CAMERON G. SHILLING
Direct Dial: 603.628.1351
Email: cameron.shilling@mclane.com
Admitted in NH and MA
900 Elm Street, P.O. Box 326
Manchester, NH 03105-0326
T 603.625.6464
F 603.625.5650

November 11, 2024

Via Online Submission Only
Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Breach Notification

To Whom It May Concern:

I am writing on behalf of BBS Financial Service, LLC (BBS) to notify you of a data breach. BBS has provided notification of the breach to 1,404 residents of Maine.

BBS is an accounting firm located at 302 Broadway, Methuen, Massachusetts 01844. BBS provides tax preparation, payroll, and medical billing services to its clients.

On January 29, 2024, BBS learned that data had been exfiltrated from its server network, and that the perpetrator was demanding ransom to delete it. BBS shut down its network and engaged counsel and a forensic expert to investigate. The investigation as well as negotiations with the perpetrator confirmed that data was in fact exfiltrated. In consultation with the FBI, BBS determined that the perpetrator, BianLian, was legitimate and reliable. BBS therefore negotiated and paid a ransom, and obtained credible evidence of the destruction of all data exfiltrated from its network, in order to protect affected individuals. Since the breach, BBS has monitored the dark web and, to date, has found no evidence of any disclosure of such data.

Because the breach occurred shortly before the opening of the electronic tax filing season and because BBS provides tax preparation services, BBS immediately contacted the cybersecurity division of the Internal Revenue Service, and by February 21, 2024 had initiated safeguards to mitigate the potential filing of fraudulent tax returns under the Return Integrity Compliance Services program. BBS did so before it was able to determine the identities of the individuals affected by the breach, so it did so on behalf of all of individuals involved in its tax preparation services. To date, BBS is not aware of any fraudulent tax return for any such individual arising out of this incident. BBS also filed a report about the breach through IC3.com.

BBS then worked to identify the scope of information and individuals affected by the breach. To do so, in addition to evidence recovered by its forensic expert, BBS used the spreadsheet provided by the perpetrators listing the comprised files. That spreadsheet has 961,688 lines. Each line identified the name of a compromised file, which predominantly were flat files, such as .pdfs. Due to the nature of the payroll and medical billing services that BBS provides, each file often consisted of numerous pages of data, and each page often was filled with numerous lines of text. Thus, after downloading all of that data for review purposes, even after retaining several outside data review contractors, reviewing all data in the 961,688 files was an immense and arduous task. Also, while some files could be readily reviewed to determine if they contain personally identifiable information and (if so) identify the individuals affected for notification purposes, the vast majority of the files contained incomplete or difficult to discern information for that purpose. For example, the files often had the names of individuals, in whole or in part, but no add

ress, or it was difficult for the data reviewers to determine the meanings of numbers associated with individuals. As a result, after many weeks of significant data review efforts at a pace that was yielding results

slowly, BBS decided that it would need to implement different notification strategies, and that it would need to notify affected individuals in two stages.

The first stage of notification was for BBS's tax preparation and payroll services, due to the nature of the information in those files. BBS identified the tax years and payroll periods with compromised files on the spreadsheet, extracted from its tax preparation and payroll databases the names of all taxpayers, dependents, shareholders of corporate taxpayers, and payroll recipients who were involved in any tax returns or payroll services for those affected tax years or payroll periods, deduplicated the results so that individuals did not receive multiple notifications, consolidated the results so that a family received a single notification for all affected family members, and further consolidated the results so that individuals received a single notification if they were involved in both tax preparation and payroll services (since BBS provides both such services to certain clients). Notifications to all of those individuals were mailed by BBS's notification provider, Equifax, by June 18, 2024. Attached are samples of those notification letters. 947 residents of Maine received notices from BBS in the first stage of notification.

The second notification stage was for medical billing services. The process was similar to, though more involved than, the prior processes, since many of the medical billing databases were legacy, since BBS no longer had databases for certain of its former clients, and since the notifications for pediatric practices was more involved. Thus, BBS contacted the former clients for whom it did not have a database to determine if the organizations would provide their databases to BBS for notification purposes, or if they instead preferred to notify affected individuals directly. After resolving all those issues, BBS extracted data from the databases, deduplicated and consolidated it, and notified affected individuals for all medical billing periods with compromised files. That second notification stage was sent on July 10, 2024 for adult medical practices, and by September 16, 2024 for pediatric practices. Attached are samples of those notification letters. 457 residents of Maine received notices from BBS in the second stage of notification.

Thus, a total of 1,404 residents of Maine were notified. While that may overstate the number of residents actually affected by the breach, since BBS did not review all of the data in the 961,688 files identified in the spreadsheet, BBS nonetheless provided notice to all of those individuals, since they were involved in the tax preparation, payroll, or medical billing services that BBS's provided to its clients for the tax years or the payroll or medical billing periods with compromised files.

