DORROS
LAW

August 5, 2022

Via E-Mail to Member Services: Monika.Cooper@cc.cccounty.us
Monika L. Cooper
Assistant County Counsel
Tort and Civil Rights Litigation Division
Contra Costa County Counsel's Office

Re: S.B. v. Contra Costa Regional Medical Center
Notice of Claim / Presentation of Claim

Claim Information
Claimant: *S.B. ("Client")*
Date of/Date Learned of PHI Breach: *February 20, 2022*
Provider: *Contra Costa Regional Medical Center ("Hospital"*

Dear Monika:

It was a pleasure speaking with you on Friday. Thank you for bearing with the noise in the background from Comic-Con. It is rather fun, admittedly, that the non-PHI side of my practice literally allows me to say I can go to Comic-Con for business. I hope you had a nice weekend.

Again, thank you for the call. I do believe it was very productive. Please allow this letter to summarize the substance of our call and also to constitute my client's formal notice of claim for submission to County Board of Directors. Please of course let me know if I have misstated anything from our call. I have done my best to relay the substance of our call as accurately as possible, but if indeed I have misstated something please let me know and accept my apologies up front. Per our conversation please accept this letter as my client's' formal notice of claim.

Preliminarily, we discussed that I generally try to avoid these notice of claims in these PHI privacy violation matters for the literal fact that we are dealing with privacy and by their very nature notices of government tort claims are public. We discussed my preferred route of looking toward a tolling agreement relative to the statute of limitations to avoid the need for a notice of claim at all, however unfortunately such in and of itself would require Board approval and thus due to timing it may not be the best option in this case. Secondarily I mentioned that I have handled notices of claims in privacy matters where I only use the initials of the plaintiff/claimant to try to maintain confidentiality. We agreed that in this case this may be a preferred option rather than crossing our fingers on the tolling agreement possibility.

As a formality, I will just indicate for the Board that the County's counsel/Legal Department is fully familiar with the name of the claimant/plaintiff as well as the facts and allegations regarding this claim. My client's, the claimant's, initials are S.B. I have also attached a copy of the initial notice of PHI privacy breach sent to the County's hospital, albeit redacted for privacy reasons. (**Exhibit 1**) I am also attaching a copy of the County/hospital's breach notice letter to S.B. Under relevant PHI privacy law, when a provider, such as the County hospital, confirms that a PHI privacy breach has occurred it is required to send the patient a breach notice letter confirming the occurrence of the PHI privacy breach, and describing the facts and circumstances surrounding or resulting in the breach, as well as the actions or steps taken by the provider once the breach was discovered, among other items. (**Exhibit 2**)

From our call I understand that the Hospital has identified the individual involved, responsible for the breach, and that such person was an employee of the Hospital at the time of the breach—well technically an employee by way of contract services and thus the Hospital intends to bring in the contract employment company

DORROS LAW
8730 Wilshire Boulevard, Suite 350
Beverly Hills, California 90211
Phone: (310) 997-2050 Fax: (310) 496-1320
www.dorroslaw.com

for purposes of indemnification or similar type joint liability / damages coverage legal theories. We of course would be happy to work with the Hospital / County, along with any third party contractor that the Hospital may believe is relevant, to try to reach resolution of this matter. Fundamentally the PHI privacy breach and liability flowing therefrom falls on the Hospital, however we do understand that the Hospital may also have indemnification type arguments against a third party and again we would be happy to try to coordinate discussions that involve all of the appropriate parties to be able to resolve this matter. However please understand that our position remains that the Hospital is the primarily liable party under the PHI privacy laws and would ultimately remain responsible for the damages suffered by our Client, regardless of whether the contract employment company agrees to cooperate in this matter.

With that said, I have set forth some further information in support of our Client's claim against the Hospital/County. To the extent you need further information please of course contact me at any time. I ma happy to have further calls or communications to ensure that the parties are on the same page.

A. The Claimant's initials are S.B. As mentioned above, County counsel are fully familiar with the facts of this claim and the name of the claimant.

