

STATE OF NH  
DEPT OF JUSTICE

015 FEB 24 AM 11:38

February 19, 2015

**VIA U.S. MAIL**

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

Re: **Cathrine Steinborn, DDS Data Event**

Dear Sir or Madam:

We represent Dr. Cathrine Steinborn, DDS, 1150 Scott Blvd Suite C2, Santa Clara CA 95050, and are writing to notify you of a data event that may have compromised the security of one (1) New Hampshire resident's personal and protected health information. The investigation into this event is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Dr. Steinborn does not waive any rights or defenses under New Hampshire law.

**Nature of the Data Security Event**

In the early morning of January 5, 2015, Dr. Steinborn's dental office was burglarized, and a server containing patient and responsible party electronic records was stolen. The burglary was promptly reported to the Santa Clara Police Department. To the best of our knowledge, no arrests have been made and the server has not been recovered. Since the burglary, Dr. Steinborn has increased physical security and surveillance of the premises. Dr. Steinborn has also encrypted patient and responsible party information, and enhanced physical security of the server on which this information is stored. Dr. Steinborn's investigation into this incident is ongoing.

Information that may be contained in each valid record includes name, address, date of birth, telephone number, Social Security number, dental and/or medical insurance information, health background information, treatment information, and billing information. The server did not contain bank account, driver's license, or credit/debit card information. Dr. Steinborn's office is unaware of any actual or attempted misuse of the information stored on the server at the time of the theft.

### **Notice to New Hampshire Residents**

Although the office's investigations are ongoing, it appears that the security of four (4) New Hampshire residents' personal and protected health information is affected by this incident. Dr. Steinborn's office mailed written notice to the last known address of each record holder, including the New Hampshire residents, on January 9, 2015. The office supplemented this written notice on January 13, 2015. Copies of these letters are attached hereto as *Exhibit A*.

On or about February 18, 2015, Dr. Steinborn's office provided additional written notice to affected individuals including information on how to protect against identity theft and fraud, as well as instructions on how to enroll and receive one free year of credit monitoring and identity restoration services. A copy of the February 18, 2015 letter is attached hereto as *Exhibit B*. On February 20, 2015, Dr. Steinborn's office will issue a press release and post conspicuous notice about this incident on its website. A copy of the press release and website statement is attached hereto as *Exhibit C*.

### **Other Steps Taken and To Be Taken**

In addition to providing written notice of this incident and access to one free year of credit monitoring and identity restoration services to all affected individuals, Dr. Steinborn's office is also providing notice of this incident to certain federal and other state regulators.



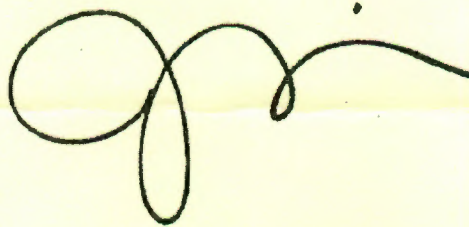
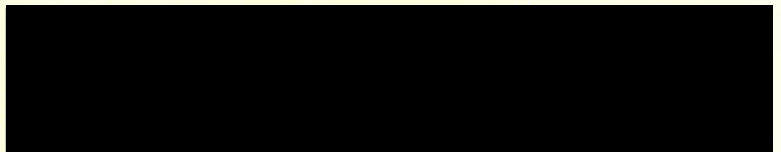
February 19, 2015

Page 3

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at [REDACTED]

Very truly yours,

A handwritten signature in black ink, consisting of a large loop followed by a horizontal line and a small dot.A large black rectangular redaction box covering the printed name and title of the signatory.

JAC

Encl.

cc: Cathrine Steinborn, DDS

# EXHIBIT A

1-9-2015

Dear Patient

I am contacting you about a burglary that occurred in my office that may result in identity theft problems. In the early morning hours, Monday, January 5, 2015, the door was forced open and the server containing your electronic records was stolen. A police report has been filed and we are working with our property manager to enhance the physical security of the building.

Your dental records and radiographs were fully backed up, so there will be no loss of continuity of care. However, your personal identity and insurance information is on the server and could be compromised.

I strongly recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change any existing accounts. You may call any of the three major credit bureaus. A report to one bureau will notify the other two of a fraud alert.

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

Use this document to demonstrate that you are a victim of a data breach to qualify for freezing and monitoring your credit file free of charge.

If you do find suspicious activity on your credit report or have reason to believe your information is being misused, call your local police and file a police report. Many creditors require a police report to absolve you of fraudulent debts. You may also file a complaint with the FTC at: [www.ftc.gov/bcp/edu/microsite/idtheft](http://www.ftc.gov/bcp/edu/microsite/idtheft) or at 1-877-id-theft (1-877-438-4338)

You may be able to protect your information from being used fraudulently by freezing your credit. For information on how, follow the link to:

<https://oag.ca.gov/idtheft/facts/freeze-your-credit>

I apologize for any inconvenience this may cause you.

Sincerely,

*C Steinborn*

Cathrine Steinborn DDS  
1150 Scott Blvd. Suite C2  
Santa Clara CA 95050

1-13-2015

Dear Patient,

We have received many questions regarding the possible data breach that occurred as a result of the theft of our computer. By addressing the questions in a group email, I hope many more people will benefit.