The information affected by the breach varied from document-to-document and depended on whether an individual was involved in tax preparation, payroll, or medical billing services. For individuals involved in tax preparation or payroll services, the affected information could have included name, address, date of birth, government issued identification number, Social Security number, and financial account number. For individuals involved in medical billing services, the affected information could have included name and address in combination with a numerical insurance billing code attributable to services provided to the individual and a health insurance group and plan number.

BBS offered all notified individuals 2 years of identity and credit monitoring and restoration services through Equifax. Also, both shortly after learning about the breach and contemporaneously with notices to individuals, BBS informed its clients about the breach and about the notifications that it was providing to individuals.

Please do not hesitate to contact me if you questions or would like more information. Thank you.

Very truly yours,

Cameron G. Shilling

Cameron G. Shilling

Bookkeeping & Business Service
Medical Billing | Bookkeeping | Payroll | Taxes

<<Guardian 1 First Name>> <<Guardian 1 Last Name>>
<<Guardian 2 First Name>> <<Guardian 2 Last Name>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Re: Data Security Breach

Dear <<Guardian 1 First Name>> <<Guardian 1 Last Name>> <<and>> <<Guardian 2 First Name>> <<Guardian 2 Last Name>>,

We write to inform you about a data security breach at BBS Financial, LLC that affected certain health information of the following individuals associated with you.

<<FM1 First Name>> <<FM1 Last Name>>	<<M1 First Name>> <<M1 Last Name>>
<<FM2 First Name>> <<FM2 Last Name>>	<<M2 First Name>> <<M1 Last Name>>
<<FM3 First Name>> <<FM3 Last Name>>	<<M3 First Name>> <<M1 Last Name>>
<<FM4 First Name>> <<FM4 Last Name>>	<<M4 First Name>> <<M4 Last Name>>
<<FM5 First Name>> <<FM5 Last Name>>	<<M5 First Name>> <<M5 Last Name>>
<<FM6 First Name>> <<FM6 Last Name>>	<<M6 First Name>> <<M6 Last Name>>

What Happened: On January 29, 2024, BBS learned that data had been exfiltrated from its network, and that the threat actor was demanding ransom for deletion of it. BBS engaged cybersecurity counsel and a forensic expert to investigate. The investigation revealed that a sophisticated threat actor had accessed a portion of BBS's network. In consultation with law enforcement, BBS's counsel and expert determined that the threat actor was legitimate and reliable. BBS therefore obtained a list of the specific records exfiltrated, negotiated and paid a ransom, and obtained credible evidence of the threat actor's destruction of all BBS data. Additionally, BBS's counsel and expert have monitored the dark web and, to date, have seen no indication of disclosure of the data.

BBS also engaged its counsel and other services providers to conduct a lengthy and thorough review of the affected data, in order to determine the contents of it and which individuals were affected. You are receiving this letter because health information of the above minors was affected.

What Data Was Affected: The affected data included medical billing records that BBS retained for certain clients. While the information in those records differed, the records could have included some or all of the following: contact information, including name address; certain medical information, including date(s) of visit(s) and numerical billing code(s) attributable to medical service(s) for billing purposes; health insurance information, including carrier and group and plan number(s); and potentially other information that BBS received from providers to support medical billing. You are receiving this letter because the records included medical billing data for services that the above individuals received from <<Practice>>.

What You Should Do: BBS is offering (at no cost to you) and encouraging the above individuals to enroll in a 2-year identity and credit protection program. The program is provided by Equifax and includes the following services: monitoring the Equifax credit report; scanning Internet sites to detect unauthorized use of Social Security, governmental identification, financial account, and health insurance numbers; fraud alerts; specialists who will help restore identity and credit if compromised; and reimbursement of certain expenses related to doing so.

The credit and identity protection differs somewhat for adults and minors. The following describes those services. To enroll an ***adult***, please use the information and code below for ***adults***. To enroll one or more dependents who are ***minors***, please use the information and code below for ***minors***. Because some of the above individuals are under the age of 18, you will need to go online to help them to enroll at www.equifax.com/activate. You can use the same Activation Code to enroll up to four minors. Please complete the following steps to enroll. ***Please be aware that you have until expiration date to enroll, so please do so promptly.***

ADULT Credit and Identity Protection – Equifax Credit Watch™ Gold – ***ADULTS ONLY***
Enrollment Instructions

- Go to https//www.equifax.com/activate
- Enter the unique Activation Code associated with your name as follows.

<<FM1 First Name>> <<FM1 Last Name>> <<Code>>
<<FM2 First Name>> <<FM2 Last Name>> <<Code>>

<<FM3 First Name>> <<FM3 Last Name>> <<Code>>
<<FM4 First Name>> <<FM4 Last Name>> <<Code>>
<<FM5 First Name>> <<FM5 Last Name>> <<Code>>
<<FM6 First Name>> <<FM6 Last Name>> <<Code>>

Click "Submit" and complete the following 4 steps.

