



February 8, 2008

Dear Sir or Madam:

We are writing to inform you that you are among a group of individuals whose personally identifiable information such as name and social security number (SSN) may have been exposed due to a recent computer theft on campus. We regret this incident and wanted to alert you after completing our investigation of the nature and scope of the data at issue. Please find below details about this incident and how to sign up for free credit monitoring services.

An external computer hard drive was reported stolen on January 3, 2008 from a locked office within the Office of Student Affairs in the Leavey Center on the Main Campus. Georgetown's Department of Public Safety responded to scene and continues to cooperate with an ongoing investigation by the District of Columbia Metropolitan Police Department. In addition, we are working with the U.S. Secret Service about this incident so that they may follow up as they determine appropriate.

A thorough internal investigation of the data that was contained on the hard drive has determined that the hard drive included personally identifiable information for students enrolled and some faculty and staff from 1998 through 2006. Since the files related to a range of cross-campus student financial transactions processed through the Office of Student Affairs, it pertained to students enrolled at the Main, Medical and Law Center campuses. No financial information, such as bank account or credit card numbers, was contained in the hard drive, nor did the hard drive contain any personal health records. This incident is limited to this one hard drive and does not extend to other University systems and services where personal data may be stored or updated.

As a precaution, we are notifying you of this situation and encouraging you to take several steps to protect yourself.

Initially, we encourage you to place a fraud alert on your credit report. This is a free service that will request creditors to verify your identity before opening a new account. To place an Initial 90-day Fraud Alert, you can contact any one of the three major credit bureaus, which are Experian®, TransUnion® and Equifax®. The agency that you contact will share your request with the other two credit bureaus, which will add the alert to your file or request that you provide them with additional information. When the alert is added to your file, you will receive a confirmation. Then, about 10-20 days later, you should receive in the mail a free credit report from each of the three credit bureaus. Once you receive your report, review it for any potential inaccuracies. Report any inaccuracies to the credit bureau that sent you

the report. If you find suspicious activity on your credit report, please call your local police or sheriff's office and file a police activity report of identity theft. You may also 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, you may wish to check your credit report every three months for the next year.

Please be aware that when you call a credit reporting agency, they will ask you to provide your SSN to proceed with the process. In other circumstances, and unless you have initiated the call, you should not provide your SSN to anyone over the telephone.

In addition to the fraud alert, we have also engaged with ConsumerInfo.com, Inc., an Experian company, to provide you with one year of credit monitoring, at no cost to you. This credit monitoring product known as **Triple Alert**SM will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity.

Your complimentary 12-month membership includes:

- Monitoring all three credit files with Experian, Equifax[®] and TransUnion[®] – everyday
- Email alerts of key changes indicating possible fraudulent activity – within 24 hours
- Monthly “No Hit” alerts, if applicable
- Dedicated team of fraud resolution representatives for victims of identity theft
- \$25,000 identity theft insurance provided by Virginia Surety Company, Inc. with no deductible*

*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

You have ninety (90) days to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership quickly. Please visit <http://partner.consumerinfo.com/gu> and enter the activation code provided below. You will be instructed on how to initiate your online membership.

Your Credit Monitoring

Additional suggestions for protecting identity can be found at our Office of Information Security website at security.georgetown.edu as well as at online resources from the Privacy Rights Clearinghouse at www.privacyrights.org/identity.htm and the federal government's identity theft website at www.ftc.gov/bcp/edu/microsites/idtheft/.

Although in this particular instance the data breach was the result of a computer theft and not any kind of system intrusion, it is an unfortunate example of the increasing importance of data security to all of us. Georgetown recognizes the potential vulnerability of this kind of information and consistently has taken steps to protect data across University systems. These steps include assigning a GoCard number and NetID as a unique identifier instead of social security numbers. We are also taking other steps to implement enhanced security procedures across campuses, and continue to identify and incorporate emerging best practices in data protection and security.

Please accept our sincere apologies for this incident. Nothing is more important to us than our relationships with our students, faculty, staff and alumni. If you have any additional questions, please do not hesitate to call Georgetown's University Information hotline at 866-740-2458 or visit identity.georgetown.edu.

Sincerely,



Todd Olson
Vice President of Student Affairs
Dean of Students



H. David Lambert
Vice President for Information Services
and Chief Information Officer