

Frequently Asked Questions

Q: What happened?

A: On October 3, 2008, the University of Florida discovered that a server containing a database with restricted information was accessed by an unauthorized intruder from outside UF. The database contained a combination of names, addresses, dates of birth, Social Security Numbers (SSN's), and in some cases, dental procedure billing codes for approximately 336,234 people who were patients at the UF College of Dentistry between 1990 and 2008.

Q: How did this happen?

A: The University of Florida's Privacy Office was notified on October 3, 2008 that a university data system was illegally accessed by an intruder. This data system contains certain unencrypted personal information about University of Florida dental patients. With the incident's discovery, we initiated a security investigation. The FBI was also notified about the breach and is conducting its own investigation. Both investigations are ongoing.

In recent years, UF added and strengthened firewalls and intrusion detection systems, encrypted the data flows containing sensitive information, and increased vigilance in identifying threats and securing servers. Unfortunately, despite these efforts, this intruder was able to exploit UF's systems and gained access to a server that stored a database with patient records by using intrusion scanning tools.

Q: I received a notification letter from the University of Florida about a computer security incident. Does that mean someone stole my personal information?

A: Not necessarily. In this particular incident, we know that an unauthorized intruder accessed a server that contained Personally Identifiable Information (PII) and some personal medical and dental information. At this time, we do not have evidence that your information or anyone else's was viewed and/or downloaded from our server. However because we are not able to guarantee that it wasn't, we are erring on the side of caution by notifying everyone whose information was on that server. An investigation is ongoing.

Q: Will UF contact me to ask for private information because of this event?

A: UF will not contact you to ask for personal information such as your SSN, credit card or banking information. If someone does contact you claiming to represent UF, you should not give out personal information. Unfortunately, in similar circumstances at other institutions, people have reportedly been contacted by individuals fraudulently claiming to represent the university and asking for personal information. UF recommends caution if you receive similar phone calls, e-mails, or text messages.

Q: Why did you have my personal information?

A: The database contained information that was necessary for the college to have a way to identify you (SSN), to know what types of dental procedures we have performed on you (dental procedure codes) in order to bill you correctly, and how to contact you (mailing address). Also, SSN's are used because some payors, such as Medicaid and Medicare, require them for processing billing information.

Q: What personal information was involved? When was it available to the unauthorized intruder?

A: The personal information included a combination of names, dates of birth, addresses, SSN, and some billing codes for patients. The information dates back to 1990. Some patients had only SSN's, some had only Protected Health Information (PHI), which were the dental procedure billing codes, and some had both. We are unable to say exactly when the intruder accessed the server. If you want to know which type of information of yours was on the server, please contact our call center at 1-866-783-5883.

Q: Is this information still at risk of disclosure to an unauthorized person?

A: The database that was illegally accessed has been reconstructed and protected. In addition, the university is conducting an internal audit to identify whether there are similar systems in other colleges and units with the same configuration as the illegally accessed server that could also be vulnerable to illegal access. UF also reported this incident to the FBI which is conducting its own investigation.

Q: If my information was among the files exposed or stolen, does this mean that I will become a victim of identity theft?

A: No. The fact that someone had access to your information does not mean that you are a victim of identity theft or that they intend to use the information to commit fraud. The university notified you about the incident so you can protect yourself. The best way to protect yourself is to place a fraud alert on your credit file and review your credit report. In this incident, we are not certain that anyone's information was viewed or downloaded.

Q: How will I know if any of my personal information was used by someone else?

A: You should place a fraud alert on your credit report or freeze your existing accounts which will alert you if someone is trying to use your personal information illegally. Contact one of the three credit report agencies below:

Equifax - 1 (800) 525-6285

P.O. Box 740241

Atlanta, GA 30374

<http://www.equifax.com>

Experian - 1 (888) 397-3742

P. O. Box 9532

Allen, TX 75013

<http://www.experian.com>

Trans Union - 1 (800) 680-7289

P. O. Box 6790

Fullerton, CA 92834

<http://www.transunion.com>

After you place a fraud alert or freeze, ask that credit agency to send you a credit report. When it arrives, review it carefully. If you find anything that looks wrong or suspicious or that you don't understand, call the credit agency at the telephone number listed on your credit report and review

the report with a member of the staff. If information in the credit report cannot be explained, you may wish to file a report of suspected identity theft with your local police or sheriff's department.

Q: Do I have to pay for the credit report?

A: No. When you place an initial fraud alert on your credit report, you are entitled to one free credit report from each of the three nationwide consumer-reporting companies. Or you may order a free credit report at <http://www.AnnualCreditReport.com>.

Q: What is a fraud alert?

A: Most credit card companies and other creditors won't issue credit without first checking the applicant's credit history. A *fraud alert* tells credit issuers that there is possible fraud associated with the account and gives them a number to call before issuing new credit in your name. This prevents others from fraudulently receiving credit in your name. When you call the credit bureau fraud line, you will be asked for identifying information and will have an opportunity to enter a number for creditors to call. Credit bureaus will send you a confirmation letter which should include instructions on how to order a free credit report. You should then request a credit report.

Q: How long does a fraud alert last?

A: An initial fraud alert lasts 90 days and it is free; you may renew it for an additional 90 days.

Q: Will a fraud alert stop me from using my credit cards?

