Georgia College & State University

Personal Identity Information Data Breach Procedure
September, 2012

In an effort to protect individuals from the growing threat of identity theft caused by data breaches, if personal identity information (PII) is breached Georgia College (GC) adheres to the notification requirements defined in the Georgia Personal Identity Protection Act (GPIPA) passed in 2005.

PII is defined by GPIPA as:

'Personal information' means an individual´s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
(A) Social security number; (B) Driver´s license number or state identification card number;
(C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
(D) Account passwords or personal identification numbers or other access codes; or
(E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual´s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

The term 'personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

Breach is defined by GPIPA as:

Breach of the security of the system' means unauthorized acquisition of an individual´s electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by a data collector (the university). Good faith acquisition or use of personal information by an employee or agent of the university for the purpose of the university is not a breach of security provided that the personal information is not used or subject to further unauthorized disclosure.

GC, upon determining that PII has been breached, adheres to GPIPA reporting requirements:

GC may utilize three primary notice methods and/or three substitute notice methods under GPIPA. The primary notice methods are written notice, telephone notice, or electronic notice. However, electronic notice only may be given if the consumer consented in advance, as outlined in 15 U.S.C.A. § 7001, to receive electronic notices in lieu of paper.

Substitute notice methods may be used by GC if: (i) the cost of giving notice through one of the primary methods exceeds $50,000; (ii) there are more than 100,000 individuals affected; or (iii) sufficient contact information is not available to provide primary notice. E-mail, conspicuous notice on the entity's webpage, and/or notification of state-wide media, consistent with GPIPA's notice timing requirements, are acceptable substitute notice methods.

Following FTC regulations, the notice from GC will be easy to understand and will include:

- a brief description of what happened, including the date of the breach (if known) and the date you discovered the breach;
- the kind of information involved in the breach (ie. Social Security numbers, financial account data, dates of birth, medication information, etc.)
- suggested steps they can take to protect themselves. GC's advice will be relevant to the kind of information that was compromised. In some cases, for example, GC will refer people to the FTC's identity theft website, www.ftc.gov/idtheft. In addition:
    - if the breach involves health insurance information, GC will suggest that people contact their healthcare providers if bills don't arrive on time in case an identity thief has changed the billing address, pay attention to the Explanation of Benefit forms from their insurance company to check for irregularities, and contact their insurance company to notify them of possible medical identity theft or to ask for a new account number.
    - if the breach includes Social Security numbers, GC will suggest that people get a free copy of their credit report from www.annualcreditreport.com, monitor it for signs of identity theft, and place a fraud alert on their credit report. If they spot suspicious activity, they should contact their local police and, if appropriate, get a credit freeze.
    - if the breach includes financial information – for example, a credit card or bank account number – GC will suggest that people monitor their accounts for suspicious activity and contact their financial institution about closing any accounts that may have been compromised.
- a brief description of the steps GC is taking to investigate the breach, protect against future breaches, and mitigate the harm from the breach; and
- how people can contact GC for more information. The notice must include a toll-free telephone number, email address, website, or mailing address.

GC may elect to go beyond any legal requirement of notice and include in the notice an offer to enroll the individual in a 1 year account monitoring service if the individual expresses a desire to receive this service.