Calibrated Healthcare

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

RE: Notice of Data Breach

Dear <<Full Name>>:

Calibrated Healthcare, LLC ("Calibrated") provides administrative and clinical healthcare services to entities across the United States. We are writing to notify you of a data incident that may impact your information that we received in connection with the services we provide to <<Data Owner/Entity>> on behalf of <<Health Plan/var data 2>>.

What Happened? On February 26, 2024, Calibrated identified suspicious activity related to certain systems within its computer network. In response, Calibrated promptly took the systems offline and began an investigation. The investigation determined that certain portions of Calibrated's network were accessed between February 25 and February 26, 2024, and, during that timeframe, certain files were likely copied without authorization. As a result of that determination, Calibrated initiated a comprehensive review of the data to determine what type of information was present and to whom it relates. This review was recently completed and identified information relating to some of our customers. We began notifying our customers on May 1, 2024, and worked with them to notify potentially impacted individuals, including you.

What Information Was Involved? While we have no evidence that any of your information has been used for identity theft or fraud, our investigation determined that the following information was present in the reviewed files and may have been impacted: name, <<Breached Elements>>.

What We Are Doing. In response to this incident, we dedicated significant resources to confirming the security of our network, conducting a comprehensive investigation, and completing a detailed review of the relevant files. We then notified our potentially affected customers and worked with them to provide notice to potentially impacted individuals as quickly as possible. As part of our ongoing commitment to the security of information in our care, we are also reviewing our existing policies and procedures and enhancing our existing security tools.

As an added precaution, we are offering you <<12/24>> months of credit monitoring and identity protection services, through Equifax, at no cost to you. If you wish to activate these services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information* section on the next page of this letter. Please note you must enroll in these services directly, as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Again, additional information and resources may be found in the *Steps You Can Take to Help Protect Personal Information* section on the next page of this letter.

For More Information. If you have additional questions regarding this incident, please call our dedicated call center at 888-596-6176, which is available between 6:00 am and 6:00pm PST, Monday through Friday.

Sincerely,
Calibrated Healthcare

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

EQUIFAX®

<Full Name>
Enter your Activation Code: <*ACTIVATION CODE*>
Enrollment Deadline: <Enrollment Deadline>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 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.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

ATTENTION: Language assistance services, free of charge, are available to you. Call 888-596-6176	English
ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 888-596-6176	Spanish
注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 888-596-6176	Chinese
ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 888-596-6176-1	Arabic
주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다 888-596-6176 번으로 전화해 주십시오.	Korean
ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 888-596-6176	Russian
ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 888-596-6176	Italian
ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 888-596-6176	French
ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 888-596-6176	Creole
אויפמערקזאם: אויב איר רעדט אידיש, זענען פארהאן פאר אייך שפראך הילף סערוויסעס פריי פון 888-596-6176-1	Yiddish
UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 888-596-6176	Polish
PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 888-596-6176	Tagalog
লক্ষ্য করুনঃ যদি আপনি বাংলা, কথা বলতে পারেন, তাহলে নিঃখরচায় ভাষা সহায়তা পরিষেবা উপলব্ধ আছে। ফোন করুন ১888-596-6176	Bengali
KUJDES: Nëse flitni shqip, për ju ka në dispozicion shërbime të asistencës gjuhësore, pa pagesë. Telefononi në 888-596-6176	Albanian
ΠΡΟΣΟΧΗ: Αν μιλάτε ελληνικά, στη διάθεσή σας βρίσκονται υπηρεσίες γλωσσικής υποστήριξης, οι οποίες παρέχονται δωρεάν. Καλέστε 1-888-596-6176	Greek
خبردار: اگر آپ اردو بولتے ہیں، تو آپ کو زبان کی مدد کی خدمات مفت میں دستیاب ہیں ۔ کال 888-596-6176	Urdu
خدمات کمک زبان به صورت رایگان در اختیار شما قرار می گیرد. زنگ زدن 888-596-6176]	Farsi
Dịch vụ hỗ trợ ngôn ngữ được cung cấp miễn phí cho bạn. Gọi 888-596-6176]	Vietnamese

