

July 15, 2008

Dear Registered Student,

On July 1, 2008, the University of Maryland's Department of Transportation Services sent all registered students, by U.S. mail, a brochure with on-campus parking information. On July 8, 2008, the University discovered that the labels on that mailing included the addressees' Social Security numbers. The numbers were not identified as Social Security numbers, and did not show the normal spacing between digits. This mailer was sent using third class, bulk mail delivery and may not have been delivered to you yet. The University apologizes, and deeply regrets this unfortunate mistake. We are taking aggressive steps to ensure that this does not happen again. We strongly recommend that you take appropriate precautions to mask, black out, or destroy this document after use.

Although there is no current information that anyone's Social Security number has been misused, the University suggests that you take the following precautionary steps:

- Immediately place a free 90-day fraud alert on your consumer credit file. A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report. It also requests that creditors contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. If you opt to contract for the Equifax service, you can place a fraud alert through Equifax, as explained below; or you can do it by contacting the U.S. Federal Trade Commission ("FTC"). To place a fraud alert through the FTC: Go to the FTC's Web site, www.ftc.gov/idtheft/ or call 1-877-ID-THEFT (438-4338).
- You may also place a security freeze on your credit file. A security freeze prevents potential credit issuers from accessing your credit file without your consent, and makes it unlikely that credit will be issued in your name. Information about how to place a security freeze can be found at the FTC's Web site at www.ftc.gov/idtheft/ (look under Consumers on the menu, and select "DETER: MINIMIZE YOUR RISK") or by calling the FTC at 1-877-ID-THEFT (438-4338).

The University is also offering a 12-month Equifax credit monitoring service, at no charge to you, to ensure that you have support necessary to monitor the security of your personal data. This program allows you to contract directly with Equifax for access to your credit report, credit monitoring, customer care, and fraud expense reimbursement insurance. To do this, you must select your choice of Equifax service, and enroll with Equifax by September 10, 2008. You can choose either Equifax Credit Watch Gold, an online service, or Equifax Credit Watch by Mail, a service done through the U.S. Mail. Program services and enrollment information are described at www.transportation.umd.edu/parkingmailer.

For additional information about this incident and Equifax services, please visit the University's Web site at www.transportation.umd.edu/parkingmailer. You may e-mail questions to the University at parkingmailer@umd.edu. If you don't have Internet access, or you wish to speak with someone at the University, call toll-free, 1-877-935-2428, Monday-Friday, 8:30 a.m. - 5:00 p.m., EST.

It is possible that dishonest people, claiming to offer University assistance, may contact you and ask for personal information. Be assured that the University of Maryland will not contact you by phone, e-mail or any other way to ask you for personal information. Please do not release any personal information in response to contacts claiming to be from the University.

We value the importance of your personal information. We encourage you to use this free Equifax service, and to review your account statements for suspicious activity. Again, we apologize, and regret any inconvenience or concern this incident may cause you.

Sincerely yours,

J. David Allen
Director
Department of Transportation Services