B. Please direct all notices and correspondences related to this matter/Claim to this office at:

Torin A. Dorros
Dorros Law
8730 Wilshire Boulevard, Suite 350
Beverly Hills, California 90211
Phone: (310) 997-2050
Fax: (310) 496-1320
E-mail: tdorros@dorroslaw.com

You have authorization to communicate with this office through electronic mail and facsimile as well as mail and express/overnight mail. Often communications via electronic mail is most effective and time efficient.

C. The following is a high level description of the facts and circumstances giving rise to our Client's Claim and claims but should give the Hospital sufficient understanding and information relating to Claimant's Claim. Please understand that some of the facts or evidence remains within the control of the Hospital and thus fundamentally would be clarified through discovery. Our Client was a patient of the Hospital. As a result, the Hospital had and maintained, and was responsible for the privacy, security, and confidentiality of our Client's protected health information ("PHI"), including her medical records. However, in violation of the relevant PHI privacy laws, the Hospital failed to protect our Client's privacy and failed to have proper security measures in place to ensure the privacy, security, and confidentiality of our Client's PHI. As a result, our Client's PHI was unlawfully disclosed, used, and released by the Hospital causing very significant damages and emotional distress for our Client.

On or about February 20, 2022, Our Client discovered the privacy breach when she learned that a Facebook page had been created purporting to belong to our Client to which copies of her PHI/medical records had been posted. In fact, and of course, this Facebook page was not created by our Client, but rather another individual whom we believe was an employee or contractor of the Hospital. In fact there are two scenarios and investigation and discovery through litigation will further clarify these facts. It is our Client's belief that a Deandra Bryant is responsible for the actual creation of the Facebook page and posting of the medical records to that page. We believe, but have yet to confirm, that Ms. Bryant is also the Hospital employee/contractor and also responsible for both accessing and disclosing the PHI without authorization. There is, however a second scenario, which factually is slightly different, but from Hospital liability and damages perspective is not really legally significant. The alternative scenario is that while Deandra Bryant was the individual that posted the PHI to Facebook that a separate Hospital employee/contractor unlawfully accessed our Client's PHI and then subsequently unlawfully disclosed it to Ms. Bryant. In truth, regardless of whether the first or second scenario above is the more accurate recitation of the factual history giving rise to the PHI breach, the resulting damages for which the Hospital would be liable remain the same, because but for the PHI breach, our Client's PHI would

not have been unlawfully posted to Facebook, which has resulted in very substantial damages and emotional distress.

Significantly it is worth highlighting that the type of information, type of PHI, that was unlawfully disclosed and ultimately posted to social media for the world to view was very hypersensitive PHI. While all PHI is in an of itself "protected" and required to be kept confidential and subject to the various PHI privacy laws, certain types of PHI, at the most basic of levels, often carry with it increased potential for significant damages if the PHI is improperly used or disclosed. In our Client's case the Hospital disclosed / released PHI related to alleged evidence of STDs and other highly personal and embarrassing information or details. This information was apparently intentionally, disclosed and released for the purpose of harming and causing substantial embarrassment and other damages to our Client. If not intentional, certainly the unauthorized disclosure, use, and/or release of our Client's PHI was negligent and resulted in substantial damages.

D. The Hospital's wrongful conduct has resulted in substantial damages and harm to Claimant for which the Hospital is liable. Claimant has suffered monetary damages, as well as substantial emotional distress, irreparable and ongoing harm, and other damages related to and resulting from the Hospital's conduct.