- 1) Santa Clara Police Report # 15-134. Phone #408-615-4700
- 2) We do not store any of your credit card or bank/check information.
- 3) We do not have your driver's license number or a photo of it.
- 4) We have the following in our files:
  - A) Name, address, phone, insurance information, DOB and group number.
  - B) Social Security number, except for children.
  - C) Your health history and dental records.
- 5) It is recommended that you place a fraud alert with a credit reporting agency. It is good for 90 days and is free. You can renew every 90 days indefinitely. The agency will offer you other programs, but these will have a cost.
- 6) A credit freeze provides the greatest protection from identity theft. In California, a freeze is free to victims of identity theft, which is why I have provided the police report case number.
- 7) Our server had two levels of password protection, but was not encrypted.
- 8) Currently, our files are in the cloud, in an encrypted form.
- 9) I will be having the new server encrypted. An IT specializing in HIPAA will complete a thorough risk evaluation and we will be implementing robust physical and IT security going forward.
- 10) The correct phone number for Experian is 888-397-3742

Thank you for all your concerned feedback.

Cathrine Steinborn DDS  
408-243-4216



# EXHIBIT B

cathrine steinborn d.d.s.

Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Name>>  
<<Address1>>  
<<Address2>>  
<<City, State ZIP>>

<<Date>>

Dear <<Name>>,

As a follow up to my previous correspondence, I am writing to provide you with additional information about the January 5, 2015 burglary at our office and helpful information on how to protect against identity theft and fraud. We remain unaware of any actual misuse of your personal and protected health information.

**What happened?** As you know, our office was burglarized on January 5, 2015. Among other things, the intruder(s) took a server containing patient and responsible party information. While our investigation into this incident is ongoing, we've determined that your address, [date of birth], [telephone number], [Social Security number], [insurance information], [medical information], [treatment information], [billing information] and name were stored on the server at the time of the theft. **The server did not contain your bank account or credit/debit card information, as we do not store this information.**

**What we are doing.** We reported this matter to law enforcement and filed a police report immediately upon discovery of the burglary. Since the burglary, we have increased physical security and surveillance of the premises. We have also encrypted patient and responsible party information, and enhanced physical security of the server on which this information is stored. We previously provided notice of this incident to you, and are providing you additional information about the incident and helpful information on protecting against identity theft and fraud. To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

#### Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **May 31, 2015** (Your code will not work after this date.)
2. Visit the **ProtectMyID Web Site to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)**
3. PROVIDE Your Activation Code: [code]

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **PC91983**

#### Additional details regarding your 12-MONTH ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.



- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance\*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

**What you can do.** You can review the enclosed helpful information on how to protect against identity theft and fraud. You can also enroll to receive the free year of credit monitoring and identity restoration services we are offering to you. Should you have any questions about the content of this letter, enrollment in the Experian ProtectMyID product, or ways you can protect yourself from the possibility of identity theft or fraud, please call our confidential hotline between 6:00 a.m. PST to 6:00 p.m. PST, Monday to Friday, at 888-653-5244.

The security of our patients' personal information is of the utmost concern to us, and we are sorry for any inconvenience and concern this incident may cause you.

Sincerely,



Dr. Cathrine Steinborn, DDS

---

\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## NOTICE OF PRIVACY SAFEGUARDS

To further protect against possible identity theft or other financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed above.

You can also further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov). For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, (888) 743-0023, [www.oag.state.md.us](http://www.oag.state.md.us). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.

For information on your medical privacy rights, we suggest you visit the website of the California Office of Privacy Protection, at [www.privacy.ca.gov](http://www.privacy.ca.gov).

# EXHIBIT C



## **California Dentist Provides Public Notice of Data Security Incident**

SANTA CLARA, CA – February 20, 2015 – Dr. Cathrine Steinborn, DDS, is providing notice of a recent office theft which may affect the security of patient and responsible party personal and protected health information.

On January 5, 2015, Dr. Steinborn's office was burglarized and a server containing patient and responsible party information was stolen. The burglary was immediately reported to Santa Clara Police Department. Since the burglary, Dr. Steinborn's office has increased physical security and surveillance of the premises. The office has also encrypted patient and responsible party information, and enhanced physical security of the server on which this information is stored. Dr. Steinborn provided notice of this incident to affected individuals on January 9, 2015, January 13, 2015, and February 18, 2015. Dr. Steinborn's investigation into this incident is ongoing. Information that may be contained in each valid record stored on the server includes name, address, date of birth, telephone number, Social Security number, dental and/or medical insurance information, health background information, treatment information, and billing information. The server did not contain bank account, driver's license, or credit/debit card information.

Although unaware of any actual or attempted misuse of the information stored on the server, Dr. Steinborn is offering each affected individual access to one free year of credit monitoring and identity restoration services. In addition to notifying affected patients and responsible parties about this incident, Dr. Steinborn is providing notice of this incident to certain federal and state regulators.

Dr. Steinborn's office encourages patients and responsible parties to remain vigilant by reviewing their account statements for any unusual activity, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, (877) 322-8228.

At no charge, individuals can also have the credit bureaus place a "fraud alert" on their credit files. A fraud alert will alert creditors to take additional steps to verify an individual's identity prior to granting credit in the person's name. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, [www.equifax.com](http://www.equifax.com); Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, [www.experian.com](http://www.experian.com); or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, [www.transunion.com](http://www.transunion.com). Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or

(877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. State attorneys general may also have advice on preventing identity theft, and instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, [www.ncdoj.gov](http://www.ncdoj.gov). For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

Dr. Steinborn's office is providing a toll-free confidential call line to address questions and concerns regarding the incident. Individuals with questions or concerns about the incident may call 888-653-5244 between 6:00 a.m. PST to 6:00 p.m. PST, Monday to Friday.