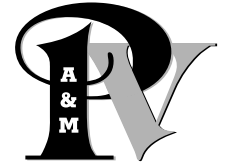




Prairie View A&M University
P.O. Box 519
Prairie View, Texas 77446-0519



MEMORANDUM

April 6, 2004

To: PVAMU Employees, Former Employees, Students and Former Students

From: Dan Williams
Executive Vice President and Chief Financial Officer

Subject: **Possible Exposure of Personal Information**

On Tuesday, March 22, 2004 it was reported to the University that an individual researching on Yahoo.com had gained access to a Prairie View A&M University report containing her name and related personal information, including social security number. This was immediately reported to the Office of Institutional Research where it was determined that most of the information was contained in a standard report that is routinely produced and sent to a state agency in Austin. Subsequently, it has been learned that other reports may have also been involved. Further investigation revealed that in March 2003 a backup folder containing some official reports had inadvertently been placed on a "web server". Steps were taken to immediately remove the folder from the server and place it on a secure storage device where an unauthorized person could not access it.

However, it appears at this time that if you have been a student or an employee of the University between January 1999 and December 2003, your name and Social Security number (SSN) might have been exposed. If your affiliation with Prairie View A&M University was prior to 1999 or after December 2003, it is less likely that your information was exposed. Nevertheless, it may be advisable for you to contact one of the Major Credit Bureaus shown on the reverse side of this memorandum as a precaution. This is an action that any person owning a credit card should do at least annually; perhaps more often for credit cards that are heavily used.

Please understand that the University has no way of determining whether any of the information contained in these official reports has ever been copied or misused by any individual or by any entity that might have any malicious or illegal intent in accessing and/or copying the information contained in the reports. At this time, we have no reason to believe that information contained in the folder was misused by anyone, but there is no way for that to be confirmed. While we are not aware of any misuse, the University cannot minimize the concern raised by an incident of this type, and we regret that it has happened. Accordingly, we are attempting to contact all individuals where there may be any potential or possibility of risk. The following information is provided to assist individuals monitoring their credit records and protecting their identity.

What is being done to protect Social Security number privacy at the University?

Prairie View A&M University is very aware of the importance of Social Security number (SSN) privacy. Many steps have already been taken to eliminate the use of SSN as the primary identifier on campus. Students have had access to services without providing their SSNs and the SSN was removed from the front of new student, staff and faculty ID cards. However, we are still required to use SSN in some of our reports and interactions with state and federal agencies. PVAMU has been identifying and removing vulnerabilities by limiting service offerings and expanding the level of control on some functional areas. Security training and awareness seminars at all levels are also planned.

Credit and Identity Protection Resources

Data theft occurs when someone obtains key pieces of someone's personal identifying information. Identity theft occurs when that information is used for any fraudulent or other unlawful purpose. The unlawful acquisition of personal identifying information does not necessarily mean that identity theft has occurred. This distinction is important when considering any response you might wish to make to the disclosure of your Social Security number.

Responding to Data Theft

One proactive measure to consider is placing a "fraud alert" on your file with the three major credit bureaus (see table on reverse side of this memorandum). This free service requests that any creditor contact you by phone at a designated number before opening a new account. The time an alert stays on your record varies for each credit bureau; however, you can request that the fraud alert be reinstated after the initial period has ended. In addition, you should qualify for a free copy of your credit report. Review your credit reports carefully to ensure no fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts.

You may also wish to order additional copies of your credit reports in the future to monitor your credit profile. If you've been declined credit, employment or housing in the last 60 days, you can receive these reports for free. If not, you will be charged \$9.95 plus any applicable taxes for a basic credit report.

Major Credit Bureaus			
	Place a Fraud Alert	Order a Credit Report	Address
Equifax www.equifax.com	1-800-525-6285	1-800-685-1111	P.O. Box 740241 Atlanta, GA 30374-0241
Experian www.experian.com	1-888-397-3742	1-888-397-3742	P.O. Box 2002 Allen, TX 75013-2002
Trans Union www.transunion.com	1-800-680-7289	1-800-916-8800	P.O. Box 6790 Fullerton, CA 92834

Responding to Identity Theft

If your personal identifying information is being used by someone else for fraudulent or criminal purposes, such as applying for a credit card or obtaining loans in your name, making unauthorized purchases, or gaining access to your bank accounts or other private information, you can follow the steps below:

- If you find any fraudulent accounts or unauthorized access on your record, contact the security departments of the creditors or financial institutions that granted the credit and close these accounts.
- If you discover misuse of your Social Security number, contact the **Social Security Fraud Hotline** at 1-800-269-0271.
- If your personal information is being used for fraudulent or criminal purposes, file a report with the police. Keep a copy of the police report in case you need proof of the crime to show the bank, credit card company, or others.
- If you are a victim of identity theft, you can also file a complaint with the **Federal Trade Commission (FTC)** by Internet: www.consumer.gov/idtheft/ (click File a Complaint from the menu at the left); Telephone: 1-877-438-4338; or TDD: 202-326-2502, including dates.

How to Contact Prairie View A&M University

E-mail—To make inquiries by e-mail please e-mail to: idinfor@pvamu.edu (Social Security Numbers should not be sent in any e-mail message.)

Telephone: (936) 857-2448 or 2449 / Institutional Research at PVAMU

(If answered by voice mail, leave your name and telephone number ONLY and your call will be returned as soon as possible).

Additional Information

These Internet sites provide information on steps you can take to protect your credit and identity.

Attorney General of Texas

www.oag.state.tx.us/consumer/idtheft.shtml

This official Attorney General of Texas site is a good starting point for learning about personal data and identity theft. It also provides tips on how to protect yourself against different types of credit fraud.

Social Security Administration

www.ssa.gov/pubs/idtheft.htm

The Social Security Administration is the government agency responsible for issuing and managing Social Security numbers. The agency's official site walks you through who to contact, when, and why. It also links to two useful fact sheets:

Fact Sheet: When Someone Misuses Your Number (05-10064)

www.ssa.gov/pubs/10064.html

Fact Sheet: Social Security-Your Number and Card (05-10002)

www.ssa.gov/pubs/10002.html

Department of Justice

www.usdoj.gov/criminal/fraud/idtheft.html

The Department of Justice site describes what can happen if you are a victim of data theft or identity fraud. It provides logical steps for action, tips for reducing your risk of fraud, and phone numbers, addresses, and links to credit bureaus and other governmental agencies you may need to contact.

Federal Trade Commission

www.ftc.gov/bcp/online/pubs/credit/idtheft.htm

This site provides a document titled ID Theft: When Bad Things Happen To Your Good Name that includes information on steps to follow if you are a victim of identity theft.

Steps to Follow If You Are A Victim

[/www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#victim](http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#victim)

ID Theft Information

www.consumer.gov/idtheft/

This is the U.S. government's central web site for information about identity theft, maintained by the Federal Trade Commission, offering government reports, consumer updates, and links to other sites.