



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

August 15, 2022

VIA EMAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois represents San Diego American Indian Health Center ("SDAIHC"), a nonprofit community health center that provides comprehensive dental, behavioral health, and community wellness services to individuals, headquartered in San Diego, California, in conjunction with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification law.

1. Nature of the Security Incident

On May 5, 2022, SDAIHC experienced a network disruption. Upon discovering this activity, SDAIHC took immediate steps to secure its network environment and engaged leading cybersecurity experts to conduct an investigation to determine what happened and whether personal information may have been accessed or acquired in conjunction with the incident. The investigation revealed that an unknown actor gained access to obtained personal and protected health information in conjunction with a ransomware attack. After conducting an internal review of this data, on July 22, 2022, SDAIHC determined that certain personal information belonging to employees and patients was involved in the incident and worked diligently to notify these consumers.

2. Type of Information and Number of Maryland Residents Affected

SDAIHC notified four (4) residents of Maryland of this data security incident via first class U.S. mail on August 15, 2022. The names and Social Security numbers, driver's license or state identification card numbers, tribal identification card numbers, medical information, health insurance information and/or dates of birth of these residents were potentially involved. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

SDAIHC reported this incident to the Federal Bureau of Investigation and will cooperate with investigative requests in an attempt to hold the perpetrator(s) of this incident responsible, if possible. SDAIHC has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, SDAIHC has offered the individuals whose information was involved 12 months of complimentary services through IDX, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

SDAIHC has also launched a comprehensive data review project with the assistance of a data review firm to examine additional files that may have been accessed or acquired without authorization to determine if they contain personal or protected health information. This project is ongoing, and SDAIHC will provide you with supplemental notice should notification be provided to additional residents in your State.

4. Contact Information

SDAIHC remains dedicated to protecting the personal information in its possession. 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.

Regards,



Donna Maddux of
LEWIS BRISBOIS BISGAARD & SMITH LLP

DM:NSJ

Enc.: Sample Consumer Notification Letter



P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-764-2924
Or Visit:
<https://response.idx.us/SDAIHC>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

August 15, 2022

Re: <<Variable>>

Dear <<First Name>> <<Last Name>>,

San Diego American Indian Health Center ("SDAIHC") is writing to inform you of a recent data security incident that may have involved your personal information. At SDAIHC, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On May 5, 2022, SDAIHC 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 network. On July 22, 2022, we learned that some of your personal information may have been involved in this incident.

What Information Was Involved? The information potentially involved includes your name and your Social Security number, driver's license or state identification card number, tribal identification card number, medical information, health insurance information, and/or date of birth.

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 <<12/24 months>> through IDX, a national leader in identity theft protection.

IDX's services include credit monitoring, 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 your identity is compromised.

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 your name, and have a U.S. residential address associated with your credit file. You can enroll in the complimentary IDX identity protection services by calling 1-833-764-2924 or going to <https://response.idx.us/SDAIHC> and using the Enrollment Code provided above.

Please note, the deadline to enroll is November 15, 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 IDX at 1-833-764-2924 from 6:00 a.m. to 6:00 p.m. Pacific Time.

On behalf of SDAIHC, 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,

A handwritten signature in black ink, appearing to read "Kevin LaChapelle". The signature is fluid and cursive, with the first name "Kevin" and last name "LaChapelle" clearly distinguishable.

Kevin LaChapelle
Chief Executive Officer
San Diego American Indian Health Center

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 proof. 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.

San Diego American Indian Health Center: San Diego American Indian Health Center, located at 2630 First Ave., San Diego, CA 92103 can be reached at: (619) 234-2158.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Rhode Island: The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov



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

November 10, 2022

VIA ELECTRONIC MAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: Notification of Data Security Incident - Update

Dear Attorney General Frosh:

Lewis Brisbois represents San Diego American Indian Health Center ("SDAIHC"), a nonprofit community health center that provides comprehensive dental, behavioral health, and community wellness services to individuals, headquartered in San Diego, California, in conjunction with a recent data security incident described in greater detail below. The purpose of this letter is to provide an update regarding the recent data security incident experienced by SDAIHC described in our previous correspondence dated August 15, 2022.