a. Damages and Injury Related to PHI Privacy Breach

First and foremost PHI privacy violations carry with them the availability for statutory damages, statutory punitive damages, statutory attorneys' fees, statutory litigation costs, and statutory civil penalties, as well as recovery of actual damages and any other relief available under the law. The statutes make it clear that recovery is cumulative and per individual violation. For example, Cal. Civ. Code § 56.35 (the first remedy section of the California Confidentiality of Medical Information Act ("CMIA")) allows for $1,000 in statutory damages, $3,000 in punitive damages, and $1,000 in attorney's fees per violation. Cal. Civ. Code § 56.36 provides for $1,000 in statutory nominal damages and up to $25,000 in civil penalties per violation. Monetary damages are available under both Cal. Civ. Code §§ 56.35 and 56.36. Injunctive relief, attorney's fees, and litigation costs may also be awarded under CMIA. Further, California's Information Practices Act, Cal. Civ. Code §§ 1798 et seq. ("CIPA") provides for a statutory minimum damages of $2,500 per violation for unlawful PHI disclosure such as has occurred in this action. Cal. Civ. Code § 1798.53. Monetary damages are available under both Cal. Civ. Code §§ 1798.48 and 1798.53. CIPA also provides for the award of injunctive relief, reasonable attorneys fees, and litigation costs. Moreover, Claimant believes the Hospital had or should have had prior knowledge of the privacy breaches and failed to notify Claimant of the breaches which would provide for liability under California's privacy breach notice statute, Cal. Civ. Code § 1798.82, a subsection of the California Customer Records Act., Cal. Civ. Code §§ 1798.80 et seq. Monetary damages are also available for violations of the this Act. Thus, for the moment not considering civil penalties, the Hospital faces potential statutory liability of at least $5,000 per violation under Civ. Code 56.35 and 56.36 as Claimant's healthcare provider; plus $2,500 per violation as a PHI privacy violating agency under Cal. Civ. Code § 1798.53—that would be a total of $7,500 per violation. We are aware of at least one privacy breach, however in litigation we intend to have our expert conduct a forensic investigation of the Hospital's EMR system relative to overall HIPAA/HITECH/CMIA compliance, but also as to determine the true number of violations, including unauthorized accesses etc. into our Client's PHI, so as to properly be able to determine the number of discrete violations, each of which carry with them separate statutory damages etc. After handling a substantial number of these PHI privacy breach matters, we are confident that this investigation will reveal that there exist far more than a single breach relative to our Client's PHI. That being said, again, we do know, and the Hospital has confirmed that there exists at least one PHI breach relative to our Client's PHI.

As noted, the above are merely the statutorily available/set forth damages relative to California's relevant statutory PHI privacy statutes. You should understand that the above does not specifically account for monetary damages related to other claims associated with PHI privacy breaches, such as common law and California Constitutional invasion of privacy, negligence/negligence per se, negligent hiring, supervision, and/or retention, breach of contract (of the Hospital's patient privacy policies or the HIPAA privacy agreement likely entered into between the Hospital and Claimant as a Hospital patient), intentional and/or negligent infliction of emotional distress, and (UCL) Cal. Bus. & Prof. Code §§ 17200 type claims. Further, depending upon the facts, the Americans with Disabilities Act also provides for protections against, and liability for, unauthorized disclosure of PHI—for purposes of this Notice of Claim, Claimant may also bring an action pursuant to the ADA, however

further investigation whether the applicability of the Act to Claimant's specific facts. Further, given we believe the Hospital knew, or should have known, of the privacy breaches and failed to provide the requisite statutory notices to Claimant, the Hospital would also be liable for damages under California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., and more specifically related to the privacy breach notice statute, Cal. Civ. Code § 1798.82. As noted above, based upon CIPA, CMIA, and other legal theories or avenues such as Claimant's seeking injunctive relief for the good of the public, i.e. for a public benefit, Claimant will be entitled to her attorneys fees, litigation costs, and other relief in this case.

As noted, the privacy violations have resulted in monetary damages, as well as non-economic damages such as without limitation, severe emotional distress, for which the Hospital is liable. Given the nature of the conduct, punitive damages would also be available. Further, attorneys fees and costs of litigation are specifically provided for under the relevant statutes.

b. Damages and Injury Related to Employment such as Hostile Workplace Environment.

While not intended to be an exhaustive list of the resulting harm from the Hospital and its employees'/contractors' conduct, Claimant has and continues to suffer ongoing damages, emotional distress, and irreparable harm. Notably, it took more than a month for Facebook even to claim that it has removed the post and PHI from Facebook and the Internet, but the reality is that once material has been posted to the Internet it is always on the Internet in one form or fashion. Unfortunately it is virtually impossible to entirely remove information from the Internet, which makes privacy violations where information is posted online all that much more damaging and harmful on many levels. With that said, understandably the unlawful disclosure of PHI and subsequent resulting posting of PHI to social media for the world to view and access has caused substantial emotional distress and trauma for the Claimant, so much so that Claimant has had to seek professional help as a direct result of and to help deal with the aftermath of the privacy violation. Moreover given the intensely embarrassing type of information that was disclosed, and the fact that co-workers specifically became aware of the information, Claimant ultimately was placed in a position where her workplace was so uncomfortable that she had to leave. Had Claimant's PHI not been disclosed by the Hospital, her co-workers would not have become aware of such information and Claimant would still have the income from such job. Indeed, Claimant now faces similar embarrassment on a very routine basis because of the PHI that was disclosed. As mentioned, the PHI was of the type that is hyper sensitive and extremely likely to cause substantial harm and embarrassment if it were to be disclosed / released to unauthorized persons. That is what occurred and the damage and ripple effects have been devastating for Claimant on both a personal and business level.

