



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: 267-930-4799
Fax: 267-930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 13, 2019

INTENDED FOR ADDRESSEE(S) ONLY

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

Mullen Coughlin, LLC represents Solara Medical Supplies, LLC (“Solara”), located at 2084 Otay Lakes Rd #102, Chula Vista, CA 91913. We write to notify your office of an incident that may affect the security of some personal information relating to one hundred and thirty-eight (138) Washington residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Solara does not waive any rights or defenses regarding the applicability of Washington data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On June 28, 2019, Solara determined that an unknown actor gained access to a limited number of employee Office 365 accounts, from April 2, 2019 to June 20, 2019, as a result of a phishing email campaign. Solara worked with third party forensic experts to investigate and respond to this incident and confirm the security of relevant Solara systems. Through this investigation on July 3, 2019, Solara determined that certain information present within the employee Office 365 accounts may have been accessed or acquired by an unknown actor at the time of the incident. Solara, therefore, undertook a comprehensive manual and programmatic review of the accounts to identify

potentially affected personal information and notify those individuals potentially affected by this incident.

Once Solara confirmed that personal information was present in the accounts, Solara continued to work with the third-party forensic experts and review its records to determine the last known address for potentially affected individuals for purposes of providing notice of this incident. On September 25, 2019, Solara concluded this review and confirmed that personal information as defined by Wash. Rev. Code Ann. § 19.255.010 (West) was present within the relevant accounts at the time of the incident including the name, Social Security number, financial account information, driver's license / state ID, and Medicare ID / Medicaid ID of one hundred and thirty-eight (138) Washington residents.

Notice to Washington Residents

While the investigation was ongoing, on August 28, 2019, Solara posted notice of this incident on its website. Once Solara confirmed mailing addresses for the potentially affected individuals, Solara supplemented the August 28, 2019 notice consistent with applicable state and federal law by mailing notice letters to individuals for whom Solara had address information. This written notice included notice to the one hundred and thirty-eight (138) Washington residents whose personal information was present in the accounts. Written notice was provided on November 13, 2019 in substantially the same form as the letter attached here as *Exhibit A*. Solara updated its website notice and this notice may be found at <https://www.solara.com/dataincident>. Solara also issued a press release on November 13, 2019 to major statewide media in Washington in substantially the same form as the media notice attached here as *Exhibit B*.

Other Steps Taken and To Be Taken

Upon learning of this incident, Solara moved quickly to investigate and respond to this incident, assess the security of relevant Solara systems, and notify potentially affected individuals. The response included resetting relevant account passwords, reviewing the contents of the email accounts to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of Solara's ongoing commitment to the security of information in its care, Solara is also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

Solara is providing potentially affected individuals access to complimentary credit monitoring and identity protection services for twelve (12) months through Kroll. These services include fraud consultation and identity theft restoration services. Solara is also providing potentially affected 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 fraud and identity theft by reviewing account statements and explanation of benefits, monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report

Office of the Attorney General

November 13, 2019

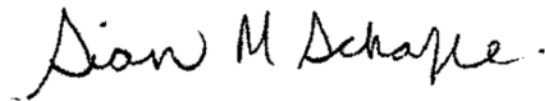
Page 3

attempted or actual identity theft and fraud. Solara notified law enforcement of this incident and is notifying relevant state and federal regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4799.

Very truly yours,

A handwritten signature in black ink that reads "Sian M. Schafle." The signature is written in a cursive, flowing style.

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/ew
Enclosure

cc:

Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
E-mail: securitybreach@atg.wa.gov

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Solara Medical Supplies, LLC ("Solara") is writing to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On June 28, 2019, Solara determined that an unknown actor gained access to a limited number of employee Office 365 accounts, from April 2, 2019 to June 20, 2019, as a result of a phishing email campaign. We worked with third party forensic experts to investigate and respond to this incident and confirm the security of relevant Solara systems. Through this investigation we determined that certain information present within the employee Office 365 accounts may have been accessed or acquired by an unknown actor at the time of the incident. We, therefore, undertook a comprehensive review of the accounts to identify potentially affected personal information. Our review determined that some of your personal information was present in an affected account at the time of the incident.

