



Allen E. Sattler  
650 Town Center Drive, Suite 1400  
Costa Mesa, CA 92626  
Allen.Sattler@lewisbrisbois.com  
Direct: 714.668.5572

September 1, 2020

**VIA ONLINE SUBMISSION**

Attorney General Xavier Becerra  
Office of the Attorney General  
California Department of Justice  
Attn: Public Inquiry Unit  
P.O. Box 944255  
Sacramento, CA 94244-2550

Re: Notice of Data Security Incident

Dear Attorney General Becerra:

We represent Coast Financial Services (“Coast”) a financial services firm located in Santa Cruz, California, with regard to a recent data security incident described in greater detail below. This letter is being sent on behalf of Coast because personal information belonging to California residents may have been affected by a recent data security incident.

**1. Nature of the security incident.**

On May 6, 2020, Coast discovered that two servers had been encrypted and rendered inaccessible. Coast’s immediate concern was to contain the incident and secure our network systems. To that end, Coast engaged a digital forensics firm to investigate the cause and scope of the incident, and determine if any information stored within their systems had been affected. On July 7, Coasts’ investigation determined that an unauthorized individual accessed files containing certain personal information. The information that may have been accessed includes tax-related documents containing information that is included in tax returns, including names, mailing addresses, and Social Security numbers. Notably, Coast is not aware of any misuse of this information as a result of this incident.

**2. Number of California residents affected.**

Approximately 517 residents of California may have been affected by this incident. Coast will be notifying the potentially affected California residents on or about September 1, 2020, via U.S. mail. A sample copy of the notification letter is being provided with this correspondence.

**3. Steps taken relating to the incident.**

Coast implemented additional safeguards to improve data security on their web server infrastructure. In addition, Coast is offering identity theft protection services through ID Experts® to provide affected persons with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

**4. Contact Information.**

Coast remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (714) 668-5572 or by e-mail at [allen.sattler@lewisbrisbois.com](mailto:allen.sattler@lewisbrisbois.com).

Please let me know if you have any questions.

Very truly yours,



Allen E. Sattler of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter



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

To Enroll, Please Call: (800) 939-4170 Or Visit: <a href="https://app.myidcare.com/account-creation/protect">https://app.myidcare.com/account-creation/protect</a> Enrollment Code: <<XXXXXXXXXX>>
--

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

September 1, 2020

**Re: Notice of Data Incident**

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of an incident that involved some of your personal information. We take the security of personal information very seriously. Therefore, we are writing to inform you of the incident, and advise you of certain steps you can take to protect your information, including enrolling in the credit monitoring and identity protection services we are offering at no cost to you. At this time, there is no evidence that there has been any use or attempted use of the information exposed in this incident. In addition, receiving a letter does not mean that you are a victim of identity theft.

**What Happened?**

On May 6, 2020, we discovered that two servers had been encrypted and rendered inaccessible. Our immediate concern was to contain the incident and secure our network systems. To that end, we engaged a digital forensics firm to investigate the cause and scope of the incident, and determine if any information stored within our systems had been affected. On July 7, our investigation determined that an unauthorized individual accessed files containing certain personal information.

**What information was involved?**

The files that were accessed by the unauthorized individual contained tax related documents, containing information that is included in tax returns, including your name, mailing address, and Social Security number.

**What We Are Doing**

As soon as we discovered the incident, we took the steps described above. We have also reported the incident to the Federal Bureau of Investigation, and will provide whatever cooperation is necessary to help prevent fraudulent activity and facilitate prosecution of the perpetrators.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

## **What You Can Do**

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is December 1, 2020.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

## **For More Information**

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Bob Mason, CPA  
Coast Financial Services

## Recommended Steps to Help Protect Your Information

**1. Website and Enrollment.** Go to <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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

**3. Telephone.** Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**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](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.