1. Register: Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. Create Account: Enter your email address, create a password, and accept the terms of use.
3. Verify Identity: To enroll in your product, we will ask you to complete our identity verification process.
4. Checkout: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

MINOR Credit and Identity Protection – Equifax Child Monitoring – ***MINORS ONLY***

Enrollment Instructions

<<M1 First Name>> <<M1 Last Name>> <<Code>>
<<M2 First Name>> <<M2 Last Name>> <<Code>>
<<M3 First Name>> <<M3 Last Name>> <<Code>>
<<M4 First Name>> <<M4 Last Name>> <<Code>>
<<M5 First Name>> <<M5 Last Name>> <<Code>>
<<M6 First Name>> <<M6 Last Name>> <<Code>>

Parent/Guardian:

Step 1:

If you already have a myEquifax™ account: Enter Activation Code at www.equifax.com/activate. Click 'Sign in here' link under 'Let's get started' header. After successfully signing in, you will skip to the Checkout Page.
If you DO NOT have an existing myEquifax™ account: Enter Activation Code at www.equifax.com/activate. Use your parent/guardian information to enroll. This will create your free MyEquifax account

Step 2:

Sign in to your myEquifax™ account. Click "Your People" module on dashboard, then the link to "Add a Child", and enter your minor's information. Please note you can use one Activation Code for up to 4 children under the age of 18. If you have more than four minors, you will need to enroll them under another parent or guardian's account.

While BBS feels that these services provide strong protection, if you feel additional measures are needed, some such steps are outlined below in the "Steps You Can Take To Help Protect Your Information."

Law Enforcement: BBS has filed a report with the FBI. If you experience identity or credit fraud, BBS encourages you to contact a local, state, or federal law enforcement authority.

For More Information: If you need help enrolling in the Equifax program, go online to www.equifax.com/activate for additional assistance. If you have questions about the incident, you can contact BBS at clientresponse@bbs1040.com or 844-236-9960. We apologize if this incident causes you concern, and are sincerely grateful for your continued trust and support of BBS.

Sincerely,

Gregory Brown, Managing Partner

Steps You Can Take to Help Protect Your Information

You can get one free report annually from each of the three credit bureaus. To obtain it, visit www.annualcreditreport.com or call 877-322-8228. You may also contact the credit bureaus directly using the information provided below to do so.

You can "freeze" or "lock" your credit report, which will prevent the credit bureaus from releasing information in your credit report without your consent, which is designed to prevent credit from being approved without consent. However, freezing or locking your credit report also may delay, interfere with, or prohibit timely approval of a request you make for a new loan, mortgage, or any other credit, since you will need to unfreeze or unlock your credit report to do so. You cannot be charged to place or lift a freeze or lock on your credit report. As an alternative to a freeze or lock, you can implement a free "fraud alert" on your credit reports. An initial fraud alert lasts for 1 year. A fraud requires a business to take steps to verify your identity before extending new credit in your name. If a victim of identity theft, you are entitled to an extended fraud alert, up to seven years. To do so, you can contact the credit bureaus as follows:

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

To implement a freeze, lock or fraud alert, you may need to provide the following: full name; SSN; date of birth; residential address for 5 years; proof of current address; governmental ID; and a police report if you are a victim of identity theft.

You can obtain further information about identity theft, credit freezes and locks, fraud alerts, and the steps you can take to protect yourself by contacting the credit bureaus, Federal Trade Commission, law enforcement, or your state Attorney General. The FTC can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 877-438-4338; and TTY 866-653-4261. The FTC encourages victims of identity theft to file a complaint with the FTC. You also can file a police report if you experience identity theft or fraud. To do so, you may need to provide proof of the identity theft or fraud. Finally, should can report identity theft or fraud to your state Attorney General.

California Residents: California Office of Privacy Protection (www.oag.ca.gov/privacy). Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 502-696-5300. Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023. New Mexico Residents: You have rights under 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. Also, under the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; they 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 a 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 under the Fair Credit Reporting Act. You can review your rights under 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. New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov/. North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400 or 877-566-7226. Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 877-877-9392. Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. Washington D.C. Residents: Office of Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 202-442-9828; https://oag.dc.gov. All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-438-4338, TTY 866-653-4261.

Bookkeeping & Business Service
Medical Billing | Bookkeeping | Payroll | Taxes

<<TP First Name>> <<TP Last Name>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Re: Data Security Breach

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

We write to inform you about a data security breach at BBS Financial, LLC (BBS). BBS prepares tax returns. You are receiving this letter for yourself and your dependents because we prepare or have prepared taxes for you for one or more years, and because certain information about your dependents was on those returns.

What Happened: On January 29, 2024, BBS learned that data had been exfiltrated from its network, and that the perpetrator was demanding ransom to delete it. BBS's cybersecurity counsel and forensic expert immediately investigated the matter. The investigation revealed that a sophisticated third party had accessed a portion of BBS's network.

