

Akin Gump

STRAUSS HAUER & FELD LLP

MICHELLE A. REED

+1 214.969.2713/fax: +1 214.969.4343

mreed@akingump.com

July 8, 2021

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: CSI Financial Services, LLC (“ClearBalance”) Security Incident

To the New Hampshire Attorney General’s Office:

We are contacting you on behalf of our client, CSI Financial Services, LLC (“ClearBalance”), about a data security incident that involved the personal identifying information of approximately 30 residents of New Hampshire. The affected New Hampshire residents will be notified of this data breach on or about July 9, 2021, substantially in the same form as the letter attached here in **Exhibit A**. ClearBalance further makes this notice on behalf of the healthcare providers for which ClearBalance is a business associate and other banking partners that indicated that they wished to be included in this notice, as listed in the attached **Exhibit B**. Please note that in submitting this notice, ClearBalance does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

What Happened

On April 26, 2021, ClearBalance detected and prevented an attempted unauthorized wire transfer of ClearBalance funds. ClearBalance immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity and contacted the FBI. Through its investigation, ClearBalance determined that there was unauthorized access to certain cloud-based ClearBalance email accounts between March 8, 2021 and April 26, 2021. The forensic specialists were able to confirm that the email environment was secured the same day the fraudulent wire transfer attempt was detected (April 26, 2021) and that the threat was eliminated. ClearBalance thereafter conducted an in-depth review process to analyze the contents of the emails that were accessed to determine what, if any, sensitive information was contained within them.

On June 21, 2021, ClearBalance determined that the compromised emails contained personal identifying information that included personal identifying information of New Hampshire residents. The exposed personal identifying information may have included some combination of

July 8, 2021

Page 2

the following: full name, tax ID, Social Security number, date of birth, other government-issued ID, telephone number, healthcare account number and balance, date of service, ClearBalance loan number and balance, and, for a small subset of individuals, personal banking information (such as the financial institution name, account number, and routing number, but not PIN or access code), clinical information, health insurance information, and full-face photographic image. This incident did not impact ClearBalance's corporate networks or software. There is no evidence at this time of any fraud or misuse of the data involved.

ClearBalance also engaged a third party who put impacted individual contact information into a consistent format and validated relevant contact information for notification. This investigation was a time-consuming process, but ClearBalance believed it was necessary to ensure appropriate precautions and that proper next steps were taken.

Steps to Protect Your State Residents

ClearBalance is providing New Hampshire residents identity theft protection services through IDX, a well-known data breach and recovery services expert that specializes in consumer support. IDX identity theft protection services include 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. CyberScan monitoring includes Dark Web monitoring of underground websites, chat rooms, and malware to identify trading or selling of any personal identifying information. ClearBalance is also providing all individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Lastly, ClearBalance is also notifying regulators as required.

To prevent similar events from occurring in the future, ClearBalance's forensic specialists assisted in determining additional security measures designed to prevent incidents of this kind in the future. ClearBalance also took significant steps to enhance security safeguards for information in its care. These measures included changing all user account passwords, implementing stronger access controls in the cloud email environment, and providing updated procedures for reporting suspicious activity.

July 8, 2021
Page 3

Contact Information

If you have any further questions regarding this incident, please do not hesitate to contact me either by telephone at (214) 969-2713, or by email at mreed@akingump.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Michelle A. Reed". The signature is written in a cursive style with a large, stylized initial "M".

Michelle A. Reed

EXHIBIT A



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

To Enroll, Please Visit:
<https://response.idx.us/clearbalance>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

July 9, 2021

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

CSI Financial Services, LLC (“ClearBalance”) writes to inform you of a data security incident at ClearBalance that involved some of your personal information. As you may know, ClearBalance services loans made by <<Bank>> to patients of hospitals or healthcare providers <<including hospital/healthcare provider>> to finance medical expenses. Although we have no evidence at this time that your information has been misused for identity theft or fraud, we are contacting you to explain the circumstances of this data security incident, and to provide information about the service we will provide to help you protect yourself.

What Happened?

