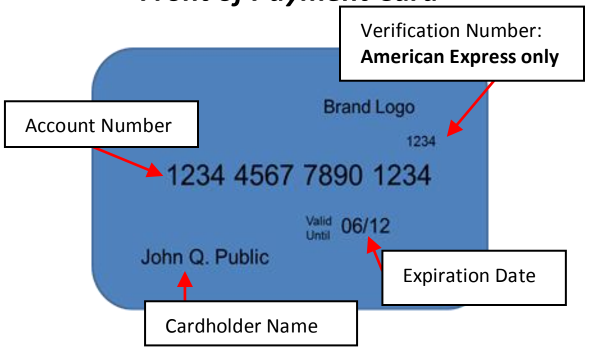
Payment Card Features

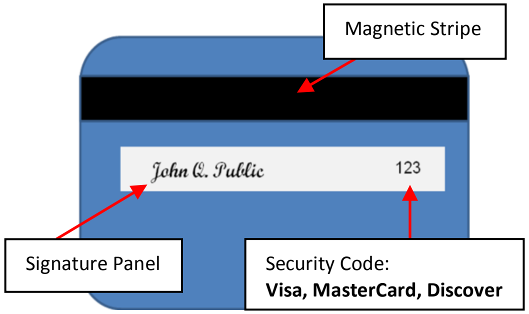
All payment card data must be kept secure at all times.

Important cardholder data is embossed and imprinted on the front and back of all payment (credit and debit) cards.

Front of Payment Card



Back of Payment Card



The **Magnetic Stripe** contains the Account Number, Cardholder Name, and Expiration Date, but does not contain the Security Code or Verification Number.

Other Payment Card Data Security Reminders

- Never share logins and/or passwords with others, including coworkers.
- Receipts, invoices, recording mechanisms, or other transaction documentation can only show the last four digits of the payment card's Account Number.
- The payment card's Expiration Date, Security Code and Verification Number should not be recorded on any transaction documentation.
- Be aware of phishing methods that attempt to trick you into providing card data for malicious purposes. **Never** provide a customer's payment card information, such as Account Number, Expiration Date, Security Code or Verification by phone or e-mail.
- Merchant Card Services and the University's card processor, Global Payments, will **never** contact a department or unit to request a customer's Account Number, Expiration Date, Security Code or Verification Number.

University of Illinois

Payment Card Data Security

The University of Illinois processes thousands of payment card transactions every day.

University employees, temporary hires, students, or volunteers who process payment card transactions on behalf of the University are responsible for protecting and securing card information at all times.

Contact Information

If you have questions or concerns about payment card security, or suspect someone of handling card data insecurely, call Merchant Card Services at 217-244-9384, or send an e-mail to: merchantcardhelp@uillinois.edu.

University of Illinois
Office of Treasury/Merchant Card Services
506 S. Wright St.
Rm. 254 Henry Admin Bldg, MC-363
Urbana, IL 61801
Phone: 217-244-9384
Fax: 217-239-6719
Web: www.treasury.uillinois.edu/merchant_card_services

Why are we doing this?

The University of Illinois has an obligation to safeguard payment card information. As a University employee, temporary hire, student, or volunteer who processes payment card transactions, **you are responsible for protecting and securing card information at all times**.

Payment card data should be treated as carefully as any other confidential information because the customer trusts that his/her payment card information will be protected.

What happens if payment card information is lost or stolen?

Stolen payment card data might be used to make counterfeit cards or sold for illegal purposes, such as facilitating identity theft.

Such a breach in security could result in significant monetary fines to the University and tremendous loss of reputation and trust from customers:

- An expensive forensic investigation must be performed to determine how the breach occurred and how much data has been lost.
- The University department will be fined for the breach and other associated costs, such as the forensic investigation.
- The entire University could lose the privilege to continue accepting payment (credit and debit) cards.

Payment Card Handling Security: Card Present

Card Present transactions are face-to-face, where the customer physically presents the actual payment card for a transaction.

The payment card's **Magnetic Stripe** is swiped during a **Card Present** transaction and read by the terminal or point-of-sale (POS) magnetic stripe reader.

A Personal Identification Number (PIN) is a private code which is not stored on the payment card or within the **Magnetic Stripe**. The customer must enter their PIN during a **Card Present Debit** transaction.

Card Present Security

- Shield the payment card from other customers while processing the transaction.
- Keep the customer's payment card in his/her view.
- Never ask a customer for his/her private Personal Identification Number (PIN).

Payment Card Handling Security: Card Not Present

In a **Card Not Present** transaction, you manually enter the payment card data that is provided by a customer via mail, telephone, or faxed order.

In addition to the Cardholder Name, Account Number, and Expiration Date, the card's billing address (includes street number and ZIP code) and Security Code or Verification Number must be entered during a **Card Not Present** transaction.

Card Not Present Security

- Phone, U.S. Mail, and stand-alone fax machines are the only secure methods for accepting payment card information to process a sale/transaction.
- Never send or accept payment card information via e-mail.
- Do not keep a copy of payment card data, such as Account Number, Expiration Date, Security Code or Verification Number, after the transaction has been authorized.
- Never store payment card data electronically, such as in a database or spreadsheet.
- Keep any papers containing payment card information secure at all times.