Data Breach Frequently Asked Questions

Incident Details:

On January 15, 2013, a university athletic trainer laptop was stolen from a rental van in Oakland, California. This laptop had information on student athletes, including names, birth dates, Social Security numbers, and medical history information that the trainers use for NCAA and medical reporting. We immediately reported the theft to the police. We have no evidence of fraudulent use of the data.

Frequently Asked Questions Relating to Incident

Q: I received a letter that my information was on a device (laptop) that was misplaced/stolen. What does that mean?

A: A laptop was stolen from an athletic trainer that had sensitive information on it. We don't have any evidence the data was compromised, but we wanted to let you know just in case.

Q: My colleague got a letter that said that personal information might have been compromised, what's going on?

A: The stolen laptop only had information about athletes during certain years (2001-2013), so only those people were notified about the incident. Other athletes, students, and staff were not as risk.

Q: When did this incident occur?

A: Jan. 15, 2013

Q – Why is there a delay between the incident and notifying me that this happened?

A: We had to make sure we knew what data was on the laptop, get everyone's contact information, and set up the process for notifying everyone. We had several people working throughout the days to get this out as quickly as possible.

Q – How did this happen?

A: On January 15, 2013, a university athletic trainer laptop was stolen from a rental van in Oakland, California. This laptop had information on student athletes, including names, birth dates, Social Security numbers, and medical history information that the trainers use for NCAA and medical reporting. We immediately reported the theft to the police. We have no evidence of fraudulent use of the data.

Q – Whose information was compromised?

A: Potentially, every BYUH athlete from 2001 to Winter 2013.

Q – What specific information was on the misplaced/stolen property?

A: It depends on the person, but it could involve your name, birth date, Social Security number, mobile phone number, and some medical history information the trainers would use.

Q – Who was involved in this incident?

A: The trainer was traveling with the BYUH women's basketball team. The data included BYUH athletes from 2001-2013.

Q – Did the misplaced/stolen item (laptop, computer tape, etc) contain any information about my phone number(s), my billing address, or other information about me?

A: The information could have included your mobile phone number and address from when you were a student. It also could have included information about what the trainers knew regarding your medical history, and your Social Security number.

Q – How many persons were impacted?

A: There were about 980 athletes impacted.

Q – Why was this information stored on the item (laptop, computer tape, etc)?

A: The trainers need information about athletes.

Q – Was the information password protected or encrypted?

A: The computer was password protected, but there is a slight chance someone could still get at the data, so we wanted to be proactive in reaching out to potentially affected people.

Q – Do you suspect that my information has been used fraudulently?

A: Although we have no evidence suggesting that your relevant personal information on the equipment has been misused, we take our obligation to help you protect your information very seriously, and deeply regret that this has happened.

Q – Has anyone been adversely affected as a result of their information being misplaced/stolen?

A: No.

Q – I am worried about someone stealing my identity. How will I know if that has happened?

A: We have arranged with ConsumerInfo.com, Inc., an Experian® company, to provide all persons impacted by this incident free credit monitoring. You should sign up for this membership using the activation code provided in the letter you received from BYUH.

Q - If my information was on the stolen property (laptop, computer tape, etc), does this mean that I'm a victim of identity theft?

A: No. The fact that this computer was stolen does not mean you are a victim of identity theft or that the information has been accessed to commit fraud. In most cases when computer equipment is stolen like this, the data on the hard drives are erased and the equipment is sold. We wanted to let you know about the incident in accordance with law and so that you can take appropriate steps to help protect your identity. The best way for you to help protect yourself is to periodically review your credit reports, which are available to anyone for free.

Q - Should I close my bank account?

A: There were no bank account or credit card numbers on the stolen computer.

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

A: No account number information was contained in the stolen computer.

Q - Can I get a copy of the police report for the theft?

A: We are working on getting a copy of the police report. If I can take down your contact information, we will send you a report as soon as it's available.

Q: What's being done to prevent this from occurring again?

A: We've already done several things to prevent this from happening again:

-We have worked with the Athletics Department to remove all Social Security numbers from what they gather (if Athletics needs it, they can contact the student)

-Trainers and coaches are deleting information from past seasons on their laptops

We're also implementing the following safeguards:

-Everyone who travels with sensitive information will get Computrace installed on their laptops, so we can remotely wipe data if the laptop is stolen.

-We're implementing a policy to require password protection AND data encryption on files with sensitive information.