What Information Was Involved? The investigation determined that some of your personal information was present in an affected account at the time of the incident including your <<ClientDef1(impacted data)>><<ClientDef2(impacted data)>>. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant Solara systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the email accounts to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

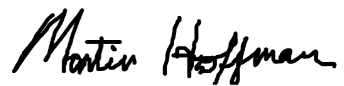
Solara notified law enforcement of this incident and is notifying relevant state and federal regulators. We are also offering you access to complimentary identity monitoring services for twelve (12) months through Kroll. These services include credit monitoring, fraud consultation and identity theft restoration services. If you wish to activate the identity monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Your Information*. There you will also find more information on the identity monitoring services we are making available to you. While Solara will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-877-460-0157 (toll free), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to Solara at: 2084 Otay Lakes Rd #102, Chula Vista, CA 91913 or visit <https://www.solara.com/dataincident>.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink that reads "Martin Hoffman". The signature is written in a cursive style with a large initial "M" and "H".

Martin Hoffman

Vice President of Compliance and Legal
Solara Medical Supplies, LLC

Steps You Can Take to Help Protect Your Information

Activate Your Complimentary Identity Monitoring

To activate Kroll's identity monitoring, fraud consultation, and identity theft restoration services, please follow the steps below:

- 1) Visit krollbreach.idMonitoringService.com to activate.
- 2) You have until **February 7, 2020** to activate your identity monitoring services. **Your membership number will not work after this date.**
- 3) Provide your personal information to Kroll, as requested.
- 4) Provide the following Membership Number: <<Member ID>>.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and 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

PO Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

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

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

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 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 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 New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 154 Rhode Island residents impacted by this incident.

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/>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

Parent or Guardian of

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

To the Parent or Guardian of <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Solara Medical Supplies, LLC ("Solara") is writing to inform you of an incident that may affect the security of some of your minor child's personal information. This notice provides information about the incident, our response, and resources available to you to help protect your minor child's information from possible misuse, should you feel it necessary to do so.

What Happened? On June 28, 2019, Solara determined that an unknown actor gained access to a limited number of employee Office 365 accounts, from April 2, 2019 to June 20, 2019, as a result of a phishing email campaign. We worked with third party forensic experts to investigate and respond to this incident and confirm the security of relevant Solara systems. Through this investigation we determined that certain information present within the employee Office 365 accounts may have been accessed or acquired by an unknown actor at the time of the incident. We, therefore, undertook a comprehensive review of the accounts to identify potentially affected personal information. Our review determined that some of your minor child's personal information was present in an affected account at the time of the incident.

What Information Was Involved? The investigation determined that some of your minor child's personal information was present in an affected account at the time of the incident including your minor child's <<ClientDef1(impacted data)>><<ClientDef2(impacted data)>>. To date, we are unaware of any actual or attempted misuse of your minor child's personal information as a result of this incident.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant Solara systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the email accounts to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

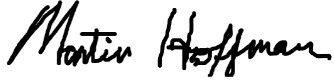
Solara notified law enforcement of this incident and is notifying relevant state and federal regulators. We are also offering you access to complimentary minor identity monitoring services for twelve (12) months through Kroll. These services include fraud consultation and identity theft restoration services. If you wish to activate Kroll's minor identity monitoring services for your minor child, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review relevant account statements, explanation of benefits, and existing credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the monitoring services we are making available to your minor child. While Solara will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-877-460-0157 (toll free), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to Solara at: 2084 Otay Lakes Rd #102, Chula Vista, CA 91913 or visit <https://www.solara.com/dataincident>.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink that reads "Martin Hoffman". The signature is written in a cursive style with a large initial "M".

Martin Hoffman
Vice President of Compliance and Legal
Solara Medical Supplies, LLC

Steps You Can Take to Help Protect Personal Information

Complimentary Minor Identity Monitoring Services

To activate Kroll's Minor Identity Monitoring services, please follow the steps below:

1. Visit **krollbreach.idMonitoringService.com** to activate and take advantage of Minor Identity Monitoring.
2. You have until **February 7, 2020** to activate monitoring services for your minor. **Your membership number will not work after this date.**
3. Your Membership Number is: **<<Member ID>>**.