In consultation with law enforcement, BBS's counsel and expert determined that the perpetrator was legitimate and reliable. BBS therefore obtained a list of the specific records exfiltrated from the third party, negotiated and paid a ransom, and obtained credible evidence of the perpetrator's destruction of all BBS data. Additionally, BBS's counsel and expert have monitored the dark web and, to date, have seen no indication of disclosure of the data.

During the above negotiations and prior to providing notice to you, we immediately contacted the cybersecurity division of the Internal Revenue Service (IRS) in order to implement safeguards to mitigate the potential electronic filing of fraudulent tax returns, since the IRS electronic tax return filing system opened in mid-January 2024. We supplied the IRS with the information necessary to activate the IRS's advanced fraud detection and prevention system, called Return Integrity Compliance Services (RICS). As a result, the IRS has implemented advanced mechanisms to detect and prevent the potential electronic filing of a fraudulent return for you for this tax year.

Because we initiated RICS, you may receive a communication from the IRS about that matter, including a request to submit certain tax forms to verify your identity, or to obtain an identity protection personal identification number (IP PIN) for the filing of electronic tax returns in the future. You may receive such a communication irrespective of whether or not a fraudulent tax return was filed in your name. If you receive such a communication, please contact us so we can assist you in addressing that matter with the IRS.

What Data Was Affected: BBS engaged its counsel and other services providers to conduct a lengthy and thorough review of the affected data to determine what it contains and who was affected. That revealed that the data included tax records BBS had for certain clients and their dependents. Information in our tax preparation files concerning individuals and their dependents varies from file-to-file. However, it commonly includes the following: Social Security numbers; 1120, 1120-S, 1065, K-1, and other such income and tax forms; contact information, including name, address, etc.; and other documents you may have provided to us to support the preparation of your tax return(s).

What You Should Do: BBS is offering (at no cost to you) and encouraging you to enroll yourself and your dependents in a 2-year identity and credit protection program. The program is provided by Equifax and includes the following: monitoring the Equifax credit report; scanning Internet sites to detect unauthorized use of Social Security, governmental identification, financial account, and health insurance numbers; fraud alerts; specialists who will help restore identity and credit if compromised; and reimbursement of certain expenses related to doing so.

You can enroll yourself and your dependents in this program either at www.equifax.com/activate. The credit and identity protection differs somewhat for adults and minors. The following describes those services. To enroll an ***adult***, please use the information and code below for ***adults***. To enroll one or more dependents who are ***minors***, please use the information and code below for ***minors***.

ADULT Credit and Identity Protection – Equifax Credit Watch™ Gold – ***ADULTS ONLY***

Enrollment Instructions

If you are an ***adult*** or enrolling an ***adult***, please complete the following steps to enroll. ***Please be aware that you have until expiration date to enroll, so please do so promptly.***

- Go to https//www.equifax.com/activate
- Enter the unique Activation Code associated with your name as follows.

<<TP First Name>> <<TP Last Name>> <<TP Code>>
<<SP First Name>> <<SP Last Name>> <<SP Code>>
<<AD1 First Name>> <<AD1 Last Name>> <<AD1 Code>>
<<AD2 First Name>> <<AD2 Last Name>> <<AD2 Code>>
<<AD3 First Name>> <<AD3 Last Name>> <<AD3 Code>>
<<AD4 First Name>> <<AD4 Last Name>> <<AD4 Code>>

Click "Submit" and complete the following 4 steps.

1. Register: Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. Create Account: Enter your email address, create a password, and accept the terms of use.
3. Verify Identity: To enroll in your product, we will ask you to complete our identity verification process.
4. Checkout: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

MINOR Credit and Identity Protection – Equifax Child Monitoring – ***MINORS ONLY***

Enrollment Instructions

After the parent or guardian has enrolled in Equifax Credit Watch Gold, please complete the following steps to enroll one or more ***minors***. ***Please be aware that you have until expiration date to enroll, so please do so promptly.***

1. Return to https//www.equifax.com/activate
2. Enter the unique Activation Code associated with the minor's name as follows.

<<MD1 First Name>> <<MD1 Last Name>> <<MD1 Code>>
<<MD2 First Name>> <<MD2 Last Name>> <<MD2 Code>>
<<MD3 First Name>> <<MD3 Last Name>> <<MD3 Code>>
<<MD4 First Name>> <<MD4 Last Name>> <<MD4 Code>>
<<MD5 First Name>> <<MD5 Last Name>> <<MD5 Code>>
<<MD6 First Name>> <<MD6 Last Name>> <<MD6 Code>>
<<MD7 First Name>> <<MD7 Last Name>> <<MD7 Code>>

Click "Submit" and complete the following 2 steps.

