Before the

Federal Trade Commission

Washington, DC 20580

In the Matter of]

]

Henry Schein, Inc.]

(Henry Schein Dental)]

March 14, 2014

STATEMENT OF JUSTIN SHAFER

I, Justin Shafer, have personal knowledge of the facts and matters discussed in thisstatement, and, if called as a witness, could and would testify as follows:

1. I am over the age of twenty-one (21) and am competent to give this statement.

2. I am a computer technician in the field of dentistry and am employed at Onsite Dental Systems, 7704 Sagebrush Ct. S., North Richland Hills, Texas.

3. I graduated from the SMU School of Engineering of Applied Sciences. I hold CompTIA A+ certification and Microsoft Certified Professional 2000 certification with 800 classroom hours.

4. I have been working in the field for over a decade. In my professional work, I routinely assist dentists who use practice management software that stores and processes patient information. As such, I have had to learn the security features of many commercially available products so that I can advise clients how to protect patient data from external and internal threats.

5. I have had numerous contacts with both Henry Schein Dental ("HSD"), Dentrix, and US-CERT concerning security vulnerabilities in Dentrix G5 and the deceptive statements HSD/Dentrixhas made in marketing it. The following is a partial chronology of my findings and contacts:

6. In August 2011, I attended the Dentrix Practice Solutions Summit held in Utah. During a presentation about the to-be-released Dentrix G5 software, we were

told that the patient data on the disk would be encrypted, as would be the TCP/IP packets.

7. Database authentication is a crucial component of data security. For database authentication to work, a username and password are required. Failing to use best practices, Dentrix G5 used a hard-coded authentication username and password. As a result, dentists could neither set nor change the administrator password in G5. Hard-coding passwords is a well-known security risk[1] and is considered a design flaw by NIST.[2]

8. Furthermore, because the login credentials were not only hard-coded, but *the same across all installations of G5*, and because cybercriminals routinely share such login credentials,any hacker who could gain access to the server would be able to easily read the contents of a dental office's patient database in plain text.[3]

9. After the event was over, I received a phone call from a Dentrix executive who said he was puzzled because a developer had been able to access a patient database without having the credentials to do so or being authorized to do so. He asked me how that could have happened. Based on his description, I informed him that one possibility was that the Faircom 9.0 server software incorporated in G5 might be exposing the username and password in unencrypted network packets that could be obtained by "packet sniffing." [4]

10. In March 2012, the month after Dentrix started shipping G5, I downloaded Faircom 9.0 and explored its security. Faircom 9.0 offered various options, including NIST-grade encryption ("Faircom Advanced Encryption," AES) and their own proprietary "encryption"("Faircom Standard Encryption"). Dentrix G5 had incorporated the proprietary version and did not give customers the option of using the AES version.

11. My testing revealed that the administrator's password could be found in RAM in plain text, which was considered insecure even by 2003 standards,[5] much less 2012 standards. I could also find the ADMIN username and password in plain text in network packets, which was also considered insecure even by 2002

[1] https://cwe.mitre.org/data/definitions/259.html
[2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4952
[3] Dentrix would later attempt to address this vulnerability through updates and Hot Fixes, but based on information and belief, they still do not permit administrators to set their own username and password.
[4] Packet sniffers are readily available to network administrators who use them to troubleshoot problems, but are also readily available to cybercriminals who use them to obtain information such as usernames and passwords that are being transmitted in plain text.
[5] http://leetupload.com/database/Misc/Papers/Web%20Papers/discovering_passwords_in_memory.pdf

standards.[6]Because of these vulnerabilities, patient data secured by "Faircom Standard Encryption" could be easily read without a decryption key or password. By definition, then, there really was no encryption since no key was required, and Dentrix's claims of "encryption" were inaccurate and misleading, at best, and fraudulent and deceptive at worst.[7]

12. In April 2012, I started trying to alert dentists to the security vulnerabilities in Dentrix G5. My initial efforts included starting a discussion thread on a popular website called DentalTown. I also created and uploaded a video to YouTube demonstrating how easy it was to bypass G5's "encryption."