Again, this should not be considered an all-inclusive or exhaustive list or summary of the various claims that Claimant may file against the Hospital nor the damages or harm suffered by Claimant. However we believe it provides the Hospital sufficient notice that should formal litigation need to proceed that Claimant intends to pursue various claims related to and arising from the Hospital's conduct which has detrimentally impacted her. Claimant would be entitled to substantial damages related to such claims in addition to attorneys fees, litigation costs, and any other relief available under law relative to the conduct and breach. While of course investigation is ongoing, and as mentioned above there is a likelihood that there are more breaches that will be revealed through discovery, we are confident that Claimants case is valued at well over $250,000 not including potential penalties, punitive damages, attorneys fees, or litigation costs.

E. As part of the Notice of Claims process we are also providing you and the Hospital with the below information regarding percipient witnesses and/or Hospital employees/contractors who are or were involved in the facts and conduct giving rise to this Claim. While investigation is ongoing and to be candid much of the information remains in the control of the Hospital, we believe at least the following individuals may have relevant information to this claim: (1) Deandra Bryant; (2) Alex Nielsen, Esq.; (3) Hospital privacy officer or HIMS officer or Compliance office or similar position related to privacy and EMR and PHI compliance; (4) S.B.. This is of course not an exhaustive list and is subject to further investigation and discovery.

F. Should litigation be necessary any action would be for an amount in controversy far in excess of the $25,000 minimum for California State Unlimited Jurisdiction cases. Indeed, exclusive of potential penalties, punitive damages, attorneys fees, or litigation costs, we are confident that this case is valued at well over $250,000.

We look forward to the Hospital's response and, similar to what we have tried to communicate in our prior correspondences, are amenable to and welcome opening up substantial discussions to explore resolution between the parties.

Very Truly Yours,

DORROS LAW

Torin A. Dorros

Torin A. Dorros

LITIGATION HOLD NOTICE AND INSTRUCTIONS

You and/or your company/business ("You"), have been identified as a relevant party/person/entity related to significant concerns that have arisen regarding the facts, circumstances, and matters related to issues identified in the above correspondence, including without limitation those related to Your and/or Your employee's or contractor's violations of our Client's privacy, PHI, and other legal rights, and other conduct referenced in the correspondence and/or prior correspondences between the parties and/or counsel ("Matters"). As such, we request that You read and carefully adhere to the instructions provided herein this Litigation Hold Letter.

The purpose of this correspondence is to ensure that no evidence, or potential evidence, relating to the Matters is lost, altered, deleted, or destroyed. The law requires that, once litigation is foreseeable all potential parties (and requested third parties) must maintain all and not destroy any potentially relevant documents, information and data even if that means holding documents, information and data well beyond minimum periods set out by law or Your or company record-retention policies. Destruction, deletion, loss, or alteration of evidence can cause a party to lose possible defenses, not to mention subject the party (and/or third party) to civil and criminal penalties.

In connection with the Matters, You, the parties, and third parties duly notified hereby, have a legal obligation to preserve all relevant documents, information and data. As indicated, the law requires preservation of all documents, information and data relating to or concerning the matters referenced herein, including, without limitation, any subject matter related to the Matters and Your and third parties' acts and conduct related to the Matters. To the extent You may have a question as to whether Documents, information, and/or data falls under the scope of this Litigation Hold Letter you should take a broad approach and assume that such Documents, information, and/or data are covered by this Litigation Hold Letter and therefore should ensure that such information, documents, and/or data is preserved, as outlined herein.