1. Sign In: Click the 'Sign in here' link under the "Let's get started" header. Sign in with your email address and password you created when initially creating your account.
2. Checkout: Click 'Sign Me Up' to finish your enrollment. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

Add Minors

In addition to enrolling minors as described above, you also will be able to add minors to your Equifax Child Monitoring Package through your product dashboard. Do so as follows.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child"

From there, enter your child's first name, last name, date of birth and social security number. Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can have up to 4 children under the age of 18 included in your Equifax Child Monitoring Package. If you have more than four children, you will need to enroll them under another parent or guardian's account.

Key Features

1. Child Monitoring for children under the age of 18
2. Emailed notifications of activity on the child's Equifax credit report

You only have until ***expiration date*** to enroll, so please do so promptly. While BBS feels that these services provide strong protection, if you feel additional measures are needed, some such steps are outlined below in the "Steps You Can Take To Help Protect Your Information."

Law Enforcement: BBS has filed a report with the FBI. If you experience identity or credit fraud, BBS encourages you to contact a local, state, or federal law enforcement authority.

For More Information: If you need help enrolling in the Equifax program, go online to www.equifax.com for additional assistance. If you have questions about the incident, you can contact BBS at clientresponse@bbs1040.com or 844-236-9960. We apologize if this incident causes you concern, and are sincerely grateful for your continued trust and support of BBS.

Sincerely,

Gregory Brown, Managing Partner

Steps You Can Take to Help Protect Your Information

You can get one free report annually from each of the three credit bureaus. To obtain it, visit www.annualcreditreport.com or call 877-322-8228. You may also contact the credit bureaus directly using the information provided below to do so.

You can "freeze" or "lock" your credit report, which will prevent the credit bureaus from releasing information in your credit report without your consent, which is designed to prevent credit from being approved without consent. However, freezing or locking your credit report also may delay, interfere with, or prohibit timely approval of a request you make for a new loan, mortgage, or any other credit, since you will need to unfreeze or unlock your credit report to do so. You cannot be charged to place or lift a freeze or lock on your credit report. As an alternative to a freeze or lock, you can implement a free "fraud alert" on your credit reports. An initial fraud alert lasts for 1 year. A fraud requires a business to take steps to verify your identity before extending new credit in your name. If a victim of identity theft, you are entitled to an extended fraud alert, up to seven years. To do so, you can contact the credit bureaus as follows:

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

To implement a freeze, lock or fraud alert, you may need to provide the following: full name; SSN; date of birth; residential address for 5 years; proof of current address; governmental ID; and a police report if you are a victim of identity theft.

You can obtain further information about identity theft, credit freezes and locks, fraud alerts, and the steps you can take to protect yourself by contacting the credit bureaus, Federal Trade Commission, law enforcement, or your state Attorney General. The FTC can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 877-438-4338; and TTY 866-653-4261. The FTC encourages victims of identity theft to file a complaint with the FTC. You also can file a police report if you experience identity theft or fraud. To do so, you may need to provide proof of the identity theft or fraud. Finally, should can report identity theft or fraud to your state Attorney General.

California Residents: California Office of Privacy Protection (www.oag.ca.gov/privacy). Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 502-696-5300. Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023. New Mexico Residents: You have rights under 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. Also, under the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; they 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 a 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 under the Fair Credit Reporting Act. You can review your rights under 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. New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov/. North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400 or 877-566-7226. Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 877-877-9392. Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident. Washington D.C. Residents: Office of Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 202-442-9828; https://oag.dc.gov. All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-438-4338, TTY 866-653-4261.

Bookkeeping & Business Service
Medical Billing | Bookkeeping | Payroll | Taxes

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Re: Data Security Breach

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

We write to inform you about a data security breach at BBS Financial, LLC. BBS prepares corporate tax returns. You are receiving this letter because we prepare or have prepared taxes for the below entity or entities, and your information was included in their tax returns for one or more years.

<<Corporate Entity 1>>
<<Corporate Entity 2>>
<<Corporate Entity 3>>
<<Corporate Entity 4>>
<<Corporate Entity 5>>

What Happened: On January 29, 2024, BBS learned that data had been exfiltrated from its network, and that the perpetrator was demanding ransom to delete it. BBS's cybersecurity counsel and forensic expert immediately investigated the matter. The investigation revealed that a sophisticated third party had accessed a portion of BBS's network.

In consultation with law enforcement, BBS's counsel and expert determined that the perpetrator was legitimate and reliable. BBS therefore obtained a list of the specific records exfiltrated from the third party, negotiated and paid a ransom, and obtained credible evidence of the perpetrator's destruction of all BBS data. Additionally, BBS's counsel and expert have monitored the dark web and, to date, have seen no indication of disclosure of the data.

What Data Was Affected: BBS engaged its counsel and other services providers to conduct a lengthy and thorough review of the affected data to determine what it contains and who was affected. That revealed that the data included tax records BBS had for certain clients. Information in our corporate tax preparation files varies from file-to-file. However, it commonly includes the following: Social Security numbers on K-1s; and contact information, including name, address, etc.

