Most of us carry credit or debit cards that we use each and every day. We often hand them to complete strangers with the faith that they will conduct the transaction that we have requested and return our cards to us safely. In 2010, there were reported losses of $48 billion dollars that affected 11 million Americans.

Source: http://www.creditcards.com/

If you have questions about credit cards, you are interested in applying to take credit cards for a University-related activity, or you just want to know more, contact UVA Payment Card Services or visit our website at www.virginia.edu/finance/ecommerce.
Quick U.Va. Credit Card Facts

Any University-related payment card activities must be authorized through the UVA Payment Card Services before any payment card activities are initiated. Contracts must not be negotiated with credit card processing companies or companies accepting any funds by credit card on behalf of a unit or a person without pre-approval. All merchant accounts for accepting credit cards payments must be similarly approved by the UVA Payment Card Services.

Once approved, credit cards may be accepted for goods, services, course registration, fees, gifts to the university and any other charges included on a student bill are conducted through the University’s online “QuikPay at UVA” system.

The University most commonly allows authorized merchants to operate card swipe terminal and/or web-based payment card activities. The department is responsible for all expenses associated with credit card merchant accounts and cannot adjust the price of goods or services based upon the method of payment.

Retaining sensitive cardholder data (e.g.: the credit card number, etc.) for unavoidable operating purposes must be approved by the UVA Payment Card Services. Any such physical or electronic data must be secured and encrypted as required by the University Payment Card Guidelines, University policy University Policy IRM-015 “Electronic Storage of Highly Sensitive Data”, and in accordance with PCI Data Security Standards.

Departments must assure that all computers handling credit card data possess the most recent updated versions of University recommended antivirus and spyware detection software. Departments must also run University recommended sensitive data detection software at least once a month to insure that credit card data is not stored on the computer.

PCI DSS and the University

PCI DSS is an abbreviation for the Payment Card Industry Data Security Standards. In 2005, all major credit card companies (Visa, AMEX, MC, Discover card, and JCB) developed common standards to protect cardholder data. Compliance with these standards are required for anyone handling, storing, or transmitting payment card data. The penalties for violations are financially significant and may result in the inability to conduct future payment card activities.

The University and all departments or persons that handle payment card data related to the University of Virginia have a contractual obligation to adhere to the PCI Data Security Standard (PCI DSS). We adhere to these standards to protect our customer/client data and to limit our liability so that we may continue to process payment cards transactions. Each University ‘merchant’ is responsible for adhering to all of the PCI DSS standards and for annually certifying their continued compliance by submitting the PCI DSS Self Assessment Questionnaire (SAQ) appropriate to their credit card activities.

These questionnaires vary in length from approximately 21 to over 200 questions depending upon the type of credit card activity that the ‘merchant’ chooses to engage in.

The PCI SAQ requirements and questions span the following categories:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS also requires us to insure that any software providers or payment card partners (those associated with the University that are handling credit cards on our behalf or that we are recommending our clients to) are also PCI compliant in order for us to continue to utilize their services.

U.Va.’s GOLDEN Rules

1. Thinking of taking credit cards or changing your current process? Contact UVA Payment Card Services first!
2. Do NOT request or send any credit card information by email. If someone emails their data to you, remove the data before replying to make them aware that, for their own safety, they should not do this again. Do not process any payments received by email!
3. NEVER record data in any electronic format (Excel files, databases, etc.) unless authorized by the University Comptroller and in compliance with University Policy IRM-015 ‘Electronic Storage of Highly Sensitive Data’.
4. Do NOT request, record, or store any of the magnetic stripe data or the credit card confirmation code (three digit on the back of many cards and 4-digits on the front of American Express, often referred to as the “CVV2” code).
5. Do NOT enter payment card data into devices or computers other than an authorized non-computer based point-of-sale “swipe” terminal.

For a complete list of the UVA Credit Card Requirements, visit our website at: http://www.virginia.edu/finance/ecommerce/docs.html

Has data been compromised or lost?
The first 24 hours are critical!!

Immediately Contact:
- Your department/unit’s ITS Local Support Partner (LSP) & UVA Payment Card Services.
- Notify the UVA Police at: http://www.virginia.edu/uvapolice/contact.htm.
  Always submit the Security Incident Report as soon as possible. (http://its.virginia.edu/security/reporting.html).