RESOURCE

Guidance on Using Credit Cards and Financial Account Information

Credit card numbers and financial account numbers are protected by state law. In addition, as a condition of accepting credit card payments the University must meet the Payment Card Industry's strict Data Security Standards (PCI DSS). The University's **Data Protection Standards** explain what departments that collect, access, share, send, use or store this Restricted Use data like credit card and financial account numbers must do to ensure that it is safe and secure. The University's **PCI Policy** explains what departments that accept credit card payments are required to do.

EVERYONE

- **DON'T** accept credit card payments unless your department has been approved. Learn more through the Credit Card Acceptance Website and you follow the **Payment Card Industry (PCI) Policy**.
- **DON'T** request, access, use or store credit card or financial account numbers unless there is a legitimate business need to do so and your department has confirmed that it complies with the policies described above.

- **DO** read the **Data Protection Standards** and be sure you understand how to secure sensitive information.
- **DO** help minimize risk. Be on the lookout for University forms (paper or electronic), emails, or old files (electronic or paper) that contain financial account numbers. If it

doesn't seem necessary, say something. Ask your supervisor, **Information Security or Compliance Services for help** determining whether it is appropriate for financial account numbers to be in those places and, if not, how to safely and security destroy the information.

- **DO** report any suspected data breach to **Information Security** immediately.

DEPARTMENTS THAT ACCESS, USE OR STORE FINANCIAL ACCOUNT NUMBERS

- **DON'T** store financial account numbers on unencrypted laptops, USB drives or portable devices like Dropbox or Google Drive that have not been approved by Information Security.
- **DON'T** email or otherwise transmit financial account numbers electronically. If it's absolutely necessary, contact Information Security to identify a secure way to do so. The University's **encrypted email system** may be used to send sensitive information to individuals and organizations outside of the University.

- **DO** make sure to follow the **Data Protection Standards** and the **Payment Card Industry Policy**.
- **DO** contact **Information Security** or **Financial Affairs** if you need help determining whether your collection or use of financial account numbers is appropriate.
- **DO** make sure that financial account numbers are stored in locked file cabinets or encrypted electronic storage.
- **DO** take special care to destroy financial account numbers responsibly. Information Security provides **simple explanations** for destroying paper records, CDs, DVDs, files, storage devices, and the like.
- **DO** contact Procure to Pay (P2P) if you plan to buy or use software that will use or store financial account numbers to ensure that the contract has appropriate protections in place.
- **DO** report any suspected data breach to **Information Security** immediately.

Consequences

- A data breach involving financial account numbers may lead to identity theft or stolen funds. You don’t want either of those to happen to you; you should do what you can to minimize the risk that it happens to others.
- If there is a data breach that involves financial account numbers the University may be required to notify every individual whose information has been breached and may provide credit monitoring. In addition, the University may be required to notify state attorneys general and credit card companies about the breach. The department in which the breach occurs will participate in these efforts.
- Regulators may impose fines or penalties and individuals who are harmed may file lawsuits.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related BU Policies and Procedures

- **Data Protection Standards**
- **Payment Card Industry (PCI) Policy**.
- **Payment Card Industry Data Security Standards**