"Documents, information, and data" as used herein means not only hard copy documents, but also audio recordings, videotapes, e-mails, instant messages, social media posts, social media messages, word processing documents, spreadsheets, databases, calendars, telephone logs, Internet usage files, and all other electronically stored information (including metadata) maintained, created, received, indexed, and/or otherwise recorded, logged, or stored by You, the parties, and/or third parties on computer systems. Sources of the documents and data include, without limitation, all hard copy files, computer hard drives, computer servers, removable media (e.g., CDs, DVDs and flash drives), laptop computers, PDAs, Blackberry devices, cell phones, smartphones, and any other locations where hard copy and electronic data is or may be stored. Keep in mind that any of the above-mentioned sources of relevant information may include personal computers You or Your employees use or have access to at home, or other locations. It also includes inaccessible storage media, such as back-up tapes which may contain relevant electronic information that does not exist in any other form. The above should not be deemed an all-inclusive list of sources of documents, information, and data—Your obligation is to preserve all documents, information, and data.

In order to comply with Your legal obligations, You, the parties (and notified third parties) must immediately preserve not only all existing paper copies of documents, including drafts and revisions, but also all electronically stored information, including drafts and revisions, in its existing electronic format (along with all metadata) that relate or pertain to, without limitation, the matters and issues described or referenced above. In order to comply with this Litigation Hold, You should immediately suspend deletion, overwriting, or any other possible destruction of documents, information, and data related to the Matters, as well as suspend Your current document destruction policy and/or automatic deletion function on Your computers, servers, or other electronic devices.

EXHIBIT 1

DORROS
LAW

March 01, 2022

Via E-Mail to Member Services: member.services@cchealth.org
Privacy Officer
CONTRA COSTA REGIONAL MEDICAL CENTER
2500 Alhambra Avenue
Martinez, CA 94553

Re: S[redacted] Br[redacted] v. Contra Costa Regional Medical Center
Notice of HIPAA/CMIA//PHI Privacy Violations

Dear Privacy Officer:

Dorros Law is retained counsel for S[redacted] Br[redacted] (our "Client") regarding certain serious violations of our Client's privacy rights, including violations of the Health Information Portability and Accountability Act ("HIPAA"), California Confidentiality of Medical Information Act ("CMIA"), and/or other relevant privacy laws and regulations ("PHI Privacy Laws") committed by Contra Costa Regional Medical Center ("You"). We have been engaged to see if we can resolve this serious matter prior to the need for litigation, however, if resolution cannot be achieved expeditiously, litigation or other options will be pursued.

Our Client was Your patient and thus You became privy to, and/or in possession of, our Client's protected private and confidential medical and other personal identifying information ("PHI"). As we are certain You are aware there are serious consequences for a healthcare provider/covered entity's, and/or its employees', violation of its/their privacy obligations relative to a patient's PHI. That is precisely what has occurred.

In violation of our Clients' privacy rights and related PHI Privacy Laws You and/or Your employees or contractors disclosed, used, or released our Client's PHI without authorization, and/or allowed our Client's PHI to be disclosed, used, released, or accessed without authorization, and otherwise failed to properly protect and secure our Client's PHI. In short, You and/or Your employee permitted an unauthorized third party to gain access, obtain, use, and exploit our Client's PHI without our Client's authorization and subsequently our Client's PHI was used in a fashion to try to harm and cause emotional distress, embarrassment, and other harm to our Client. Indeed, our Client's PHI, including an image of her PHI and medical record were specifically uploaded to Facebook in a further attempt to cause damage to our Client.

Please understand that, as a result of Your serious violations of our Client's privacy rights and related PHI Privacy Laws, our Client has suffered significantly including substantial emotional distress not to mention other damages. Moreover, simply as a result of the violations, under CMIA, let alone other bases for liability, including without limitation, common law and California Constitutional invasion of privacy, infliction of emotional distress, negligence and negligence per se, negligent hiring, retention, and supervision, breach of express and/or implied contract, and California Business and Professions Code §§ 17200 et seq., You are liable for actual damages, statutory damages, punitive damages, and attorney's fees.

While there remains the possibility to resolve this matter without the need for litigation, time is of the essence. We will need a response to this letter and realistic progress toward resolution on an expedited basis to avoid the need for court intervention. Therefore, we would request that you contact us within ten days of the date of this letter to discuss this serious matter.