Calibrated Healthcare complies with applicable federal civil rights laws and does not discriminate, exclude people, or treat them differently on the basis of, or because of, race, color, national origin, age, disability, or sex. Calibrated Healthcare is providing free aids and services to people with disabilities to communicate effectively with us, such as qualified sign language interpreters, and written information in other formats (large print, audio, accessible electronic formats, other formats). Calibrated Healthcare is providing free language services to people whose primary language is not English, such as qualified interpreters and information written in other languages. If you need these services, please call 888-596-6176. If you believe that Calibrated Healthcare has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance in person, by phone, or mail at:

Calibrated Healthcare
3633 Inland Empire Boulevard, #301
Ontario, CA 91764
(866) 955-0044

You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, electronically through the Office for Civil Rights Complaint Portal, available at https://ocrportal.hhs.gov/ocr/portal/lobby.jsf, or by mail or phone at:

U.S. Department of Health and Human Services
200 Independence Avenue, SW Room 509F, HHH Building Washington, D.C. 20201
1-800-368-1019 (TTY: 1-800-537-7697)

Complaint forms are available at http://www.hhs.gov/ocr/office/file/index.html.

You can also file a civil rights complaint with the California Department of Health Care Services, Office of Civil Rights by phone, in writing, or electronically:

- By phone: Call 1-916-440-7370. If you cannot speak or hear well, please call 711 (Telecommunications Relay Services).
- In writing: Fill out a complaint form or send a letter to: Deputy Director, Office of Civil Rights
  Department of Health Care Services
  Office of Civil Rights
  P.O. Box 997413, MS 0009
  Sacramento, CA 95899-7413
  Complaint forms are available at http://www.dhcs.ca.gov/Pages/Language_Access.aspx.
- Electronically: Send an email to CivilRights@dhcs.ca.gov

Breach Help

Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

Credit or Debit Card Number

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

Credit Card

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to $50 when you report them, and most banks have a zero-liability policy.[1]

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

Debit Card

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

2. Report any unauthorized transactions to your bank immediately to avoid liability. Your liability for fraudulent transactions is limited to $50 if you report them within two days. Your bank may have a zero liability policy. But as time passes, your liability increases, up to the full amount of the transaction if you fail to report it within 60 days of its appearance on your bank statement.[2]

3. Consider cancelling your debit card. The card is connected to your bank account. Cancelling it is the safest way to protect yourself from the possibility of a stolen account number being used to withdraw money from your bank account. Even though it would likely be restored, you would not have access to the stolen money until after your bank has completed an investigation.

Social Security Number

Here's what to do if the breach notice letter says your Social Security number was involved.

1. Contact the three credit bureaus. You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. What it means to put a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed. For information on a stronger protection, a security freeze, see ***How to Freeze Your Credit Files*** at *www.oag.ca.gov/privacy/info-sheets*.

3. Review your credit reports. Look through each one carefully. Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4. If you find items you don't understand on your report, call the credit bureau at the number on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to contact the creditors involved and report the crime to your local police or sheriff's office.

Password and User ID

In the case of an online account password breach, you may receive a notice by email or when you go to the log-on page for your account. Here are steps to take if you learn that your password and user ID or email address, or perhaps your security question and answer, were compromised.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.

2. If you use the same password for other accounts, change them too.

3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.

4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.

5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.

   Example: "I love tropical sunsets" becomes 1luvtrop1calSuns3ts!

6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation (*www.eff.org*) lists some free versions and computer magazines offer product reviews.

Bank Information

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)

2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

Driver's License Number

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at *dlfraud@dmv.ca.gov*. Do not include personal information on your e-mail.

Medical or Health Insurance Information

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.

2. If the letter says your health insurance or health plan number was involved, contact

your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow up on it with your insurer or plan. For more on medical identity theft, see ***First Aid for Medical Identity Theft: Tips for Consumers***, at *www.oag.ca.gov/privacy/info-sheets*.

For more details on what to do if you suspect that your information is being used to commit identity theft, see the ***Identity Theft Victim Checklist*** at *www.oag.ca.gov/idtheft/information-sheets*.

NOTES

[1] Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

[2] Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.