What You Should Do: BBS is offering (at no cost to you) and encouraging you to enroll yourself in a 2-year identity and credit protection program. The program is provided by Equifax and includes the following: monitoring the Equifax credit report; scanning Internet sites to detect unauthorized use of Social Security, governmental identification, financial account, and health insurance numbers; fraud alerts; specialists who will help restore identity and credit if compromised; and reimbursement of certain expenses related to doing so.

You can enroll in this program at www.equifax.com/activate.

ADULT Credit and Identity Protection – Equifax Credit Watch™ Gold – ***ADULTS ONLY***
Enrollment Instructions

Please complete the following steps to enroll. ***Please be aware that you have until expiration date to enroll, so please do so promptly.*** Go to https//www.equifax.com/activate. Enter the unique Activation Code associated with your name as follows.

<<First Name>> <<Last Name>> <<Code>>

Click "Submit" and complete the following 4 steps.

1. Register: Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. Create Account: Enter your email address, create a password, and accept the terms of use.
3. Verify Identity: To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

You only have until ***expiration date*** to enroll, so please do so promptly. While BBS feels that these services provide strong protection, if you feel additional measures are needed, some such steps are outlined below in the "Steps You Can Take To Help Protect Your Information."

Law Enforcement: BBS has filed a report with the FBI. If you experience identity or credit fraud, BBS encourages you to contact a local, state, or federal law enforcement authority.

For More Information: If you need help enrolling in the Equifax program, go online to www.equifax.com for additional assistance. If you have questions about the incident, you can contact BBS at clientresponse@bbs1040.com or 844-236-9960. We apologize if this incident causes you concern, and are sincerely grateful for your continued trust and support of BBS.

Sincerely,

Gregory Brown, Managing Partner

Steps You Can Take to Help Protect Your Information

You can get one free report annually from each of the three credit bureaus. To obtain it, visit www.annualcreditreport.com or call 877-322-8228. You may also contact the credit bureaus directly using the information provided below to do so.

You can "freeze" or "lock" your credit report, which will prevent the credit bureaus from releasing information in your credit report without your consent, which is designed to prevent credit from being approved without consent. However, freezing or locking your credit report also may delay, interfere with, or prohibit timely approval of a request you make for a new loan, mortgage, or any other credit, since you will need to unfreeze or unlock your credit report to do so. You cannot be charged to place or lift a freeze or lock on your credit report. As an alternative to a freeze or lock, you can implement a free "fraud alert" on your credit reports. An initial fraud alert lasts for 1 year. A fraud requires a business to take steps to verify your identity before extending new credit in your name. If a victim of identity theft, you are entitled to an extended fraud alert, up to seven years. To do so, you can contact the credit bureaus as follows:

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

To implement a freeze, lock or fraud alert, you may need to provide the following: full name; SSN; date of birth; residential address for 5 years; proof of current address; governmental ID; and a police report if you are a victim of identity theft.

You can obtain further information about identity theft, credit freezes and locks, fraud alerts, and the steps you can take to protect yourself by contacting the credit bureaus, Federal Trade Commission, law enforcement, or your state Attorney General. The FTC can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 877-438-4338; and TTY 866-653-4261. The FTC encourages victims of identity theft to file a complaint with the FTC. You also can file a police report if you experience identity theft or fraud. To do so, you may need to provide proof of the identity theft or fraud. Finally, you should report identity theft or fraud to your state Attorney General.

California Residents: California Office of Privacy Protection (www.oag.ca.gov/privacy). Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 502-696-5300. Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023. New Mexico Residents: You have rights under 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. Also, under the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; they 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 a 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 under the Fair Credit Reporting Act. You can review your rights under 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. New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov/. North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400 or 877-566-7226. Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 877-877-9392. Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident. Washington D.C. Residents: Office of Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 202-442-9828; https://oag.dc.gov. All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-438-4338, TTY 866-653-4261.

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Re: Data Security Breach

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

We write to inform you about a data security breach at BBS Financial, LLC. BBS provides payroll services for certain employers. You are receiving this letter because we provide or have provided payroll services for <<Employer 1>> and <<Employer 2>> for one or more years, and your information was included in their payroll processing files.

What Happened: On January 29, 2024, BBS learned that data had been exfiltrated from its network, and that the perpetrator was demanding ransom to delete it. BBS's cybersecurity counsel and forensic expert immediately investigated the matter. The investigation revealed that a sophisticated third party had accessed a portion of BBS's network.

In consultation with law enforcement, BBS's counsel and expert determined that the perpetrator was legitimate and reliable. BBS therefore obtained a list of the specific records exfiltrated from the third party, negotiated and paid a ransom, and obtained credible evidence of the perpetrator's destruction of all BBS data. Additionally, BBS's counsel and expert have monitored the dark web and, to date, have seen no indication of disclosure of the data.