13. In addition to trying to alert dentists about the security vulnerabilities, I was also in direct communication with Dentrix to share my findings and concerns about their security vulnerabilities and claims of "encryption." Appendices A, B, and C contain some of my e-mail communications to/from them about their security issues during the period April – June, 2012. Note that I pointed out that Social Security numbers could be read in plain text, which poses a significant risk of identity theft if the patient database is accessed or acquired by a hacker.[8]

14. On May 1, 2012, Michael Allsop, Director of Marketing for Henry Schein Practice Solutions (Dentrix), left me a voicemail. The voicemail said Henry Schein's legal department was looking into my posting the YouTube video. Michael said I might have violated the non-disclosure agreement (NDA) I signed during my 2011 Practice Solutions Summit.[9]Allsop suggested that if I were to bill them, they could pay me a consultation fee, but I should consider removing the video. He repeated the offer and request when I returned his call, and added that I was giving the Dentrix developers a professional black eye. I declined his offer of a consultation fee but agreed to remove the video after making it clear to him that my sole motivation was to get HSD to take the security in G5 more seriously.

15. On August 9, 2012, Dentrix offered me the opportunity to beta-test Dentrix G5 Productivity Pack 1. The service pack was supposed to include some security enhancements. I declined their offer because of the non-disclosure clause in the agreement, but it was my understanding at the time that Productivity Pack 1 included a purported Fix for packet sniffing the password on the network.

[6] http://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself

[7] Although the vulnerability rests in Faircom's module, it was Dentrix's decision to use that option instead of Faircom's Advanced Encryption Standard, which would have provided NIST-grade AES encryption. Similarly, it was Dentrix's decision to hard-code administrator login credentials instead of allowing dentists to set their own credentials.

[8] These are just a small sample of numerous communications via e-mail and phone. Should the Commission need additional documentation that HSD/Dentrix was informed of their misleading marketing claims, I can provide it.

[9] I was not disclosing anything I learned from them or the Summit. To the contrary, I was disclosing what they had not been transparent about – their security design flaws and vulnerabilities.

16. In September 2012, and unrelated to the Dentrix G5 issues described above, I discovered that a dentist using an earlier version of Dentrix had suffered a data security breach, and that his entire patient database with over 11,000 patients' protected health information had been uploaded to a torrent site in plain text. I notified the dentist (Dr. DiGiallorenzo of Williamsport, Pennsylvania). I also notified Dentrix of the breach, as their entire software for Dentrix 11.0 had also been uploaded to the torrent site, where anyone could download their proprietary software. In discussing the breach with Dentrix, I took the opportunity to point out that this breach showed why having genuine encryption for the patient database was important.

17. By October 2012, Dentrix was still advertising G5 as providing encryption but still had not effectively addressed the two major security issues with G5 described previously: the hard-coded credentials issue and the use of "standard encryption" that was not genuine encryption. I informed Dentrix that I might report my concerns to US-CERT.

18. In response, I received a phone call from Howard Bangerter, Dentrix's Product Manager, saying, in part, that the Henry Schein legal team works on Christmas and they are not someone I want to mess around with. In a subsequent call, he asked me if I had noticed who had viewed my LinkedIn account.

19. On October 7, 2012, I alerted the United States Computer Emergency Readiness Team (US-CERT) to the hard-coded credentials issue (Appendix D contains a copy of my e-mail to US-CERT).

20. Also on October 7 2012, I received a voicemail from Howard Bangerter, telling me "I'm not sure you're gonna be happy about what's happened here." At the time, I had no idea what he meant.[10]

21. According to their records, on October 15, 2012, US-CERT notified Dentrix of the packet sniffing vulnerability.[11]

22. Even after submitting a report to US-CERT, I continued trying to encourage Dentrix to stop describing their product as providing "encryption."

[10] I preserved the voicemails mentioned in this statement should they be needed.

[11] Coincidentally, perhaps, shortly thereafter, my mugshot from a 2001 arrest was posted on mugshot.com. It had never appeared on the Internet before and the accompanying text indicated, "This Official Record was collected from a Law Enforcement agency on 10/22/2012." After seeing that, I recalled Bangerter's message about LinkedIn. I checked my infrequently used LinkedIn account and received a notification from LinkedIn that a lawyer from Proskauer Rose had viewed my profile. Proskauer Rose is HSD's external counsel.

23. Despite my efforts, in November of 2012, Dentrix gave an interview in which it promoted G5's encryption as providing greater security and helping dentists comply with HIPAA.[12] After I read the article, I contacted Steve Roberts, Dentrix's Director of Product Strategy. I inquired about the article's claims regarding "storing and transmitting patient data," asking him how Dentrix G5 was storing and transmitting encrypted data without the use of Faircom's Advanced Encryption. I also asked him about the problem of finding the ADMIN hard-coded password that was the same for all Dentrix installations. He told me he would look into the statements Dentrix had given DentalTown in the interview, and told me that Faircom and Dentrix had previously met to review the statements given. I never heard back from Dentrix regarding these issues. Following that email to him, everyone I knew at Dentrix stopped communicating with me, except for Ryan Beardall (Support Operations and Technical Mentor) for Dentrix Technical Support.

