Electronic Banking

Federal Trade Commission | ftc.gov

For many people, 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, rights, responsibilities — and sometimes, fees. Do your research. You may find some electronic banking services more practical for your lifestyle than others.

Electronic Fund Transfers

Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology in place of 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 that require 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 with you. The federal Electronic Fund Transfer Act (EFT Act) covers some electronic consumer transactions.

Here are some common EFT services:

ATMs are electronic terminals that let you bank almost virtually 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 your transactions take place

at remote locations. Generally, ATMs must tell you they charge a fee and the amount on or at the terminal screen before you complete the transaction. Check with your institution and at ATMs you use for more information about these fees.

Direct Deposit lets you authorize specific deposits — like paychecks, 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pre-authorize recurring withdrawals to pay companies you aren't familiar with; funds from your bank account could be withdrawn improperly. Monitor your bank account to make sure direct recurring payments take place and are for the right 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 your institution to make these transfers.

Personal Computer Banking lets you handle many banking transactions using your personal computer. For example, you may use your computer to 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. Transactions can take place in-person, online, or by phone. The process is similar to using a credit card, with some important exceptions: a debit card purchase or payment transfers money quickly from your bank account to the company's account, so you

have to have sufficient 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. 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 dealing with errors, 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 gets 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 sign a receipt and you get a copy for your records. When your check is given 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 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; the funds are transferred from your account into their account. For a mailed check, you still should get notice from a company that expects to send your check information through the system electronically. For example, the company might include the notice on your monthly statement. The notice also should state if the company will electronically collect a fee from your

account — like a "bounced check" fee — if you don't have enough money to cover the transaction.

Be careful with online and telephone transactions that may involve the 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 its website or explain the process on the phone. The merchant also should ask for your permission to electronically debit your bank account for the item you're buying or paying on. However, because online and telephone electronic debits don't occur face-to-face, be cautious about sharing your bank account information. Don't give out this information when you have no experience with the business, when you didn't initiate the call, or when the business seems reluctant to discuss the process with you. Check your bank account regularly to be sure that the right amounts were transferred.

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, general purpose reloadable cards, 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. 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.

For details, see *Gift Cards* at **consumer.ftc.gov**.

Disclosures

To understand your rights and responsibilities for your EFTs, read the documents you get from the financial institution that issued your "access device" – the card, code or other way you access your account to transfer money electronically. Although the method varies by institution, it often involves a card and/or a PIN. No one should know your PIN but you and select employees at your 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 format you can keep.

- a summary of your liability for unauthorized transfers
- the phone number and address for a contact if you think an unauthorized transfer has been or may be made, the institution's "business days" (when 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 get documentation of transfers and to stop payment on a pre-authorized transfer, and how you stop payment
- a notice describing how to report an error on a receipt for an EFT or your 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 when the institution will share information about your account with third parties
- a notice that you may have to pay a fee charged by operators of ATMs where you don't have an account, for an EFT or a balance inquiry at the ATM, and charged by networks to complete the transfer.

You also will get two more 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, pre-authorized transfers from your account need your written or similar authorization, 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, for transfers over $15. The receipt must show the amount and date of the transfer, and its type, like "from savings to checking." It also must show a number or code that identifies the account, and list the terminal location and other information. When you make a point-of-sale transfer, you'll probably get your terminal receipt from the salesperson.

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 statement. If the pre-authorized payments vary, however, you should get 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, the account number, the amount of any fees charged, the account balances at the beginning and end of the statement cycle, and the address and phone 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 is to notify the financial institution by certified letter. Ask for a return receipt so you can prove that the institution got your letter. Keep a copy of the letter for your records.

Under federal law, the institution has no obligation to conduct an investigation if you miss 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. An institution usually is permitted to take more time — 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 directly from your bank account. Or you may have a debit card that can be used for a various types of retail purchases. These purchases will appear on your bank statement. In case of an error on your account, however, you should contact the card issuer (for example, the oil company or bank) at the address or phone number provided by the company for errors. 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 before someone uses the card without your permission, you can't be responsible for any unauthorized withdrawals. But if unauthorized use occurs before you report it, the amount you can be responsible for depends on 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 of unauthorized use.
- If you report the 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 don't report an unauthorized use of your card within 60 days after the card issuer mails your statement to you, you risk unlimited loss; you could lose all the money in that account, the unused portion of your maximum line of credit established for overdrafts, and maybe more.

If an extenuating circumstance, like lengthy travel or illness, keeps you from notifying the card issuer within the time allowed, the notification period must be extended. In addition, if state law or your contract imposes lower liability limits than the federal EFT Act, the lower limits apply.

Once you report the loss or theft of your ATM or debit card to the card issuer, you're not responsible for additional unauthorized use. Because unauthorized transfers may appear on your statements, though, read each statement you receive after you've reported the loss or theft. If the statement shows transfers that you didn't make or that you need more information about, contact the card issuer immediately, using the special procedures it provided for reporting errors.

For more information, see *Lost or Stolen Credit, ATM, and Debit Cards* at **consumer.ftc.gov**.

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 sufficient funds, 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 accounts that you already have, unless you opt-in, the transaction will be declined if you don't have the funds to pay it, and you can't be charged an overdraft fee. If you open a new account, the bank can't charge you an overdraft fee for your one-time debit card or ATM transactions, either, 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 whether to opt-in. If you opt-in, you can cancel any time; if you don't opt-in, you can do it later.

These rules do not apply to recurring payments from your account. For those transactions, your bank can enroll you in their usual overdraft coverage. If you don't want the coverage (and the fees), contact your bank to 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 isn't delivered, it's as if you paid cash: It's up to you to resolve the problem with the seller and get your money back.

One exception: If you arranged for recurring payments out of your account to third parties, like insurance companies or utilities, you can stop payment if you notify your institution at least three business days before the scheduled transfer. The notice may be written or oral, but the institution may require a written follow-up within 14 days of your oral notice. If you don't follow-up in writing, the institution's responsibility to stop payment ends.

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

Additional Rights

The EFT Act protects your right of choice in two specific situations: First, financial institutions can't require you to repay a loan by preauthorized electronic transfers. Second, if you're required to get your salary or government benefit check by EFT, you can choose the institution where those payments will be deposited.

For More Information and Complaints

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 statements so 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 process your check information electronically when you pay by check.
- Read your monthly statements promptly and carefully. Contact your bank or other financial

institution immediately if you find unauthorized transactions and errors.

If you think a financial institution or company hasn't met its responsibilities to you under the EFT Act, you can complain to the appropriate federal agency. Visit the Consumer Financial Protection Bureau (**consumerfinance.gov**) or **HelpWithMyBank.gov**, a site maintained by the Office of the Comptroller of the Currency, for answers to frequently-asked questions on topics like bank accounts, deposit insurance, credit cards, consumer loans, insurance, mortgages, identity theft, and safe deposit boxes, and for other information about federal agencies that have responsibility for financial institutions.

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 the video, *How to File a Complaint*, at **consumer.ftc.gov/media** 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
ftc.gov
August 2012