What Data Was Affected: BBS engaged its counsel and other services providers to conduct a lengthy and thorough review of the affected data to determine what it contains and who was affected. That revealed that the data included payroll BBS had for certain clients. Information in BBS' payroll processing files concerning individuals varies from file-to-file. However, it commonly includes the following: contact information, including name, address, etc.; government-issued identification number, including driver's license number, passport number, etc.; Social Security numbers; date of birth; financial information, including bank and financial account number, etc.; and other information provided by BBS' clients to support their payroll processing.

What You Should Do: BBS is offering (at no cost to you) and encouraging you to enroll yourself in a 2-year identity and credit protection program. The program is provided by Equifax and includes the following: monitoring the Equifax credit report; scanning Internet sites to detect unauthorized use of Social Security, governmental identification, financial account, and health insurance numbers; fraud alerts; specialists who will help restore identity and credit if compromised; and reimbursement of certain expenses related to doing so.

You can enroll in this program at www.equifax.com/activate.

ADULT Credit and Identity Protection – Equifax Credit Watch™ Gold – ***ADULTS ONLY***

Enrollment Instructions

Please complete the following steps to enroll. ***Please be aware that you have until expiration date to enroll, so please do so promptly.*** Go to https//www.equifax.com/activate Enter the unique Activation Code associated with your name as follows.

<<First Name>> <<Last Name>> <<Code>>

Click "Submit" and complete the following 4 steps.

1. Register: Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. Create Account: Enter your email address, create a password, and accept the terms of use.
3. Verify Identity: To enroll in your product, we will ask you to complete our identity verification process.
4. Checkout: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

You only have until ***expiration date*** to enroll, so please do so promptly. While BBS feels that these services provide strong protection, if you feel additional measures are needed, some such steps are outlined below in the "Steps You Can Take To Help Protect Your Information."

Law Enforcement: BBS has filed a report with the FBI. If you experience identity or credit fraud, BBS encourages you to contact a local, state, or federal law enforcement authority.

For More Information: If you need help enrolling in the Equifax program, go online to www.equifax.com for additional assistance. If you have questions about the incident, you can contact BBS at clientresponse@bbs1040.com or 844-236-9960. We apologize if this incident causes you concern, and are sincerely grateful for your continued trust and support of BBS.

Sincerely,

Gregory Brown, Managing Partner

Steps You Can Take to Help Protect Your Information

You can get one free report annually from each of the three credit bureaus. To obtain it, visit www.annualcreditreport.com or call 877-322-8228. You may also contact the credit bureaus directly using the information provided below to do so.

You can "freeze" or "lock" your credit report, which will prevent the credit bureaus from releasing information in your credit report without your consent, which is designed to prevent credit from being approved without consent. However, freezing or locking your credit report also may delay, interfere with, or prohibit timely approval of a request you make for a new loan, mortgage, or any other credit, since you will need to unfreeze or unlock your credit report to do so. You cannot be charged to place or lift a freeze or lock on your credit report. As an alternative to a freeze or lock, you can implement a free "fraud alert" on your credit reports. An initial fraud alert lasts for 1 year. A fraud requires a business to take steps to verify your identity before extending new credit in your name. If a victim of identity theft, you are entitled to an extended fraud alert, up to seven years. To do so, you can contact the credit bureaus as follows:

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

To implement a freeze, lock or fraud alert, you may need to provide the following: full name; SSN; date of birth; residential address for 5 years; proof of current address; governmental ID; and a police report if you are a victim of identity theft.

You can obtain further information about identity theft, credit freezes and locks, fraud alerts, and the steps you can take to protect yourself by contacting the credit bureaus, Federal Trade Commission, law enforcement, or your state Attorney General. The FTC can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 877-438-4338; and TTY 866-653-4261. The FTC encourages victims of identity theft to file a complaint with the FTC. You also can file a police report if you experience identity theft or fraud. To do so, you may need to provide proof of the identity theft or fraud. Finally, should can report identity theft or fraud to your state Attorney General.

California Residents: California Office of Privacy Protection (www.oag.ca.gov/privacy). Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 502-696-5300. Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023. New Mexico Residents: You have rights under 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. Also, under the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; they 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 a 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 under the Fair Credit Reporting Act. You can review your rights under 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. New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov/. North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400 or 877-566-7226. Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 877-877-9392. Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident. Washington D.C. Residents: Office of Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 202-442-9828; https://oag.dc.gov. All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-438-4338, TTY 866-653-4261.

Bookkeeping & Business Service
Medical Billing | Bookkeeping | Payroll | Taxes

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Re: Data Security Breach

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

We write to inform you about a data security breach at BBS Financial, LLC. BBS provides medical billing services for certain providers. You are receiving this letter because we provide or have provided medical billing services for the below provider or providers for one or more years, and your health information was included in their records.

<<Practice 1>>
<<Practice 2>>
<<Practice 3>>

What Happened: On January 29, 2024, BBS learned that data had been exfiltrated from its network, and that the threat actor was demanding ransom for deletion of it. BBS engaged cybersecurity counsel and a forensic expert to investigate. The investigation revealed that a sophisticated threat actor had accessed a portion of BBS's network.