After you have logged in for the first time, you will see a screen with the title "Confirm Your Information". Before Minor Identity Monitoring services can be activated, you must follow the instructions below:

1. Change the "First Name" and "Last Name" fields to a parent or guardian's name.
2. Change the address that appears to the parent or guardian's current address.
3. Enter the parent or guardian's date of birth and Social Security number.
4. Enter the email address and password you would like to use for the account.
5. Click the "Create Account" button. After the account is created, you will be able to activate your child's identity monitoring service.

Minor Identity Monitoring detects when names, addresses, and credit information are associated with your minor's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and credit reports for suspicious activity. Under U.S. law individuals with credit reports are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a 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 a credit report, if one exists.

While minors should not have a credit history, individuals with credit reports have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in their credit report without express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in an individual's name without 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 a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application an individual makes 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

PO Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

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, individuals with credit reports 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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
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 information, 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 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 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 New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 154 Rhode Island residents impacted by this incident.

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/>.



A Division of
DUFF & PHELPS

TAKE ADVANTAGE OF MINOR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Minor Identity Monitoring. Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your minor child's identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If your minor child becomes a victim of identity theft, an experienced Kroll licensed investigator will work on their behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your minor child's investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

EXHIBIT B

Solara Medical Supplies Provides Notice of a Data Breach

Chula Vista, California (November 13, 2019) – Solara Medical Supplies, LLC (“Solara”) provides notice of an incident that may affect the security of some information relating to certain individuals associated with Solara including current and former patients and employees.

What Happened? On June 28, 2019, Solara determined that an unknown actor gained access to a limited number of employee Office 365 accounts, from April 2, 2019 to June 20, 2019, as a result of a phishing email campaign. Solara worked with third party forensic experts to investigate and respond to this incident and confirm the security of relevant Solara systems. Through this investigation on July 3, 2019, Solara determined that certain information present within the employee Office 365 accounts may have been accessed or acquired by an unknown actor at the time of the incident. Solara undertook a comprehensive manual and programmatic review of the accounts to identify what personal information was stored within the accounts and to whom that information related.

What Information Was Involved? The personal information present in the accounts at the time of the incident varied by individual but may have included first and last names and one or more of the following data elements: name, address, date of birth, Social Security number, Employee Identification Number, medical information, health insurance information, financial information, credit / debit card information, driver’s license / state ID, passport information, password / PIN or account login information, billing / claims information, and Medicare ID / Medicaid ID.

What is Solara Doing? Solara takes this incident and security of personal information in its care seriously. Solara moved quickly to investigate and respond to this incident, assess the security of relevant Solara systems, and notify potentially affected individuals. This response included resetting relevant account passwords and reviewing and enhancing existing Solara policies and procedures to reduce the likelihood of a similar future event. Solara reported this incident to law enforcement and relevant state and federal regulators. Solara is also notifying potentially impacted individuals so that they may take further steps to best protect their information, should they feel it is appropriate to do so. In an abundance of caution, Solara is offering access to credit monitoring and identity protection services at no cost to impacted individuals.

What Can Impacted Individuals Do? Solara has established a dedicated assistance line for individuals seeking additional information regarding this incident. Individuals may call 1-877-460-0157 (toll free), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time with questions if they would like additional information. Individuals may also write to Solara at 2084 Otay lakes Rd #102, Chula Vista, CA 91913 or email Compliance@solaramedicalsupplies.com with questions. Additional information can also be found on Solara’s website, <https://www.solara.com/dataincident>. Potentially affected individuals may also consider the information and resources outlined below.

Solara encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud and to review account statements, credit reports, and explanation of benefits forms for suspicious activity. Under U.S. law, individuals with credit reports 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. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report. The credit reporting agencies may be contacted as follows:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.experian.com

www.transunion.com

www.equifax.com

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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 276999001, 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 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 New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 154 Rhode Island residents impacted by this incident.

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/>.