Very Truly Yours,

DORROS LAW

Torin A. Dorros

Torin A. Dorros

DORROS LAW
8730 Wilshire Boulevard, Suite 350
Beverly Hills, California 90211
Phone: (310) 997-2050 Fax: (310) 496-1320
www.dorroslaw.com

LITIGATION HOLD NOTICE AND INSTRUCTIONS

You and/or your company/business ("You"), have been identified as a relevant party/person/entity related to significant concerns that have arisen regarding the facts, circumstances, and matters related to issues identified in the above correspondence, including without limitation those related to Your and/or Your employee's or contractor's violations of our Client's privacy, PHI, and other legal rights, and other conduct referenced in the correspondence and/or prior correspondences between the parties and/or counsel ("Matters"). As such, we request that You read and carefully adhere to the instructions provided herein this Litigation Hold Letter.

The purpose of this correspondence is to ensure that no evidence, or potential evidence, relating to the Matters is lost, altered, deleted, or destroyed. The law requires that, once litigation is foreseeable all potential parties (and requested third parties) must maintain all and not destroy any potentially relevant documents, information and data even if that means holding documents, information and data well beyond minimum periods set out by law or Your or company record-retention policies. Destruction, deletion, loss, or alteration of evidence can cause a party to lose possible defenses, not to mention subject the party (and/or third party) to civil and criminal penalties.

In connection with the Matters, You, the parties, and third parties duly notified hereby, have a legal obligation to preserve all relevant documents, information and data. As indicated, the law requires preservation of all documents, information and data relating to or concerning the matters referenced herein, including, without limitation, any subject matter related to the Matters and Your and third parties' acts and conduct related to the Matters. To the extent You may have a question as to whether Documents, information, and/or data falls under the scope of this Litigation Hold Letter you should take a broad approach and assume that such Documents, information, and/or data are covered by this Litigation Hold Letter and therefore should ensure that such information, documents, and/or data is preserved, as outlined herein.

"Documents, information, and data" as used herein means not only hard copy documents, but also audio recordings, videotapes, e-mails, instant messages, social media posts, social media messages, word processing documents, spreadsheets, databases, calendars, telephone logs, Internet usage files, and all other electronically stored information (including metadata) maintained, created, received, indexed, and/or otherwise recorded, logged, or stored by You, the parties, and/or third parties on computer systems. Sources of the documents and data include, without limitation, all hard copy files, computer hard drives, computer servers, removable media (e.g., CDs, DVDs and flash drives), laptop computers, PDAs, Blackberry devices, cell phones, smartphones, and any other locations where hard copy and electronic data is or may be stored. Keep in mind that any of the above-mentioned sources of relevant information may include personal computers You or Your employees use or have access to at home, or other locations. It also includes inaccessible storage media, such as back-up tapes which may contain relevant electronic information that does not exist in any other form. The above should not be deemed an all-inclusive list of sources of documents, information, and data—Your obligation is to preserve all documents, information, and data.

In order to comply with Your legal obligations, You, the parties (and notified third parties) must immediately preserve not only all existing paper copies of documents, including drafts and revisions, but also all electronically stored information, including drafts and revisions, in its existing electronic format (along with all metadata) that relate or pertain to, without limitation, the matters and issues described or referenced above. In order to comply with this Litigation Hold, You should immediately suspend deletion, overwriting, or any other possible destruction of documents, information, and data related to the Matters, as well as suspend Your current document destruction policy and/or automatic deletion function on Your computers, servers, or other electronic devices.

EXHIBIT 2

CONTRA COSTA HEALTH PLAN
A Division of Contra Costa Health Services
A Culture of Caring for 45 Years

APPEALS, GRIEVANCES & DISPUTES

May 30, 2022

[redacted]

NOTICE OF DATA BREACH

What Happened?

On February 28, 2022, you contacted Contra Costa Health Plan and informed us that your protected health information has been posted to social media.

What Information was Involved?

While we believe the risk to the information is limited, we wanted to notify you the information on the letter containing your lab test results included your name, medical record number, address, date of service, and lab results. This did not include your Social Security Number.

What We Are Doing:

We have no indication to believe that your medical record information is being used for fraud or other criminal activity. All known images and posts made to social media have been deleted as of March 15, 2022.

