FTC Facts
For Consumers

focus on CREDIT

Federal Trade Commission
For The Consumer

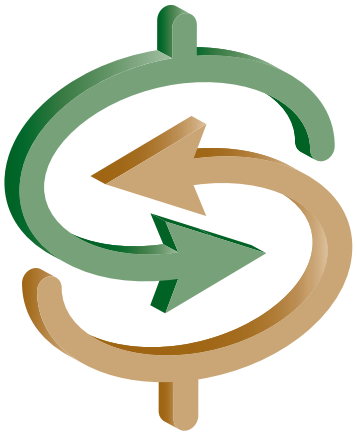
ftc.gov ■ 1-877-ftc-help

March 2012

Electronic Banking

For many consumers, electronic banking means 24-hour access to cash through an automated teller machine (ATM) or Direct Deposit of paychecks into checking or savings accounts. But electronic banking involves many different types of transactions.

Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. EFTs are initiated through devices like cards or codes that let you, or those you authorize, access your account. Many financial institutions use ATM or debit cards and Personal Identification Numbers (PINs) for this purpose. Some use other types of debit cards such as those that require, at the most, your signature or a scan. For example, some use radio frequency identification (RFID) or other forms of "contactless" technology that scan your information without direct contact. The federal Electronic Fund Transfer Act (EFT Act) covers **some** electronic consumer transactions.



Electronic Fund Transfers

EFTs offer several services that you may find practical:

- *ATMs* are electronic terminals that let you bank almost any time. To withdraw cash, make deposits, or transfer funds between accounts, you generally insert an ATM card and enter your PIN. Some financial institutions and ATM owners charge a fee, particularly if you don't have accounts with them or if you engage in transactions at remote locations. Generally, ATMs must tell you they charge a fee and its amount on or at the terminal screen before you complete the transaction. Check the requirements with your institution and at ATMs you use for more information about these fees.

- *Direct Deposit* lets you authorize specific deposits, (like paychecks and Social Security checks and other benefits) to your account on a regular basis. You also may pre-authorize direct withdrawals so that recurring bills (like insurance premiums, mortgages, utility bills,

and gym memberships) are paid automatically. Be cautious before you pre-authorize direct recurring withdrawals to pay companies you aren't familiar with; funds from your bank account could be withdrawn improperly. Also monitor your bank account to ensure that direct recurring payments from your account to others are for the correct amount.

- *Pay-by-Phone Systems* let you call your financial institution with instructions to pay certain bills or to transfer funds between accounts. You must have an agreement with the institution to make such transfers.
- *Personal Computer Banking* lets you handle many banking transactions via your personal computer. For instance, you may use your computer to view your account balance, request transfers between accounts, and pay bills electronically.
- *Debit Card Purchase or Payment Transactions* let you make purchases or payments with a debit card, which also may be your ATM card. This could occur at a store or business, online, or by phone. The process is similar to using a credit card, with some important exceptions. While the process is fast and easy, a debit card purchase or payment transfers money – fairly quickly – from your bank account to the company's account. So it's important that you have funds in your account to cover your purchase. This means you need to keep accurate records of the dates and amounts of your debit card purchases, payments, and ATM withdrawals. Also be sure you know the store or business before you provide your debit card information to avoid the possible loss of funds through fraud. Your liability for unauthorized use, and your rights for error resolution, may be different for a debit card than a credit card.
- *Electronic Check Conversion* converts a paper check into an electronic payment in a store or when a company receives your check in the mail.

  When you give your check to a cashier in a store, the check is run through an electronic system that captures your banking information and the amount of the check. You're asked to sign a receipt and you get a copy for your records. When your check is handed back to you, it should be voided or marked by the merchant so that it can't be used again. The merchant electronically sends information from the check (but not the check itself) to your bank or other financial institution, and the funds are transferred into the merchant's account.

  When you mail-in a check for payment to a merchant or other company, they may electronically send information from your check (but not the check itself) through the system, and the funds are transferred from your account into their account. For a mailed check, you should still receive advance notice from a company that expects to send your check information through the system electronically. For example, the merchant or other company might include the notice on your monthly statement. The notice also should state if the merchant or company will electronically collect from your account a fee – like a "bounced check" fee – if you have insufficient funds to cover the transaction.

Be especially careful with online and telephone transactions that may involve use of your bank account information, rather than a check. A legitimate merchant that lets you use your bank account information to make a purchase or pay on an account should post information about the process on their website or explain the process over the phone. The merchant also should ask for your permission to electronically debit your bank account for the item you're purchasing or paying on. However, because online and telephone electronic debits don't occur face-to-face, be cautious in revealing your bank account information to others. Don't give this information to sellers with whom you have no prior experience or with whom you have not initiated the call, or to companies that seem reluctant to provide information or discuss the process with you. Also check your bank account regularly to be sure that correct amounts were transferred.

Be especially careful with online and telephone transactions that may involve use of your bank account information, rather than a check.

Not all electronic fund transfers are covered by the EFT Act. For example, some financial institutions and merchants issue cards with cash value stored electronically on the card itself. Examples include prepaid phone cards, mass transit passes, and some gift cards. These "stored-value" cards, as well as transactions using them, may not be covered by the EFT Act, or they may be subject to different rules under the EFT Act. (See *Buying, Giving and Using Gift Cards* at **ftc.gov/consumer**). This means you may not be covered for the loss or misuse of the card. Ask your financial institution or merchant about any protections offered for these cards.

Disclosures

To understand your legal rights and responsibilities regarding your EFTs, read the documents you receive from the financial institution that issued your "access device." That is, a card, code or other means of accessing your account to initiate electronic fund transfers. Although the means varies by institution, it often involves a card and/or a PIN. No one should know your PIN except you and select employees of the financial institution. You also should read the documents you receive for your bank account, which may contain more information about EFTs.

Before you contract for EFT services or make your first electronic transfer, the institution must give you the following information in a form you can keep.

- A summary of your liability for unauthorized transfers.
- The telephone number and address of the person to be notified if you think an unauthorized transfer has been or may be made, a statement of the institution's "business days" (which is, generally, the days the institution is open to the public for normal business), and the number of days you have to report suspected unauthorized transfers.

- The type of transfers you can make, fees for transfers, and any limits on the frequency and dollar amount of transfers.
- A summary of your right to receive documentation of transfers, to stop payment on a pre-authorized transfer, and the procedures to follow to stop payment.
- A notice describing the procedures you must follow to report an error on a receipt for an EFT or your periodic statement, to request more information about a transfer listed on your statement, and how long you have to make your report.
- A summary of the institution's liability to you if it fails to make or stop certain transactions.
- Circumstances under which the institution will disclose information to third parties concerning your account.
- A notice by operators of ATMs where you don't have an account that you may have to pay a fee for an EFT or a balance inquiry at the ATM.

In addition to these disclosures, you will receive two other types of information for most transactions: terminal receipts and periodic statements. Separate rules apply to deposit accounts from which pre-authorized transfers are drawn. For example, you must provide authorization that is written or similarly authenticated for pre-authorized transfers from your account, and a copy of that authorization must be given to you. Additional information about pre-authorized transfers is in your contract with the financial institution for that account. You're entitled to a terminal receipt each time you initiate an electronic transfer, whether you use an ATM or make a point-of-sale electronic transfer. The receipt must show the amount and date of the transfer, and its type, such as "from savings to checking." When you make a point-of-sale transfer, you'll probably get your terminal receipt from the salesperson.

Keep and compare your EFT receipts with your periodic statements the same way you compare your credit card receipts with your monthly credit card statement.

You won't get a terminal receipt for regularly occurring electronic payments that you've pre-authorized, like insurance premiums, mortgages, or utility bills. Instead, these transfers will appear on your periodic statement. If the pre-authorized payments vary, however, you should receive a notice of the amount that will be debited at least 10 days before the debit takes place.

You're also entitled to a periodic statement for each statement cycle in which an electronic transfer is made. The statement must show the amount of any transfer, the date it was credited or debited to your account, the type of transfer and type of account(s) to or from which funds were transferred, and the address and telephone number for inquiries. You're entitled to a quarterly statement whether or not electronic transfers were made.

Keep and compare your EFT receipts with your periodic statements the same way you compare your credit card receipts with your monthly credit card statement. This will help you make the best use of your rights under federal law to dispute errors and avoid liability for unauthorized transfers.

Errors

You have 60 days from the date a periodic statement containing a problem or error was sent to you to notify your financial institution. The best way to protect yourself if an error occurs – including erroneous charges or withdrawals from an account, or for a lost or stolen ATM or debit card – is to notify the financial institution by certified letter, return receipt requested, so you can prove that the institution received your letter. Keep a copy of the letter for your records.

> ***If your credit card is lost or stolen, you can't lose more than $50. If someone uses your ATM or debit card without your permission, you can lose much more.***

If you fail to notify the institution of the error within 60 days, you may have little recourse. Under federal law, the institution has no obligation to conduct an investigation if you've missed the 60-day deadline.

Once you've notified the financial institution about an error on your statement, it has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that the error has occurred. If the institution needs more time, it usually is permitted to take up to 45 days to complete the investigation – but only if the money in dispute is returned to your account and you're notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

An error also may occur in connection with a point-of-sale purchase with a debit card. For example, an oil company might give you a debit card that lets you pay for gas purchases directly from your bank account. Or you may have a debit card that can be used for various types of retail purchases. These purchases will appear on your periodic statement from the bank. In case of an error on your account, however, you should contact the card issuer (for example, an oil company or a bank) at the address or phone number provided by the company. Once you've notified the company about the error, it has 10 business days to investigate and tell you the results. In this situation, it may take up to 90 days to complete an investigation, if the money in dispute is returned to your account and you're notified promptly of the credit. If no error is found at the end of the investigation, the institution may take back the money if it sends you a written explanation.

Lost or Stolen ATM or Debit Cards

If your *credit card* is lost or stolen, you can't lose more than $50. If someone uses your *ATM or debit card* without your permission, you can lose much more.

If you report an ATM or debit card missing to the institution that issues the card (card issuer) before it's used without your permission, you can't be held responsible for any unauthorized withdrawals.

If unauthorized use occurs before you report it, the amount you can be held responsible for depends upon how quickly you report the loss to the card issuer.

- If you report the loss within two business days after you realize your card is missing, you won't be responsible for more than $50 for unauthorized use.
- If you fail to report the loss within two business days after you realize the card is missing, but 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 transfer.
- If you fail to report an unauthorized transfer within 60 days after the card issuer mails your statement to you, you risk unlimited loss. For example, you could lose all the money in that account, the unused portion of your maximum line of credit established for overdrafts, and possibly other amounts.

If you failed to notify the card issuer within the time periods allowed because of an extenuating circumstance, such as lengthy travel or illness, it must reasonably extend the notification period. In addition, if state law or your contract imposes liability limits that are lower than under the federal EFT act, those lower limits apply.

Once you report the loss or theft of your ATM or debit card to the card issuer, you're no longer responsible for additional unauthorized transfers occurring after that time. Because these unauthorized transfers may appear on your statements, however, you should carefully review each statement you receive after you've reported the loss or theft. If the statement shows transfers that you did not make or that you need more information about, contact the card issuer immediately, using the special procedures it provided for reporting errors.

Overdrafts for One-Time Debit Card Transactions and ATM Cards

If you make a one-time purchase or payment with your debit card or use your ATM card and don't have the funds to cover it, an overdraft can occur. Your bank must get your permission to charge you a fee to pay for your overdraft on a one-time debit card transaction or ATM transaction. They also must send you a notice and get your opt-in agreement before charging you for this purpose.

For accounts that you have already, if you don't opt-in, the transaction usually will be declined if you have insufficient funds to pay it, and you cannot be charged an overdraft fee. If you open a new account, the bank also cannot charge you an overdraft fee for your one-time debit card or ATM transactions, unless you opt-in to the fees. The bank will give you a notice about opting-in when

you open the account, and you can decide your preference. If you do opt-in, be aware that you have the right to cancel the agreement at any time. If you do not opt-in, you can reconsider later and change your decision.

These rules do not apply to recurrent payments that you set up for making regular debits to your account. For those transactions, your bank can still enroll you in their usual overdraft coverage. If you prefer not to have that coverage (and the fees), contact your bank and see if they will let you discontinue it for those payments.

Limited Stop-Payment Privileges

When you use an electronic fund transfer, the EFT Act does not give you the right to stop payment. If your purchase is defective or your order is not delivered, it's as if you paid cash. That is, it's up to you to resolve the problem with the seller and get your money back.

There is one situation, however, when you can stop payment. If you've arranged for regular payments out of your account to third parties, such as insurance companies, you can stop payment if you notify your institution at least three business days before the scheduled transfer. The notice may be oral or written, but the institution may require a written follow-up within 14 days of the oral notice. If you fail to provide the written follow-up, the institution's responsibility to stop payment ends.

Although federal law provides only limited rights to stop payment, individual financial institutions may offer more rights or state laws may require them. If this feature is important to you, you may want to shop around to be sure you're getting the best "stop-payment" terms available.

Other Rights

The EFT Act protects your right of choice in two specific situations regarding use of electronic fund transfers. First, generally the Act prohibits financial institutions from requiring you to repay a loan by preauthorized electronic transfers. Second, if you're required to receive your salary or government benefit check by EFT, you have the right to choose the institution that will receive these funds.

Suggestions

If you decide to use EFT, keep these tips in mind:

- Take care of your ATM or debit card. Know where it is at all times; if you lose it, report it as soon as possible.
- Choose a PIN for your ATM or debit card that's different from your address, telephone number, Social Security number, or birthdate. This will make it more difficult for a thief to use your card.
- Keep and compare your receipts for all types of EFT transactions with your periodic statements. That way, you can find errors or unauthorized transfers and report them.
- Make sure you know and trust a merchant or other company before you share any bank account information or pre-authorize debits to your account. Be aware that some merchants or companies may use electronic processing of your check information when you provide a check for payment.

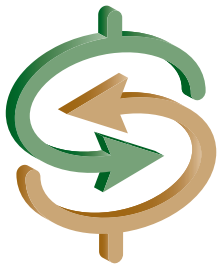
- Review your monthly statements promptly and carefully. Contact your bank or other financial institution immediately if you find unauthorized transactions and errors.

Where to File Complaints

If you think a financial institution or company has failed to fulfill its responsibilities to you under the EFT Act, you may wish to complain to the appropriate federal agency. Visit **www.Helpwithmybank.gov,** a site maintained by The Office of the Comptroller of the Currency. This site provides answers to more than 250 frequently-asked questions on topics like bank accounts, deposit insurance, credit cards, consumer loans, insurance, mortgages, identity theft, and safe deposit boxes.

The FTC works 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 get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.

Watch a video, *How to File a Complaint,* at **ftc.gov/video** to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.



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