In consultation with law enforcement, BBS's counsel and expert determined that the threat actor was legitimate and reliable. BBS therefore obtained a list of the specific records exfiltrated, negotiated and paid a ransom, and obtained credible evidence of the threat actor's destruction of all BBS data. Additionally, BBS's counsel and expert have monitored the dark web and, to date, have seen no indication of disclosure of the data.

What Data Was Affected: BBS engaged its counsel and other service providers to conduct a lengthy and thorough review of the affected data, in order to determine the contents of it and which individuals were affected. The affected data included medical billing records that BBS retained for certain clients. Those records contained the names of the patient and provider, and in some cases also include contact information, including your name, address, etc.; information about your family members; medical information including dates of visits, service(s) provided, record numbers, etc.; numerical billing code for the medical service(s) provided; health insurance information, including insurance provider, group number, and plan; and other information provided by providers to support medical billing.

What You Should Do: BBS is offering (at no cost to you) and encouraging you to enroll yourself in a 2-year identity and credit protection program. The program is provided by Equifax and includes the following: monitoring the Equifax credit report; scanning Internet sites to detect unauthorized use of Social Security, governmental identification, financial account, and health insurance numbers; fraud alerts; specialists who will help restore identity and credit if compromised; and reimbursement of certain expenses related to doing so.

You can enroll in this program at www.equifax.com/activate.

ADULT Credit and Identity Protection – Equifax Credit Watch™ Gold – ***ADULTS ONLY***

Enrollment Instructions

Please complete the following steps to enroll. ***Please be aware that you have until expiration date to enroll, so please do so promptly.*** Go to https//www.equifax.com/activate Enter the unique Activation Code associated with your name as follows.

<<First Name>> <<Last Name>> <<Code>>

Click "Submit" and complete the following 4 steps.

1. Register: Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. Create Account: Enter your email address, create a password, and accept the terms of use.
3. Verify Identity: To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

You only have until ***expiration date*** to enroll, so please do so promptly. While BBS feels that these services provide strong protection, if you feel additional measures are needed, some such steps are outlined below in the "Steps You Can Take To Help Protect Your Information."

Law Enforcement: BBS has filed a report with the FBI. If you experience identity or credit fraud, BBS encourages you to contact a local, state, or federal law enforcement authority.

For More Information: If you need help enrolling in the Equifax program, go online to www.equifax.com for additional assistance. If you have questions about the incident, you can contact BBS at clientresponse@bbs1040.com or 844-236-9960. We apologize if this incident causes you concern, and are sincerely grateful for your continued trust and support of BBS.

Sincerely,

Gregory Brown, Managing Partner

Steps You Can Take to Help Protect Your Information

You can get one free report annually from each of the three credit bureaus. To obtain it, visit www.annualcreditreport.com or call 877-322-8228. You may also contact the credit bureaus directly using the information provided below to do so.

You can "freeze" or "lock" your credit report, which will prevent the credit bureaus from releasing information in your credit report without your consent, which is designed to prevent credit from being approved without consent. However, freezing or locking your credit report also may delay, interfere with, or prohibit timely approval of a request you make for a new loan, mortgage, or any other credit, since you will need to unfreeze or unlock your credit report to do so. You cannot be charged to place or lift a freeze or lock on your credit report. As an alternative to a freeze or lock, you can implement a free "fraud alert" on your credit reports. An initial fraud alert lasts for 1 year. A fraud requires a business to take steps to verify your identity before extending new credit in your name. If a victim of identity theft, you are entitled to an extended fraud alert, up to seven years. To do so, you can contact the credit bureaus as follows:

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

To implement a freeze, lock or fraud alert, you may need to provide the following: full name; SSN; date of birth; residential address for 5 years; proof of current address; governmental ID; and a police report if you are a victim of identity theft.

You can obtain further information about identity theft, credit freezes and locks, fraud alerts, and the steps you can take to protect yourself by contacting the credit bureaus, Federal Trade Commission, law enforcement, or your state Attorney General. The FTC can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 877-438-4338; and TTY 866-653-4261. The FTC encourages victims of identity theft to file a complaint with the FTC. You also can file a police report if you experience identity theft or fraud. To do so, you may need to provide proof of the identity theft or fraud. Finally, you can report identity theft or fraud to your state Attorney General.

California Residents: California Office of Privacy Protection (www.oag.ca.gov/privacy). Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 502-696-5300. Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023. New Mexico Residents: You have rights under 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. Also, under the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; they 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 a 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 under the Fair Credit Reporting Act. You can review your rights under 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. New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov/. North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400 or 877-566-7226. Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 877-877-9392. Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. Washington D.C. Residents: Office of Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 202-442-9828; https://oag.dc.gov. All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-438-4338, TTY 866-653-4261.