24. On December 17, 2012, Dentrix released Productivity Pack 1. My testing revealed that despite their attempt to address the hard-coding vulnerability, I could still find the hard-coded passwords to the Dentrix G5 database.

25. On April 26, 2013, US-CERT released a security advisory that confirmed my findings and concerns about Dentrix G5's hard-coded database credentials.[13] Their advisory included a vendor statement from Henry Schein Dental[14] and recommended users deploy PP1 Hotfix1.[15]

26. On April 29, 2013, I notified US-CERT about Faircom's/Dentrix's claims of "encryption" when there was no encryption but only data obfuscation. I also posted a YouTube video that demonstrated the problem.

27. On June10, 2013, US-CERT released a security advisory regarding flaws in Faircom Standard Encryption.[16]The "encryption" Dentrix G5 had touted in its marketing was described by US-CERT as a "weak obfuscation algorithm that may be unobfuscated without knowledge of a key or password."

[12] http://www.dentaltown.com/dentaltown/article.aspx?i=304&aid=4146

[13] http://www.kb.cert.org/vuls/id/948155

[14] http://www.kb.cert.org/vuls/id/JALR-8ZRHUK HSD is correct that a firewall provides some protection, but given how often firewalls are breached, the hard-coded credentials issue remains a significant concern, and one that HSD could have avoided by allowing customers to set their own login credentials.

[15] Because I had reported still being able to obtain username and password despite Productivity Pack 1, Dentrix came out with PP1 Hotfix 1 in February 2013, and US-CERT listed that as the solution. As subsequent testing revealed, however, Hotfix 1 did not solve the problem, either. I have been able to gain access to Dentrix databases throughout all of the patches released to date, without having physical access to a server.

[16] http://www.kb.cert.org/vuls/id/900031

28. In response to US-CERT rejecting its description as “encryption,” Faircom agreed to re-brand its “standard encryption” option as “data camouflage.”

29. On June 16, 2013, the National Institute of Standards and Technology (NIST) also issued an advisory about Faircom’s “standard encryption.”[17]

30. Despite government concerns and Faircom’s re-branding, from June 2013 until January 2014, Dentrix continued to market G5 as providing “encryption.”

31. In December 2013, I was contacted by “Dissent Doe” of PHIprivacy.net, a patient privacy advocate and breach blogger. Doe was following up on a report on WNEP about the DiGiallorenzo breach I had discovered.[18]She informed me that as a result of her investigation, she, too, had become concerned about Dentrix’s claims of encryption in G5.

32. In January 2014, Doe reportedly spoke with Rhett Burnham of Dentrix to discuss their marketing of G5 as providing “encryption.” According to her report of the meeting(which Dentrix did not dispute), Dentrix maintained that it could continue to call its security “encryption” under HIPAA’s definition. Doe and cryptographers she subsequently interviewed and quoted in her blog entry publicly disagreed.[19] Shortly after she published her concerns with supporting statements by cryptographers, Dentrix reversed their position and re-branded its security in G5 as “data masking.”

33. Since re-branding G5’s security in January 2014, Dentrix has published an article on data security in its newsletter[20] and has had certain advertisements on external sites updated or corrected. It has also replaced references on its website to “encryption” with “data masking.” But it has reportedly declined to send individual notification letters to G5 customers to explain to them that what they purchased and believed was “encryption” was not and is not encryption. [21]

34. Because they marketed weak obfuscation as “encryption” and because they continued to market it that way after it should have been clear that they should not be describing it as encryption, and because they have failed to individually notify those who purchased G5, there may be many dentists still laboring under the misimpression that G5 encrypts their patient data, like the dentist in California

[17] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0148

[18] http://wnep.com/2013/12/09/stolen-data-on-thousands-of-williamsport-area-dental-patients/

[19] http://www.phiprivacy.net/dentrix-claims-it-encrypts-their-data-but-does-it/

[20] http://www.dentrix.com/articles/content.aspx?id=529

[21] http://www.phiprivacy.net/update-does-dentrix-need-to-send-individual-notification-letters-rescinding-its-encryption-claim/

whose computer was stolen and who then innocently but mistakenly reassured his patients that their stolen data were encrypted.[22]

35. Because millions of patients' protected health information continues to remain at risk given the security flaws and vulnerabilities in G5, and because Dentrix made misleading marketing claims that it has not adequately corrected by contacting all its customers inform them, I urge the Commission to take action to protect patients and consumers and to use its authority to address this situation.

