University of Houston System
Identity Theft Prevention Program
Executive Summary
FY 2011

The system-wide compliance officer is required annually to prepare an executive summary of all activities of the Identity Theft Prevention Programs of the component institutions (Audit and Compliance Committee Planner, Item 5.06). Listed below are the reports from each component.

University of Houston and UH System Administration

Since May 2009, all UH System employees and students receive automated email messages whenever there is a change in the University database to their bank account information, email address, home address, or W-4 withholding. The email instructs the employee or student to contact University Information Technology (UIT) Security if they did not initiate this change. UIT Security has received several inquiries as a result of this email notification, in many cases because the email notification was unexpected. Each inquiry was investigated to verify the change was authorized and legitimate.

In March 2010, UIT Security made Identity Finder software available to all UHS faculty, staff and students. This software locates sensitive and personally identifying information on computers. Through campus-wide initiatives, UIT Security is partnering with business owners to remove or protect sensitive data where it is located.

In August 2010, the University of Houston entered into a multi-year contract with Xerox for copier service following a competitive evaluation process. One of the evaluation criteria was the ability of the vendor to safeguard and erase images stored on the copier's hard drive, since these images might contain confidential information. Xerox agreed to configure all of its copiers to immediately erase images on the hard drive after each job. In addition, UIT Security worked with UH departments to ensure that hard drives in copiers from other vendors would be erased or destroyed before leaving the department.

As of August 31, 2011, all 94 UH System credit card merchants (i.e., UHS departments that accept credit cards) were in compliance with payment card industry (PCI) standards. The major thrust of PCI standards is the protection of personal identifying information and prevention of fraud for merchants that accept credit cards. UH System merchant employees are required to complete annual training to refresh their knowledge of PCI standards so that credit card information is protected.

During October and November 2011, all UH departments with "covered accounts," as defined by the Federal Trade Commission's Red Flag Rules, will complete their third annual web training to provide appropriate department personnel with an overview of the requirements for securing personal identifying information. Each of these departments developed identity theft prevention procedures tailored to their operation.

University of Houston – Clear Lake

Each department that was identified as having access to sensitive, confidential and financial information (Red Flag) has written procedures to safeguard that information. These procedures help departments to safeguard the information available to them and help detect possible violations. UH System has put in place notifications to all employees when any changes are made to the employees confidential information. At the start of each new fiscal year each department is asked to review and modify their procedures as necessary and inform all employees of the procedures. This notification is documented and sent to the Associate Vice President for Finance.

During FY 2011 there were no reported cases of identity theft or violation of university procedures.

University of Houston-Downtown

Since May 2009, all UHD employees and students receive automated email messages whenever there is a change in the University database to their bank account information, email address, home address, or W-4 withholding. The email instructs the employee or student to contact University of Houston-Downtown Information Technology (UHD IT) Security if they did not initiate this change. UHD IT Security has not received any inquiries as a result of this email notification during the past year.

On March 16, 2011, UHD reconfirmed that it is in compliance with payment card industry (PCI) standards. UHD had migrated to one of the PCI-compliant processes offered by Bank of America, the bank UH System uses for its operations. The major thrust of PCI standards is the protection of personal identifying information and prevention of fraud for merchants that accept credit cards.

Beginning in Summer 2011, UHD implemented a new security tool, Identity Finder, to limit the potential for identity theft and unintended exposure of private information. The tool enables faculty and staff to search for and remove sensitive information from their computers, laptops, and other hard drive locations. To date, the product has been installed on more than 95% of the university's faculty and staff desktop PCs, and instructions for its use have been provided via university e-mail. Based on feedback received by many faculty and staff, it has already been a highly successful deployment.

In October/November 2010, UHD employees in positions in departments that manage "covered accounts" that could be subject to identity theft completed the UH-System Red Flag Rules mandatory training. Employees in those positions at the end of FY 2011 are scheduled to participate in the Red Flag Rules mandatory training again in FY2012. The purpose of this training is to provide appropriate department personnel with an overview of the requirements for securing personal identifying information.

UHD Reported Incidents since Program Inception

Since the Identity Theft Program was formally implemented, there have been no known reports of identity theft or any compromises of financial/privileged information involving students or employees at UHD.

University of Houston-Victoria

In FY11 there were no known reports of confirmed identity theft fraud or the unauthorized compromise of financial or other privileged information involving students or employees.

The original departmental areas participating in the UHV Identity Theft Program included the Bursar's Office, Admissions and Records, the Financial Aid department, Human Resources, Student Solutions and Information Technology. In FY11, the Academic Schools Online Support Technicians also began participating in the campus identity theft program due to their responsibility for resetting certain passwords. The UHV program includes departments who oversee covered accounts as well as departments involved in operations where there is a reasonable likelihood that identity theft could occur.

General program oversight of the campus program, including implementing and updating the campus identity theft program, as described in UHV Policy A-27, continues to be the responsibility of a Program Administrative Group comprised of the Campus Compliance Officer (Program Administrator), Bursar, Information Security Officer and the HR Director.

UHV FY10 Awareness and Prevention Activities –

- Sixty Six (66) employees from key departments and operational areas completed the role based Red Flag Identity Theft training module. *(Admissions, Financial Aid, Student Solutions, Information Security, Human Resources, Bursar's Office)*
- Student Listserv E-mail notices were sent by Admissions and Records at the start of the fall and spring semesters informing students of the campus Identity Theft Program;
- Employees and students received automatic email notifications through the HRMS database when changes were made to their email or mailing addresses confirming the change. University employees also received notifications when changes are made to W-4 and insurance information or Direct Deposit information changes were made to their personal accounts.
- The departments of Admissions, Financial Aid, Student Solutions, Human Resources, the Bursar's Office, and Online Academic Technicians have department protocols in place to help verify identity and prevent the unauthorized release of financial or other confidential personal information. These areas have been instructed to review their written protocols annually.

UHV Confirmed Incidents of Identity Theft during FY10

Admissions and Records	- None
Bursar's Office	- None
IT Security and Service Desk	- None
Human Resources	- None
Financial Aid Department	- None