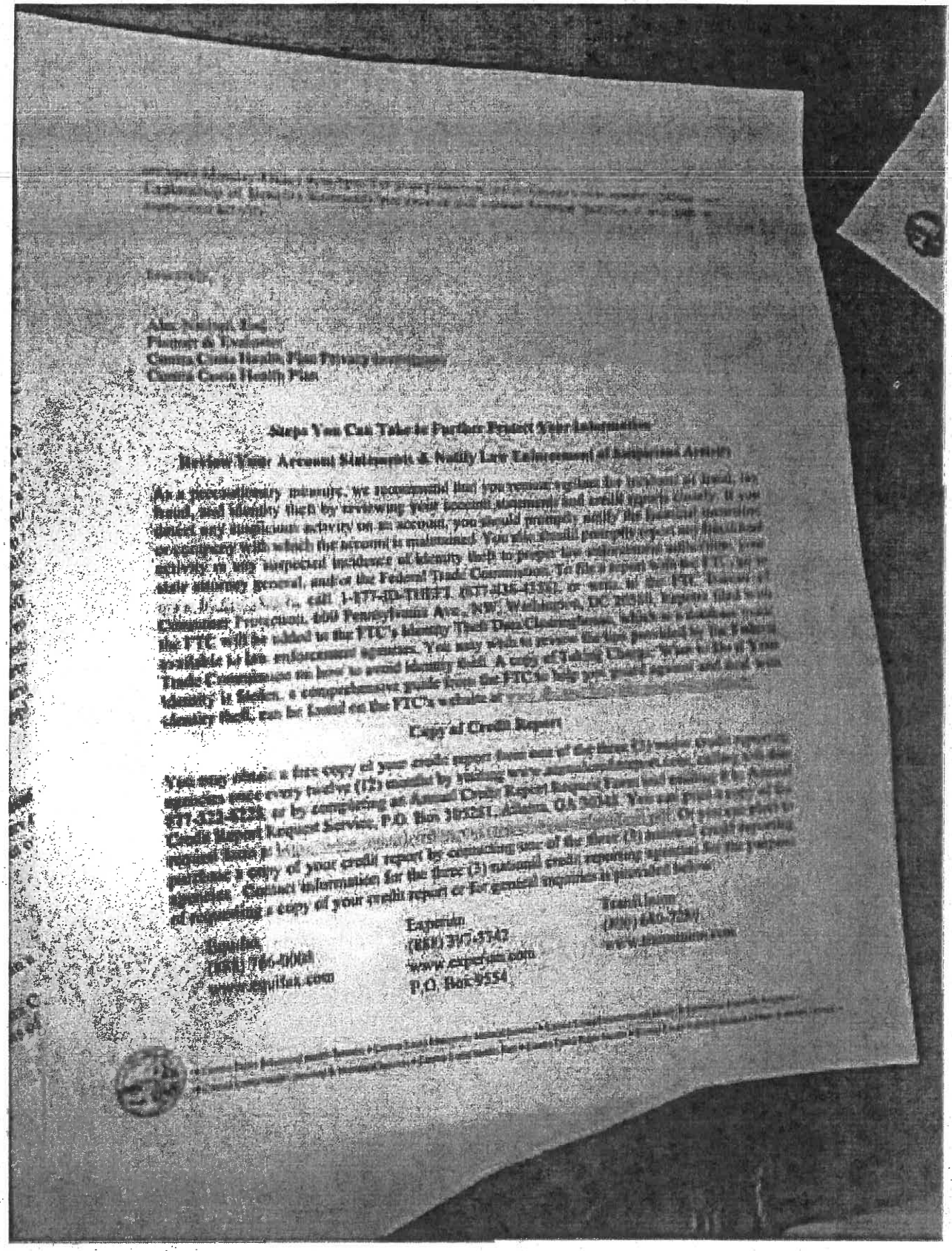
What You Can Do:

Please continue to monitor the social media accounts of your acquaintances who were involved with the initial post. If you believe you are the victim of identity theft, you should contact law enforcement immediately.

We also recommend that you consider taking advantage of the credit monitoring and identity theft services described above. Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information), which provides further information on ways you can protect your information.