(Signed) ________________________________

Justin Shafer

[22] http://www.phiprivacy.net/dentrix-claims-it-encrypts-their-data-but-does-it/

Appendices

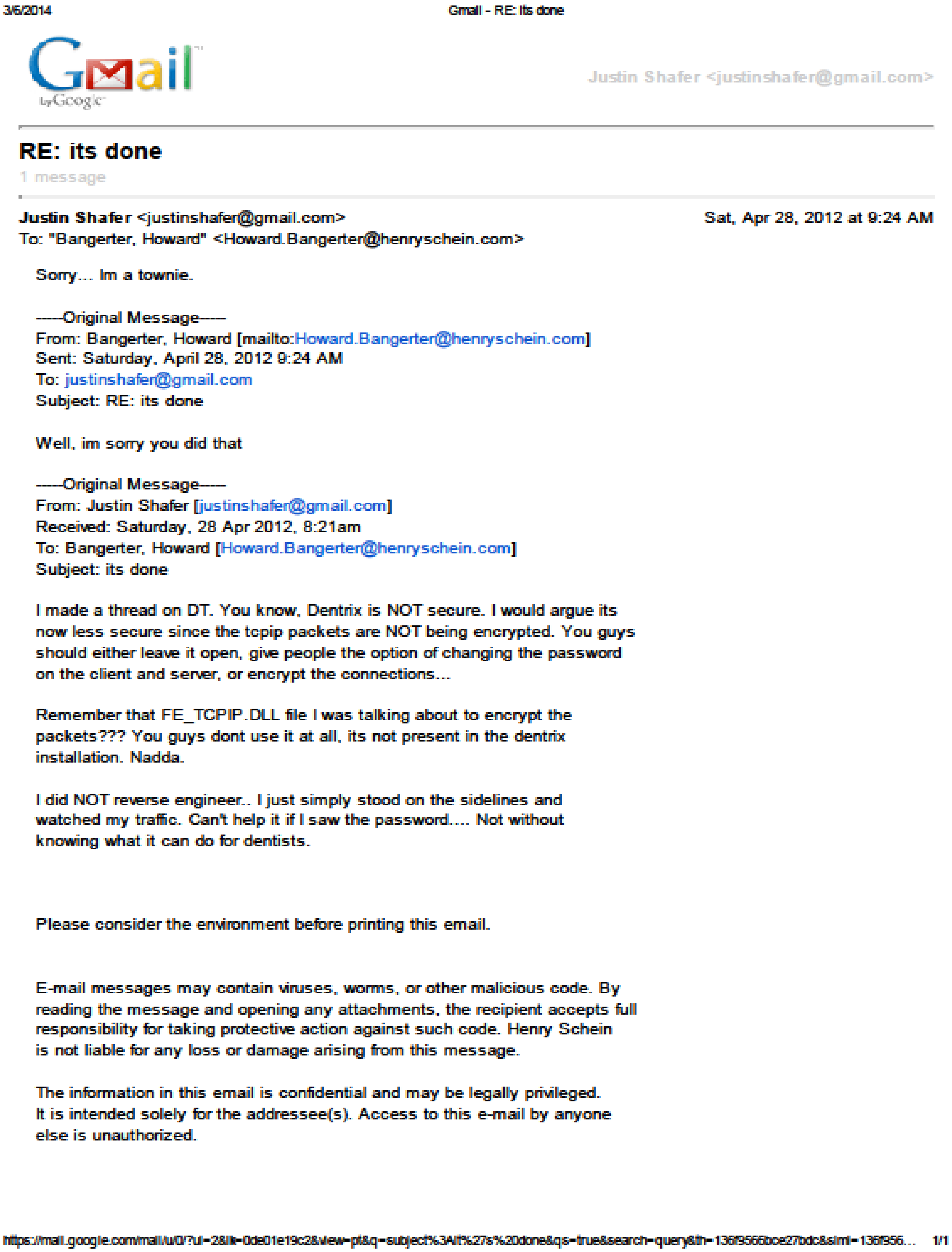
A. Email to Howard Bangerter of Dentrix dated April 28, 2012 regarding unencrypted packets, my post on DentalTown, and a YouTube video I had created.

B. Email to Howard Bangerter dated May 2, 2012 regarding Dentrix G5's lack of true encryption.

C. Email to Howard Bangerter dated June 25, 2012 demonstrating (using fake data displayed in .gif file) that Social Security numbers are exposed in plain text in G5.

