program in which they sought services and did not include an address for the individuals. We immediately began a second review of our internal records to match the individuals to the program in which they participated and to find the address, if necessary, so that we could provide them with notice. This review was completed on May 12, 2020.

What Information Was Involved? CSI determined that the impacted email accounts contained the following types of information: your name and [data elements]. At this time, we are unaware of any actual misuse of personal information relating to this event, and we are providing this notice in an abundance of caution.

What We Are Doing. The security, privacy, and confidentiality of your personal information are among our highest priorities. Upon learning of this incident, CSI immediately took steps to secure the email account and launched an in-depth investigation to determine the nature and scope of the incident. CSI is also reporting this incident to certain regulatory authorities, as required. While we are unaware of any misuse of your information as a result of this incident, we are offering you access to [XX] months of credit monitoring and identity restoration services through ID Experts at no cost to you.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information," which contain information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We recognize that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-800-939-4170. This toll-free line is available Monday – Friday from 6:00 am to 6:00 pm PST.

We sincerely regret the inconvenience this event may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Martha J Bassett

Martha Bassett
Corporate Compliance Officer

Steps You Can Take to Protect Your Information

Complimentary One-Year of Credit Monitoring Service

As an added precaution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect_and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. The deadline to enroll in free MyIDCare services is September 15, 2020.

2. **Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

Monitor Your Accounts/Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will 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. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

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