FOR MORE INFORMATION:

Protecting your privacy and personal information is important to us, and the County sincerely regrets any inconvenience that this incident may have caused you. CCHP respects your right to file a complaint. If you need any assistance or have further concerns, please contact the CCHP Member Services Department at (877) 661-6230 and press option 2 for help or TTY at 711. They



Planner & Evaluator
Contra Costa Health Plan Privacy Investigator
Contra Costa Health Plan

Steps You Can Take to Further Protect Your Information

Review Your Account Statements & Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a report with the FTC, you may call 1-877-ID-THEFT (877-438-4338), or write to the FTC Bureau of Consumer Protection, 600 Pennsylvania Ave., NW, Washington, DC 20580. Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. A copy of Taking Charge: What to Do If Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at

Copy of Credit Report

You may obtain a free copy of your credit report from one of the three (3) nationwide credit reporting agencies once every twelve (12) months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at

You may purchase a copy of your credit report by contacting one of the three (3) nationwide credit reporting agencies. Contact information for the three (3) national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(888) 766-0008
www.equifax.com

Experian
(888) 397-3742
www.experian.com
P.O. Box 9554

TransUnion
(800) 680-7289
www.transunion.com

P.O. Box 740241
Atlanta, GA 30374

Allen, TX 75013

P.O. Box 2000
Chester, PA 19016

Fraud Alert

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report contact one of the three (3) credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com

Security Freeze

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1 (800) 685-1111	1 (888) 397-3742	1 (888) 909-8872
https://www.freeze.equifax.com	https://experian.com/freeze	www.transunion.com/freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.) Your Social Security Number
Your date of birth (month, day and year)
Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
Include applicable fee. Call or visit each of the credit reporting company websites

NONDISCRIMINATION NOTICE

Discrimination is against the law. Contra Costa Health Plan (CCHP) follows State and Federal civil rights laws. CCHP does not unlawfully discriminate, exclude people or treat them differently because of sex, race, color, religion, ancestry, national origin, ethnic group identification, age, mental disability, physical disability, medical condition, genetic information, marital status, gender, gender identity or sexual orientation.

CCHP provides:

- Free aids and services to people with disabilities to help them communicate better, such as:
  - ✓ Qualified sign language interpreters
  - ✓ Written information in other formats (large print, audio, accessible electronic formats, other formats)
- Free language services to people whose primary language is not English, such as:
  - ✓ qualified interpreters
  - ✓ information written in other languages

If you need these services, contact CCHP between 8 AM - 5 PM by calling 1-877-661-6230. If you cannot hear or speak well, please call TTY 711. Upon request, this document can be made available to you in braille, large print, audio cassette or electronic form. To obtain a copy in one of these alternative formats, please call or write to:

Contra Costa Health Plan
595 Center Ave Ste 100, Martinez, CA 94553
1-877-661-6230 (TTY 711)

HOW TO FILE A GRIEVANCE

If you believe that CCHP has failed to provide these services or unlawfully discriminated in another way on the basis of sex, race, color, religion, ancestry, national origin, ethnic group identification, age, mental disability, physical disability, medical condition, genetic information, marital status, gender, gender identity, or sexual orientation, you can file a grievance with CCHP's Civil Rights Coordinator. You can file a grievance by phone, in writing, in person, or electronically:

- By phone: Contact CCHP between 8 AM - 5 PM by calling 1-877-661-6230. Or, if you cannot hear or speak well, please call TTY/TDD 711.
- In writing: Fill out a complaint form or write a letter and send it to: **CCHP Civil Rights Coordinator, Member Grievance Unit, 595 Center Avenue, Suite 100, Martinez, CA 94553** or fax it to: **1-925-313-6037**.
- In person: Visit your doctor's office or CCHP and say you want to file a grievance.
- Electronically: Visit CCHP's website at www.contracostahealthplan.org.

OFFICE OF CIVIL RIGHTS – CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

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

- By phone: Call **916-440-7370**. If you cannot speak or hear well, please call **TTY/TDD 711 (Telecommunications Relay Service)**.
- 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.

OFFICE OF CIVIL RIGHTS – U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

If you believe you have been discriminated against on the basis of race, color, national origin, age, disability, or sex, you can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights by phone, in writing, or electronically:

- By phone: Call **1-800-368-1019**. If you cannot speak or hear well, please call TTY/TDD **1-800-537-7697**.