D. Email to US-CERT dated October 7, 2012 regarding Dentrix G5 hard coded credentials issue.

Appendix A



3/6/2014 Gmail - RE: Its done

Justin Shafer <justinshafer@gmail.com>

RE: its done

1 message

Justin Shafer <justinshafer@gmail.com> Sat, Apr 28, 2012 at 9:24 AM
To: "Bangerter, Howard" <Howard.Bangerter@henryschein.com>

Sorry... Im a townie.

-----Original Message-----
From: Bangerter, Howard [mailto:Howard.Bangerter@henryschein.com]
Sent: Saturday, April 28, 2012 9:24 AM
To: justinshafer@gmail.com
Subject: RE: its done

Well, im sorry you did that

-----Original Message-----
From: Justin Shafer [justinshafer@gmail.com]
Received: Saturday, 28 Apr 2012, 8:21am
To: Bangerter, Howard [Howard.Bangerter@henryschein.com]
Subject: its done

I made a thread on DT. You know, Dentrix is NOT secure. I would argue its now less secure since the tcpip packets are NOT being encrypted. You guys should either leave it open, give people the option of changing the password on the client and server, or encrypt the connections...

Remember that FE_TCPIP.DLL file I was talking about to encrypt the packets??? You guys dont use it at all, its not present in the dentrix installation. Nadda.

I did NOT reverse engineer.. I just simply stood on the sidelines and watched my traffic. Can't help it if I saw the password.... Not without knowing what it can do for dentists.

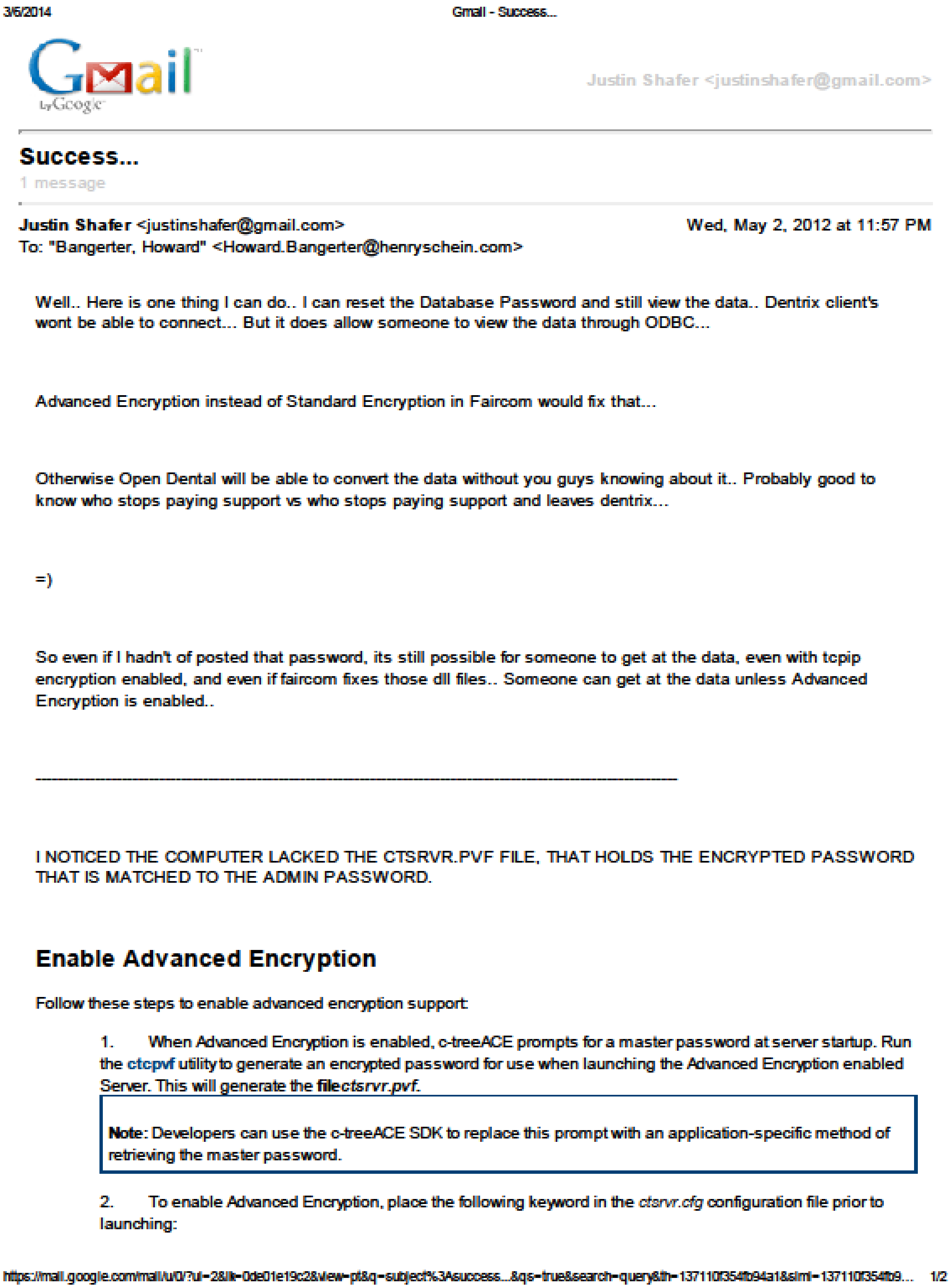
Please consider the environment before printing this email.