On April 26, 2021, ClearBalance detected and prevented an attempted unauthorized wire transfer of ClearBalance funds. We immediately engaged a forensic investigator to aid in an investigation and contacted the FBI. Through our investigation, we determined that there was unauthorized access to certain ClearBalance email accounts between March 8, 2021 and April 26, 2021. On June 21, 2021, our investigation also determined that there was unauthorized access to emails that contained personal information related to certain individuals participating in the ClearBalance program, including you. This incident did not impact our corporate networks or software, and did not involve the systems, databases, or medical records systems of any hospital, healthcare provider, or bank. Again, at this time, we have no evidence of any fraud or misuse of your information.

What Information Was Involved?

The personal information impacted by this incident included your <<Variable text field for each individual. Not all individuals will have all data elements listed: Name, tax ID, social security number, date of birth, other government-issued ID, telephone number, healthcare account number and balance, date of service, ClearBalance loan number and balance, personal banking information (such as the financial institution name, account number and routing number, but not your PIN or access code), clinical information, health insurance information, and full-face photographic image.>>.

What We Are Doing.

We take the security of the data entrusted to us very seriously. Upon learning of this incident, we immediately took steps to identify and remediate the cause of the compromise, including changing the passwords for the compromised email accounts, and to determine what information was impacted. We engaged an external forensic investigator to aid our investigation and our remediation efforts. This forensic investigator was able to confirm that our email environment was secured the same day the fraudulent wire attempt was detected (April 26, 2021) and that the threat was eliminated.

To prevent similar events from occurring in the future, we also took significant steps to enhance the security safeguards for information in our care. These measures included changing all user account passwords, implementing stronger access controls on our network and providing updated procedures for reporting suspicious activity.

Although we have no evidence that any of your personal information has been misused as a result of this incident, to help relieve concerns following this incident, we are offering identity theft protection services through IDX, a well-known data breach and recovery services expert that specializes in consumer support. IDX identity theft protection services include 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. CyberScan monitoring includes Dark Web monitoring of underground websites, chat rooms, and malware to identify trading or selling of any personal information. With this protection, IDX also will help you resolve issues if your identity is compromised.

What You Can Do.

We encourage you to enroll in free IDX identity protection services by visiting <https://response.idx.us/clearbalance> or by calling 1-833-406-2409 and using the Enrollment Code provided above. Please note that we are unable to independently take this step for you. IDX representatives are available Monday through Friday from 9 am to 9 pm Eastern Time. Please note the deadline to enroll is October 9, 2021. You will need to reference the enrollment code at the top of this letter when enrolling, so please do not discard this letter.

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.

For More Information.

In addition to enrolling in the complimentary identity protection and credit monitoring services described above, we encourage you to please review the enclosed “Recommended Steps to Help Protect Yourself,” which describes other steps you can take to help protect your personal information. These steps include recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

If you have any questions or would like to learn additional information about this incident, the IDX representatives available at 1-833-406-2409, Monday through Friday from 9 am to 9 pm Eastern Time, can help you. We regret that this incident has occurred and apologize for any concerns or inconvenience that it may cause.

Sincerely,



Michelle Tygart
Chief Compliance Officer

(Enclosure)



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://response.idx.us/clearbalance> 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 IDX identity protection 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, IDX will be able to assist you.

3. 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 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 IDX identity protection, notify them immediately by calling or by logging into the IDX 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.

4. 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

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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. If you are a victim of identity theft, you have the right an extended fraud alert which is good for 7-years.

A credit freeze does not apply to any person or entity, or its affiliates, or collection agencies acting on behalf of any person or entity that you have an existing account or loan with and requests information in your credit report for the purpose of reviewing or collecting outstanding balances on a credit card or other credit account, loan, or other bills. This information includes activities related to account maintenance, monitoring credit line increases, loan and account upgrades, and loan approvals.

The credit reporting agencies have 3-business days after receiving your request to place a credit freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5-business days and provide you with a unique personal identification number (“PIN”) or password or both that can be used by you to authorize the removal of or a temporary or permanent lifting of the credit freeze to allow creditors to access your credit report.

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

5. 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.

6. 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: This notification was not delayed by law enforcement. Visit the California Office of Privacy Protection (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, 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, 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, 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, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, 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, Telephone: 401-274-4400. Approximately 23 Rhode Island residents were impacted in this data security incident.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General’s Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

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

EXHIBIT B

New Hampshire

Entities Affected:

Palomar Health (1 impacted)

MetaBank (3 impacted)

Western Alliance Bank (26 impacted)