



HIGH POINT UNIVERSITY
OFFICE OF INSTITUTIONAL ADVANCEMENT

RECEIVED
OFF OF THE ATTY GENERAL
2010 JUL 26 P 3:00

July 15, 2010

The Honorable Douglas F. Gansler
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Dear Mr. Attorney General:

Pursuant to Section 14-3504(h) of the Maryland Personal Information Protection Act, Md. Code Ann., Commercial Law § 14-3504(h), we are writing to notify you about an incident affecting information maintained by High Point University (the "University") related to approximately [634] Maryland residents.

As detailed in the enclosed letter to potentially affected individuals, in late June 2010, we discovered that the credit card number of an individual who had used his credit card to conduct transactions with the University had been used to make unauthorized charges in the name of an individual who worked at the University and had access to the credit card number. To date, we have learned that the credit card numbers of approximately [nine (9)] such individuals have been misused. The employee in whose name the unauthorized charges were made had access to University records containing some or all of the following personal information: name, Social Security number, credit card number, and parent's maiden name.

As soon as we learned of the unauthorized charges, we reported the incident to law enforcement officials and promptly terminated the employee involved. We are fully cooperating with the law enforcement investigation of this matter as we continue to investigate the incident. Further, we are examining the measures we can take to prevent incidents of this kind from happening again. We have safeguards in place to protect the security of personal information, and we are reviewing them in light of this incident to determine whether any changes should be made to our procedures and practices. Based on the results of our investigation to date we have no reason to believe that information about any Maryland resident has been misused.

The Maryland residents are being provided written notification pursuant to Md. Code Ann., Commercial Law § 14-3504(b)(2) on or about the date first written above. A sample copy of the notification letter is enclosed.

Please direct any questions and comments to me at 336-841-9202.

Sincerely,

William H. Duncan
Vice President for Financial Affairs

Enc.

July 21, 2010

<Addressee>

<Add1>

<Add2>

<City>, <State> <Zip>

Dear <Sal>,

We are writing to inform you about a recent incident that might involve unauthorized access to personal information about you. In late June 2010, we discovered that the credit card number of an individual who had used his credit card to conduct transactions with High Point University (the "University") had been used to make unauthorized charges in the name of an individual who worked at the University and had access to the credit card number. To date, we have learned that the credit card numbers of approximately **[nine (9)]** such individuals have been misused.

We take our obligation to protect the privacy of personal information of our students and alumni very seriously, and have undertaken a thorough investigation of this matter. Based on the results of the investigation to date, we have no reason to believe that the information about you was misused. Nonetheless, we have determined that the individual in whose name the unauthorized charges were made did have access to University records containing some or all of the following personal information about you: name, Social Security number, credit card number, and parent's maiden name.

We deeply regret that this incident occurred. We want to advise you of steps we have taken to safeguard personal information about you following our discovery of this incident and of the additional safeguards that we are making available to you, so that you can take action to protect yourself against potential misuse of personal information about you.

As soon as we learned of the unauthorized access, we reported the incident to law enforcement officials and promptly terminated the employee involved. We are fully cooperating with the law enforcement investigation of this matter as we continue to investigate the incident. Further, we are examining the measures we can take to prevent incidents of this kind from happening again. We have safeguards in place to protect the security of personal information, and we are reviewing them in light of this incident to determine whether any changes should be made to our procedures and practices.

Under these circumstances, it is advisable to remain vigilant against the possibility of fraud and/or identity theft by monitoring your account statements and credit reports for unusual activity. If you notice unauthorized charges on your credit card statement, contact your credit card issuer immediately about the charges in question. In the event that you ever suspect that you are a victim of identity theft, you should report the incident to local law enforcement or the Attorney General of your state, and consider other actions as described in the enclosure entitled, "Identity Theft Prevention Information and U.S. State Disclosures."

As a precaution, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call or write one of the three credit reporting agencies listed below. This will let you automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to

obtain a free copy of your credit report from each. Furthermore, you can keep the fraud alert in place by calling again after 90 days.

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 6790
Fullerton, CA 92834-6970
1-800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. You should remain vigilant by reviewing your financial accounts and monitoring your credit reports (available for free at www.annualcreditreport.com or 877-322-8228).

For more information about preventing identity theft, we suggest that you contact the Federal Trade Commission or the North Carolina Attorney General's Office, at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-438-4338
www.ftc.gov

Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

We value our students and alumni, and remain committed to ensuring the safety and security of personal information. If you have any concerns or questions about this matter or if you believe that personal information about you has been misused, please contact Bill Duncan at bduncan@highpoint.edu and/or (336) 841-9202.

Sincerely,



William H. Duncan
Vice President for Financial Affairs
High Point University
833 Montlieu Avenue
High Point, NC 27262

Enc.

IDENTITY THEFT PREVENTION INFORMATION AND U.S. STATE DISCLOSURES:

For residents of Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia and West Virginia: State law requires disclosure that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report at www.annualcreditreport.com, by calling 877-322-8228, or by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111

Experian
P.O. Box 2104
Allen, TX 75013-0949
1-888-397-3742

TransUnion
P.O. Box 1000
Chester, PA 19022
1-800-916-8800

For residents of Iowa: State law advises that if you suspect identity theft, you should report it to law enforcement or to the Iowa Office of the Attorney General.

For residents of Maryland: You may obtain information from the Maryland Office of the Attorney General about steps you can take to prevent identity theft:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For residents of Oregon: State law advises that if you suspect identity theft, you should report it to law enforcement and the Federal Trade Commission.

For residents of Massachusetts and West Virginia: It is required by your state laws that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit. To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail, at the address(es) listed below. Please note that if you wish to place a security freeze on your credit report with multiple consumer reporting agencies, you must directly contact each consumer reporting agency.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, without middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and proof of your current address, such as a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted to the consumer reporting agency a valid police report, investigative report, or complaint to a law enforcement agency relating to the identity theft incident.

The consumer reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The consumer reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The consumer reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three consumer reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The consumer reporting agencies have three (3) business days after receiving your request to remove the security freeze.