1. Nature of the Security Incident

On May 5, 2022, SDAIHC experienced a network disruption. Upon discovering this activity, SDAIHC took immediate steps to secure its network environment and engaged leading cybersecurity experts to conduct an investigation to determine what happened and whether personal information may have been accessed or acquired in conjunction with the incident. The investigation determined that an unknown actor gained access to and obtained data from the SDAIHC network without authorization.

SDAIHC conducted an internal review of this data and, on July 22, 2022, determined that certain personal information belonging to employees and patients was involved in the incident. Beginning on August 15, 2022, SDAIHC mailed notice of this incident to all potentially impacted individuals for whom SDAIHC had identifiable address information.

As discussed in our previous letter, SDAIHC then worked diligently with experts to review the impacted data set and identify any additional potentially-impacted individuals with address

information. That process was completed on October 14, 2022, and on November 10, 2022, SDAIHC provided notice of this incident to those individuals.

2. Type of Information and Number of Maryland Residents Affected

On November 10, 2022, SDAIHC notified an additional three (3) residents of Maryland of this data security incident via first class U.S. mail. The total number of Maryland residents notified in both mailings is seven (7). The following personal and protected health information may have been involved in the incident: name, address, Social Security number, driver's license or state identification card number, tribal identification card number, passport number, medical information, health insurance information, and/or date of birth. A sample copy of the notification letter sent on November 10, 2022 is included with this correspondence.

3. Steps Taken Relating to the Incident

SDAIHC reported this incident to the Federal Bureau of Investigation and will cooperate with investigative requests in an attempt to hold the perpetrator(s) of this incident responsible, if possible. SDAIHC also notified all relevant state regulators and the Office of Health and Human Services Office of Civil Rights.

SDAIHC has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, SDAIHC has offered the individuals whose information was involved twelve (12) months of complimentary services through IDX, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

4. Contact Information

SDAIHC remains dedicated to protecting the personal information in its possession. 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.

Regards,



Donna Maddux of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enc.: Sample Consumer Notification Letter(s)



Return to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-764-2924
Or Visit:
<https://response.idx.us/SDAIHC>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

November 10, 2022

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

San Diego American Indian Health Center (“SDAIHC”) is writing to inform you of a recent data security incident that may have involved your personal information. At SDAIHC, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On May 5, 2022, SDAIHC 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. The investigation revealed that an unknown actor gained access to and obtained certain data from the network. SDAIHC then worked with experts to conduct a comprehensive review of the potentially impacted data to determine what personal information may have been impacted. On October 14, 2022, we learned that some of your personal information may have been impacted in this incident.

What Information Was Involved? The information potentially involved includes your name and your Social Security number, driver’s license or state identification card number, tribal identification card number, medical information, health insurance information, and/or date of birth.

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 <<twelve (12)/twenty-four (24)>> months through IDX, a national leader in identity theft protection.

IDX’s services include credit monitoring, 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 your identity is compromised.

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 your 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 your name, and have a U.S. residential address associated with your credit file. You can enroll in the complimentary IDX identity protection services by calling 1-833-764-2924 or going to <https://response.idx.us/SDAIHC> and using the Enrollment Code provided above.

Please note, the deadline to enroll is February 10, 2023. 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 IDX at 1-833-764-2924 from 6:00 a.m. to 6:00 p.m. Pacific Time.

On behalf of SDAIHC, 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,

A handwritten signature in black ink, appearing to read "Kevin LaChapelle". The signature is fluid and cursive, with the first name "Kevin" and last name "LaChapelle" clearly distinguishable.

Kevin LaChapelle
Chief Executive Officer
San Diego American Indian Health Center

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 proof. 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.

San Diego American Indian Health Center: San Diego American Indian Health Center, located at 2630 First Ave., San Diego, CA 92103 can be reached at: (619) 234-2158.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Rhode Island: The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov