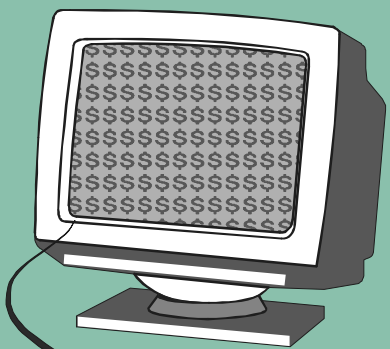
FTC FACTS for Consumers

FOR THE CONSUMER
www.ftc.gov
FEDERAL TRADE COMMISSION
1-877-FTC-HELP

A Consumer's Guide to

e-Payments



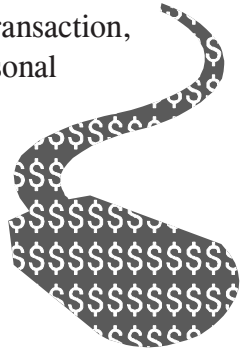
credit
Charge
debit
stored-value

The Internet has taken its place beside the telephone and television as an important part of people's lives. Consumers use the Internet to shop, bank and invest online. Most consumers use credit or debit cards to pay for online purchases, but other payment methods, like "e-wallets," are becoming more common.

The Federal Trade Commission (FTC) wants you to know about these payment technologies and how to make your transactions as safe and secure as possible. Keep these tips in mind as other forms of electronic commerce, like mobile and wireless transactions, become more available.

AND HOW WOULD YOU LIKE TO PAY?

Most online shoppers use credit cards to pay for their online purchases. But debit cards — which authorize merchants to debit your bank account electronically — are increasing in use. Your debit card may be an automated teller machine (ATM) card that can be used for retail purchases. To complete a debit card transaction, you may have to use a personal identification number (PIN), some form of a signature or other identification, or a combination of these identifiers. Some cards have both credit and debit features: You select the payment



option at the point-of-sale. But remember, although a debit card may look like a credit card, the money for debit purchases is transferred almost immediately from your bank account to the merchant's account. In addition, 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.

Other electronic payment systems — sometimes referred to as "electronic money" or "e-money" — also are now common. 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 colleges and universities, at gas stations, and for prepaid telephone use. Many retailers also sell stored-value cards in place of gift certificates. Some stored-value cards work offline, say, to buy a candy bar at a vending machine; 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. Some stored-value cards contain computer chips that make them "smart" cards: These cards may act like a credit card

as well as a debit card, and also may contain stored value.

Some Internet-based payment systems allow value to be transmitted through computers, sometimes called "e-wallets." You can use "e-wallets" to make "micropayments" — very small online or offline payments for things like a magazine or fast food. When you buy something using your e-wallet, the balance on your online account decreases by that amount. "E-wallets" may work by using some form of stored value or by automatically accessing an account you've set up through a computer system connected to your credit or debit card account.

"PAYING" IT SAFE

The FTC encourages you to take steps to make sure your transactions are secure and your personal information is protected. Although you can't control fraud or deception on the Internet, you can take action to recognize it, avoid it and report it. Here's how.

- **Use a secure browser** — software that encrypts or scrambles the purchase information you send over the Internet — to help guard the security of your information as it is transmitted to a website. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available

from the manufacturer. You also can download some browsers for free over the Internet. When submitting your purchase information, look for the "lock" icon on the browser's status bar, and the phrase "https" in the URL address for a website, to be sure your information is secure during transmission.

- **Check the site's privacy policy**, before you provide any personal financial information to a website. In particular, determine how the information will be used or shared with others. Also check the site's statements about the security provided for your information. Some websites' disclosures are easier to find than others — look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If you're not comfortable with the policy, consider doing business elsewhere.

- **Read and understand the refund and shipping policies** of a website 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 — your address, telephone number, Social Security number, bank account number or e-mail 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 by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- **Keep records of your online transactions and check your e-mail** 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 credit or debit card issuer immediately if your credit or debit card or checkbook is lost or stolen, or if you suspect someone is using your accounts without your permission.

REPORT PROBLEMS IMMEDIATELY

The Fair Credit Billing Act (FCBA) and Electronic Fund Transfer Act (EFTA) establish protections against lost or stolen credit or debit cards, and procedures for resolving errors on credit and bank account statements 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: The FCBA generally applies to "open end" credit accounts — that is, 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 an automobile loan.

Lost or stolen credit cards: Under the 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 itself), you have no liability for unauthorized use. It's best to notify your card issuer promptly upon discovering the loss. Many 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: The FCBA's settlement procedures apply to disputes about "billing errors" for open-end 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.

For more information on e-commerce and the Internet, visit www.ftc.gov.

To take advantage of the FCBA's consumer protections for errors on your account, write to the creditor at the address given for "billing inquiries," not the address for sending your payments. 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: The EFTA applies to electronic fund transfers — transactions involving automated teller machines (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 two 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.

EFT errors: The EFTA's error procedures apply to certain problems. This can include:

- electronic fund transfers that you — or anyone you've authorized to use your account — have not made;

- incorrect electronic fund transfers;
- omitted electronic fund transfers;
- a failure to properly reflect electronic fund transfers; and
- electronic fund transfers for which you request an explanation or documentation, because of a possible error.

To take advantage of the EFTA's error resolution procedures, you must notify your financial institution of the problem not 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 three business days of completing its investigation. The error must be corrected within one 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 stored-value: The FCBA and the EFTA may not cover stored-value cards or transactions involving them, so you may not be covered for loss or misuse of the card. However, stored-value cards still might be useful for micropayments and

other small purchases online because they can be convenient and — in some cases — offer anonymity. Before you buy a stored-value card or other form of e-money, ask the issuer for written information about the product's features. Find out the card's dollar limit, whether it is reloadable or disposable, if there's an expiration date, and any fees to use, reload or redeem (return it for a refund) the product. At the same time, ask about your rights and responsibilities. For example, does the issuer offer any protection in the case of a lost, stolen, misused, or malfunctioning card, and who do you call if you have a question or problem with the card?

FOR MORE INFORMATION

Your financial institution, local consumer protection agency and law enforcement agencies like the Federal Trade Commission or your state Attorney General are among the many organizations working to help consumers understand electronic commerce and new online payment options.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft

and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education

March 2003

FEDERAL TRADE COMMISSION	FOR THE CONSUMER
1-877-FTC-HELP	www.ftc.gov