



# Guide to Online Payments

UNIVERSITY OF CALIFORNIA POLICE DEPARTMENT  
601 Westwood Plaza, Los Angeles, California 90095  
310.825.1491 ■ 310.206.2550 Fax  
<http://www.ucpd.ucla.edu>



EMERGENCY: CALL 911

**This is information about payment technologies and how to make your transactions as safe and secure as possible.**

You use the Internet to shop. Most use credit or debit cards to pay for online purchases, but other payment methods, like PayPal, are becoming more common.

Online shoppers use credit cards to pay for their online purchases. Debit cards authorize merchants to debit your bank account electronically. Your debit card may be an ATM card that can be used for retail purchases. Some cards have both credit and debit features: You select the payment option at the point-of-sale. Although a debit card may look like a credit card, the money for debit purchases is transferred immediately from your bank account to the merchant's account. Also, your liability limits for a lost or stolen debit card and unauthorized use are different from your liability if your credit card is lost, stolen or used without your authorization. There are other electronic payment systems. Their goal is to make purchasing simpler. For example, stored-value cards let you transfer cash value to a card. They're commonly used on public transportation, at universities, at gas stations and for pre-paid telephone use. Many retailers also sell stored-value cards in place of gift certificates. Others work online, for example, to buy an item from a website. Some have both offline and online features. Some cards can be "reloaded" with additional value, at a cash machine; other cards are disposable you throw them away after you use all their value.

## Protect Your Information

You can take steps to make sure your transactions are secure and your personal information is protected. Here's how:

- Use a secure browser software that encrypts the information you send over the Internet to protect the security of your information as it is transmitted. Be sure your browser has up-to-date encryption capabilities by using the latest version available. When submitting your information, look for the "lock" icon on the browser's status bar and "https" in the URL address for a site, to be sure your information is secure during transmission.
- Check the privacy policy before you provide any personal information to a site. Specifically, determine how the information will be used or shared with others. Check the site's statements about the security provided for your information. Some website disclosures are easier to find than others. Look at the bottom of the home page, on order forms or in the FAQs section of a site. If you're not comfortable with the policy, consider doing business elsewhere.
- Check the refund and shipping policies of a site you visit, before you make your purchase. Look closely at disclosures about the website's refund and shipping policies. Again, search through the website for these disclosures.
- Keep your personal information private. Don't disclose your personal information such as your address, phone number, SSN, bank account number or email address unless you know who's collecting the information, why they're collecting it and how they'll use it.
- Give payment information only to businesses you know and trust, and only when and where it

is appropriate like an order form. Never give your password to anyone online, even your Internet service provider. Do not download files sent to you or click on links from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your computer.

- Keep records of your online transactions and check your email for contacts by merchants with whom you're doing business. Merchants may send you important information about your purchases.

- Review your monthly credit card and bank statements for any errors or unauthorized purchases promptly and thoroughly. Notify your card issuer immediately if your credit or debit card is lost or stolen, or if someone is using your accounts without your permission.

**Fair Credit Billing Act (FCBA) and Electronic Fund Transfer Act (EFTA) establish protections against lost or stolen credit/debit cards and procedures for resolving errors that can include:**

- Credit charges or electronic fund transfers that you or anyone you've authorized to use your account have not made;
- Credit charges or electronic fund transfers that are incorrectly identified or show the wrong amount or date;
- Computation or similar errors;
- A failure to properly reflect payments or credits, or electronic fund transfers;
- Not mailing or delivering credit billing statements to your current address, as long as that address was received by the creditor in writing at least 20 days before the billing period ended; and

- Credit charges or electronic fund transfers for which you request an explanation or documentation, because of a possible error.

**For Credit:** FCBA generally applies to "open end" credit accounts like credit cards and revolving charge accounts, like department store accounts. It does not apply to loans or credit sales that are paid according to a fixed schedule until the entire amount is paid back, like a car loan.

**Lost or Stolen Credit Cards:** Under FCBA, your liability for lost or stolen credit cards is limited to \$50. If the loss involves only your credit card number (not the card), you have no liability for unauthorized use. Notify your card issuer promptly upon discovering the loss. Most companies have toll-free numbers and 24-hour service to deal with such emergencies. Always follow up with a letter and keep a copy for your records.

**Billing Errors:** FCBA's settlement procedures apply to disputes about "billing errors" for openend accounts, including unauthorized charges (you cannot be liable for more than \$50 for unauthorized credit charges); charges for goods or services you didn't accept or weren't delivered as agreed; charges that are incorrectly identified or show the wrong amount or date; math errors; a failure to properly reflect payments or credits; not mailing or delivering credit billing statements to your current address, if the address was received by the creditor in writing at least 20 days before the billing period ended; and charges for which you request an explanation or documentation, because of a possible error.

To take advantage of FCBA's protections for errors on your account, write to the creditor at the address given for billing inquiries. Include

your name, address, account number and a description of the billing error. Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. And if you send your letter by certified mail return receipt requested, you'll have proof that the creditor received it. Include copies (not originals) of sales slips or other documents that support your position. Keep a copy of your dispute letter. The creditor must acknowledge your dispute in writing within 30 days after it is received, unless the problem is resolved within that period. The creditor must conduct an investigation and either correct the mistake or explain why the bill is believed to be correct, within two billing cycles (but not more than 90 days), unless the creditor provides a permanent credit instead. You may withhold payment of the amount in dispute and any related finance charges and the creditor may not take any action to collect that amount during the dispute.

**For Debit:** EFTA applies to electronic fund transfers transactions involving ATMs, debit cards and other point-of-sale debit transactions and other electronic banking transactions that can result in the withdrawal of cash from your bank account.

**Lost or Stolen Debit Cards:** If someone uses your debit card or makes other electronic fund transfers, without your permission, you can lose from \$50 to \$500 or more, depending on when you report the loss or theft. If you report the loss within two business days after you discover the problem, you will not be responsible for more than \$50 for unauthorized use. However, if you do not report the loss within 2 business days after you realize the card is missing, but you do report its loss within 60 days after your statement is mailed to you, you could lose as much as \$500 because of an unauthorized withdrawal. And if you do not report an unauthorized transfer or

withdrawal within 60 days after your statement is mailed to you, you risk unlimited loss. That means you could lose all the money in your account and the unused portion of your maximum line of credit established for overdrafts.

Some financial institutions may voluntarily cap your liability at \$50 for certain types of transactions, regardless of when you report the loss or theft; because this is voluntary, their policies could change at any time. Ask your financial institution about its liability limits. To take advantage of EFTA's error resolution procedures, you must notify your financial institution of the problem no later than 60 days after the statement containing the problem or error was sent. Although most financial institutions have a toll-free number to report the problem, you should follow-up in writing. For retail purchases, your financial institution has up to 10 business days to investigate after receiving your notice of the error. The financial institution must tell you the results of its investigation within 3 business days of completing its investigation. The error must be corrected within 1 business day after determining the error has occurred. If the institution needs more time, it may take up to 90 days, in many situations, to complete the investigation - but only if it returns the money in dispute to your account within 10 business days after receiving notice of the error, while it reviews your concerns.

**For more information on crime prevention, contact:**

## **CRIME PREVENTION UNIT**

**UCLA Police Department**

**601 Westwood Plaza  
Los Angeles, CA 90095  
(310) 825-6111**

**[www.ucpd.ucla.edu](http://www.ucpd.ucla.edu)**

*“Working together to keep our community safe”*