Thank you for reading the first edition of the *PCI Compliance Newsflash* quarterly newsletter.

The University of Utah currently has more than 235 departments accepting credit and debit cards throughout the School of Medicine, University Hospital, and Lower Campus. We process thousands and thousands of transactions each year. That makes the University stewards of a lot of credit card numbers! It is up to us, as merchants, to protect the personal data that our customers and donors trust us with. Visa, MasterCard, Discover, American Express, and JCB have created the Payment Card Industry Data Security Standard to protect their cardholders and merchants from fraud.

The PCI DSS is a dynamic standard that adapts to changes in fraud trends in our card carrying world. In an effort to keep you apprised of changes, and to continue expanding your knowledge of how the PCI DSS affects you, this newsletter will be sent to all Department Contacts and their Cognizant Authorities on a quarterly basis. Each edition will include information such as: tips on processing transactions, how to maintain physical and electronic security of cardholder data, interesting facts about the payment card industry, and any changes in the PCI DSS and University’s guidelines and procedures. The newsletter may also provide information on your compliance requirements and the resources that are available to achieve compliancy.

As always, the Income Accounting and Student Loan Services Department will help you renew your compliancy each year, answer any questions you may have, and help you find processing solutions that will work best for your department. Feel free to pass on the information from this newsletter to other departments who are looking into accepting payment cards.

If you would like to request a PCI topic for a future newsletter, please email pci@utah.edu or call Kim Stringham at 585-5686.
Data Breach Investigations Report was released by the Verizon Business RISK team in cooperation with the United States Secret Service. The statistics from breach investigations during 2009 are very telling as to how data breaches can occur.

### WHAT COMMONALITIES EXIST?
98% of all data breached came from servers
85% of attacks were not considered highly difficult
61% were discovered by a third party
86% of victims had evidence of the breach in their log files
96% of breaches were avoidable through simple or intermediate controls
79% of victims subject to PCI DSS had not achieved compliance

### WHO IS BEHIND DATA BREACHES?
70% resulted from external agents
48% were caused by insiders
11% implicated business partners
27% involved multiple parties

### HOW DO BREACHES OCCUR?
48% involved privilege misuse (up 26% from 2008)
40% resulted from hacking (down 24% from 2008)
38% utilized malware
28% employed social tactics
15% comprised physical attacks

### Processing Tip
When accepting a payment card in a “face to face” transaction, hold the card until the customer has signed the receipt. Compare the signature to the signature on the card. If they match, hand the card and the customer’s receipt back to him. If the signatures don’t match...ask for additional ID. If you suspect fraud, call the merchant helpdesk and tell them you have a CODE 10!

This one step can guard against fraud and save you money!

### Reminder!
An email will be sent to your Department Contact when it’s time to renew your PCI DSS Compliance. It happens every year. You will have 30 days to complete your Annual Agreement, Training, and Questionnaire.

Check out the Payment Card Acceptance and E-Commerce Website. Tons of merchant information at your fingertips!

For questions regarding this newsletter, contact Kim Stringham at 585-5686, email kim.stringham@utah.edu