A: No; a fraud alert will not stop you from using your existing credit cards or other accounts.

Q: Can I still apply for credit after I place a fraud alert on my credit report?

A: Yes, but a fraud alert may slow the process of receiving new credit since the purpose of a fraud alert is to help protect you against an identity thief opening credit accounts in your name. Potential creditors receive a special message alerting them to the possibility of fraud, and they know they should re-verify the identity of a person applying for credit.

Q: What is a Credit or Security Freeze?

A: A notice placed by you that prohibits the credit reporting agency from releasing any credit information to a third party without your written authorization. A freeze is a permanent action, but can be lifted temporarily as needed, using a password. Lenders would not have access to your credit report to approve new credit. Your information can still be released to your existing creditors. To place, you must request in writing to each of the three credit agencies. There is a \$10 fee to place, remove, or temporarily lift. No fee is charged if you provide proof that you are a victim of identity theft or are more than 65 years old.

Q: How else can I request my free annual credit file disclosure?

A: Go to the Identity Theft Resource Center <http://www.idtheftcenter.org/> and the Annual Credit Report site at <http://www.AnnualCreditReport.com>. While credit bureaus offer fee-based monitoring services, it is up to individual parties to determine whether they wish to pay for such services.

Q: Should I order all my credit file disclosures at one time or space them out over 12 months?

A: It is entirely your choice whether you order all three credit reports at the same time or order one now and others later. The advantage of ordering all three at the same time is that you can compare them. On the other hand, the advantage of ordering one now and others later is that you can keep

track of any changes or new information that may appear on your credit report (for example, one credit report every four months). Remember, you are entitled to receive one free credit report through <http://www.AnnualCreditReport.com> every 12 months from each of the nationwide consumer credit reporting companies such as Equifax, Experian and TransUnion. If you order from only one company today you can still order from the other two companies at a later date.

Q: I called the credit bureau fraud line and they asked for my Social Security number. Is it okay to give it?

A: The credit bureaus ask for your Social Security number and other information to identify you and avoid sending your credit report to the wrong person. However, UF advises caution if you are contacted by someone who claims to represent UF and asks for personal information. UF will not contact you but instead will wait for you to contact us if you have any additional questions. In the case of a fraud alert, potential creditors will contact you to confirm your identity before issuing new credit in your name.

Q: Do I have to call all three credit bureaus?

A: No; you only need to contact one and request that credit bureau pass your request for fraud alert to the other bureaus.

Q: Why can't I talk to someone at the credit bureaus?

A: Each of the three bureaus uses an automated telephone system. If you are having difficulty reaching one, try another.

Q: How long does it take to receive my credit report?

A: Your report will be mailed to you within 15 days. Please allow 2-3 weeks for delivery.

Q: What is Credit Monitoring and do I have to pay for the Service?

A: Credit monitoring services protect you primarily against new account fraud. This form of fraud occurs when a criminal uses your personal information to open credit card, mobile phone, or other financial accounts using your name, Social Security number, and other personal information. Credit monitoring does not actually stop the opening of new accounts, but it usually enables you to learn about the fraudulent accounts sooner than it takes for debt collection companies to track you down. You must pay for the use of a credit monitoring service.

Q: Why doesn't UF buy a years' credit monitoring subscription for me?

A: UF does not pay for credit monitoring services. By utilizing the free fraud alerts and reviewing free credit reports for suspicious activity, you can engage in periodic monitoring of your own credit. Additionally, independent research by a consumer watchdog group indicates most credit monitoring services are ineffective. For further information about the effectiveness of credit monitoring services, go to <http://www.privacyrights.org/fs/fs33-CreditMonitoring.htm#1>.

Q: Should I contact the Social Security Administration and change my Social Security number?

A: The Social Security Administration very rarely changes a person's Social Security number. The possibility of fraudulent use of your number probably would not be viewed as justification. Also, there are drawbacks to changing your Social Security number. For example, you would lose your credit history, which could make it difficult to get new credit, go to college, rent an apartment, open a bank account or get health insurance.

Q: Should I close my bank account?

A: No; the illegally accessed database does not include any information about bank accounts.

Q: Should I close my credit card or other accounts?

A: No; the illegally accessed database does not include any information about credit card accounts or driver's licenses.

Q: I receive e-mails from E-Bay, PayPal, and other online resources including banks. Does this mean my identity has been stolen?

A: No this does not mean your identity has been stolen. However, a common method of obtaining personal information to use in identity theft is to send emails claiming to be from one of these types of companies. It is called "phishing" and you should not respond to any of these emails.

Q. What should I do if I discover fraudulent use of my personal information?

A: You should immediately report the crime to your local law enforcement agency, contact any creditors involved and notify the credit bureaus. Detailed information is available on the Federal Trade Commission's Identity Theft web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

Q: I received a letter but have never been a patient at the UF dental college. Why did I get a letter?

A: It's possible that your dental or medical provider may have utilized our services for a consultation or a biopsy. Each year, we perform thousands of consultations of that nature. In that case, we may have had your information on file in our database although you've never been personally treated at one of our dental clinics.

Q: Was there any Human Resources (personnel), UF student/academic or UF foundation information stored on the server?

A: No. The server contained no human resources, UF student/academic or UF foundation (donor) information.