E-mail messages may contain viruses, worms, or other malicious code. By reading the message and opening any attachments, the recipient accepts full responsibility for taking protective action against such code. Henry Schein is not liable for any loss or damage arising from this message.

The information in this email is confidential and may be legally privileged. It is intended solely for the addressee(s). Access to this e-mail by anyone else is unauthorized.

https://mail.google.com/mail/u/0/?ui=2&ik=0de01e19c2&view=pt&q=subject%3Ait%27s%20done&qs=true&search=query&th=136f9566bce27bdc&siml=136f956... 1/1

Appendix B



3/6/2014 Gmail - Success...

Justin Shafer <justinshafer@gmail.com>

Success...

1 message

Justin Shafer <justinshafer@gmail.com> Wed, May 2, 2012 at 11:57 PM
To: "Bangerter, Howard" <Howard.Bangerter@henryschein.com>

Well.. Here is one thing I can do.. I can reset the Database Password and still view the data.. Dentrix client's wont be able to connect... But it does allow someone to view the data through ODBC...

Advanced Encryption instead of Standard Encryption in Faircom would fix that...

Otherwise Open Dental will be able to convert the data without you guys knowing about it.. Probably good to know who stops paying support vs who stops paying support and leaves dentrix...

=)

So even if I hadn't of posted that password, its still possible for someone to get at the data, even with tcpip encryption enabled, and even if faircom fixes those dll files.. Someone can get at the data unless Advanced Encryption is enabled..

I NOTICED THE COMPUTER LACKED THE CTSRVR.PVF FILE, THAT HOLDS THE ENCRYPTED PASSWORD THAT IS MATCHED TO THE ADMIN PASSWORD.

Enable Advanced Encryption

Follow these steps to enable advanced encryption support:

1. When Advanced Encryption is enabled, c-treeACE prompts for a master password at server startup. Run the ctcpvf utility to generate an encrypted password for use when launching the Advanced Encryption enabled Server. This will generate the file*ctsrvr.pvf*.

> **Note:** Developers can use the c-treeACE SDK to replace this prompt with an application-specific method of retrieving the master password.

2. To enable Advanced Encryption, place the following keyword in the *ctsrvr.cfg* configuration file prior to launching:

https://mail.google.com/mail/u/0/?ui=2&ik=0de01e19c2&view=pt&q=subject%3Asuccess...&qs=true&search=query&th=137110f354fb94a1&siml=137110f354fb9... 1/2

Appendix C

3/6/2014 Gmail - guess I was wrong...

Gmail by Google

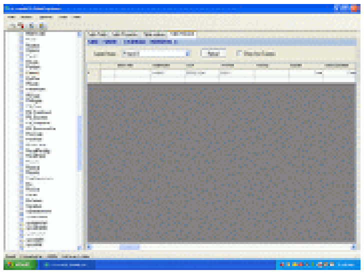
Justin Shafer <justinshafer@gmail.com>

guess I was wrong...

