University of Pittsburgh

Pittsburgh, Pennsylvania 15260

TO: Deans, Directors, and Department Chairs

FROM: Arthur G. Ramicone, Chief Financial Officer and Senior Vice Chancellor AGR
David N. DeJong, University Privacy Officer and Customer Security Officer DND

DATE: August 3, 2015

SUBJECT: Payment Card Industry Data Security Standards Compliance and Europay, MasterCard, Visa Compliant Equipment

---

Card Data Breaches

Credit card data breaches at retailers, including such notable names as Target, Neiman Marcus, eBay and Home Depot, highlight the critical importance of information security systems. The Ponemon Institute's 2014 Cost of Data Breach Study, sponsored by IBM indicates that in the U.S. the average cost of a breach to a company was $5.85 million, 8% higher than the previous year, the most expensive in the world, not including the intangible costs related to reputational risk.

These same risks apply to higher education institutions that accept credit and other types of cards (e.g., debit cards) for payment. Since 2005, breaches have occurred at such prominent names in higher education as UCLA, Ohio State, the University of Nebraska, the University of North Carolina, the University of Florida, and the University of Maryland, resulting in the compromise of sensitive data for over 3 million card accounts from those six schools alone. The costs for the University of Maryland breach may reach seven figures for the 300,000 plus records involved, according to several data-security professionals interviewed by The Chronicle of Higher Education.

Payment Card Standards

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of international security requirements for protecting cardholder data. The major credit card associations (VISA, MasterCard, American Express and Discover) require entities that store, process or transmit cardholder data to be PCI DSS compliant. PCI DSS compliance applies to all payment channels, including in-person, mail, telephone, and e-commerce. Compliance with these standards is required by the University. If the University does not comply with the security requirements or fails to rectify a security issue, it may be fined. In the event of a data compromise, fines may be waived if there is no evidence of non-compliance with PCI DSS.

Recently, in order to provide additional security in point-of-sale (POS) environments in the U.S., the credit card associations have announced implementation of Europay, MasterCard, Visa (EMV) compliant equipment (known as "chip and PIN"). ***Effective October 2015, the payment card associations will shift financial liability for fraud losses to the party that processes the transaction without chip technology.***

University Compliance

To demonstrate the University's ongoing commitment to compliance with PCI DSS and other related payment card standards and to highlight existing policies and guidance relevant to this topic, the following policy and guidance documents are being issued and are effective immediately:

- Payment Card Handling and Acceptance Policy 05-11-02
- E-Business Resource Group Guidelines
- University of Pittsburgh Payment Card Industry Technology Guidelines

E-Business Resource Group

The E-Business Resource Group (EBRG) serves as a resource to the University community that provides guidance on PCI DSS related matters. For additional information, see the EBRG website at ebusiness.pitt.edu.

Equipment Transition and PCI Training

Each University department or group which processes payment card transactions should designate one primary contact, along with an alternate, who will be responsible for coordinating PCI DSS compliance for their area. The Office of Finance will also coordinate a rollout for EMV-compliant equipment items. The names of such contacts should be submitted to the Office of Finance, to the attention of Emily Gavin, egavin@cfo.pitt.edu, on or before August 17, 2015.

All University Employees handling payment cards or related data are required to complete PCI Data Security training as part of the University's overall Information Security Awareness Training program. Computing Services and Systems Development provides this training, and it is accessible from technology.pitt.edu. Departments that currently offer an approved alternative to the University training may contact CSSD to determine what additional training may be required.

cc: Jinx P. Walton, Chief Information Officer
Alan A. Garfinkel, Interim General Counsel