1 message

Justin Shafer <justinshafer@gmail.com> Mon, Jun 25, 2012 at 3:49 AM
To: howard.bangerter@henryschein.com

SSN's are stored plain text in the database...



stuff.gif
43K

https://mail.google.com/mail/u/0/?ui=2&ik=0de01e19c2&view=pt&q=subject%3Aguess%20I%20was%20wrong&qs=true&search=query&th=13822d5b4d0559ad... 1/1

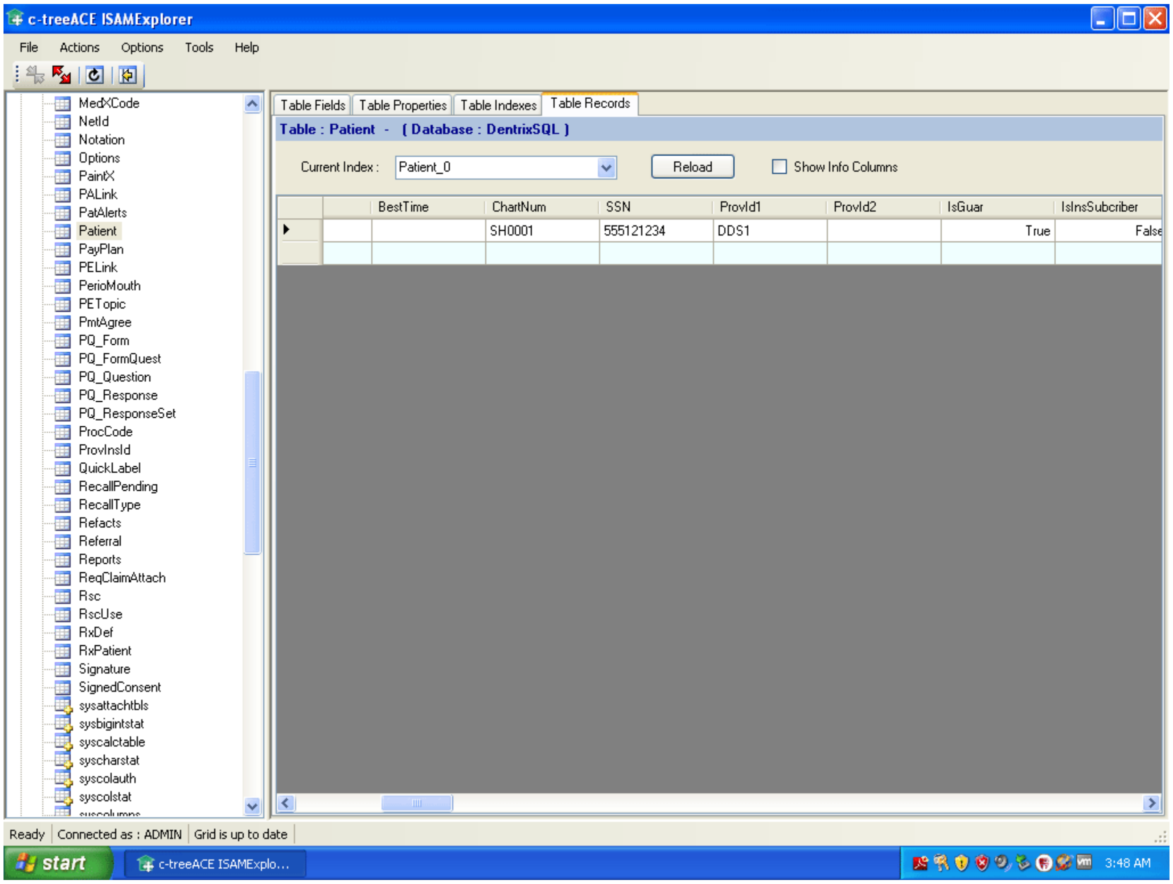


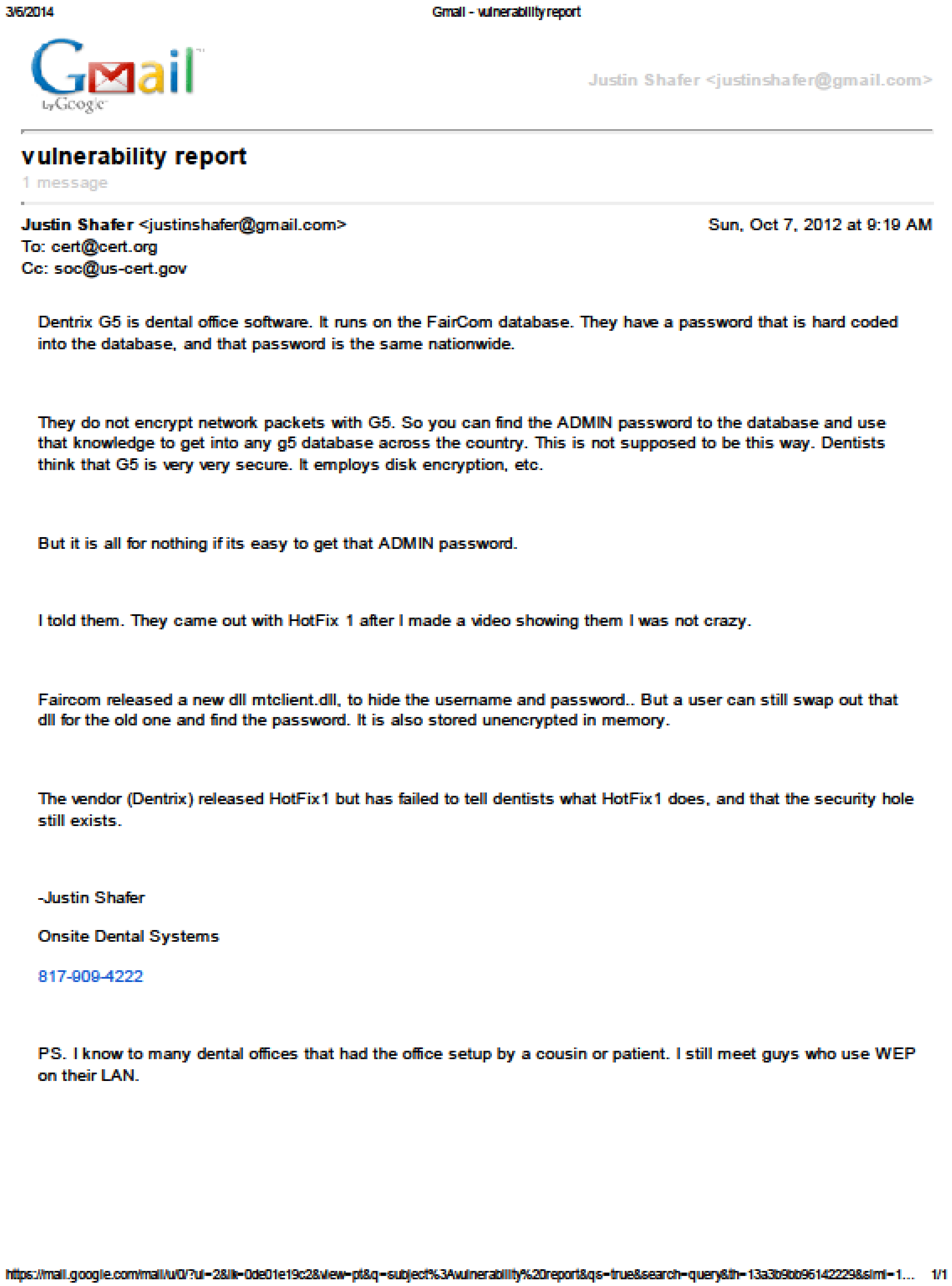
Table : Patient - (Database : DentrixSQL)

Current Index : Patient_0

		BestTime	ChartNum	SSN	ProvId1	ProvId2	IsGuar	IsInsSubcriber
▶			SH0001	555121234	DDS1		True	False

Ready | Connected as : ADMIN | Grid is up to date

Appendix D



3/6/2014 Gmail - vulnerability report

Justin Shafer <justinshafer@gmail.com>

vulnerability report

1 message

Justin Shafer <justinshafer@gmail.com> Sun, Oct 7, 2012 at 9:19 AM
To: cert@cert.org
Cc: soc@us-cert.gov

Dentrix G5 is dental office software. It runs on the FairCom database. They have a password that is hard coded into the database, and that password is the same nationwide.

They do not encrypt network packets with G5. So you can find the ADMIN password to the database and use that knowledge to get into any g5 database across the country. This is not supposed to be this way. Dentists think that G5 is very very secure. It employs disk encryption, etc.

But it is all for nothing if its easy to get that ADMIN password.

I told them. They came out with HotFix 1 after I made a video showing them I was not crazy.

Faircom released a new dll mtclient.dll, to hide the username and password.. But a user can still swap out that dll for the old one and find the password. It is also stored unencrypted in memory.

The vendor (Dentrix) released HotFix1 but has failed to tell dentists what HotFix1 does, and that the security hole still exists.

-Justin Shafer

Onsite Dental Systems

817-909-4222

PS. I know to many dental offices that had the office setup by a cousin or patient. I still meet guys who use WEP on their LAN.

https://mail.google.com/mail/u/0/?ui=2&ik=0de01e19c2&view=pt&q=subject%3Avulnerability%20report&qs=true&search=query&th=13a3b9bb96142229&siml=1... 1/1