

FEDERAL RESERVE BANK  
OF NEW YORK

Circular No. 8847  
June 11, 1980

NEW CONSUMER PAMPHLET ON ELECTRONIC FUND TRANSFERS

*To All Financial Institutions, and Others Concerned,  
in the Second Federal Reserve District:*

Enclosed is a new pamphlet, entitled, "Alice in Debitland," issued by the Board of Governors of the Federal Reserve System.

The pamphlet introduces the technology of electronic fund transfer systems through the eyes of Lewis Carroll's *Alice* who, upon encountering this new payments mechanism, is convinced that "something interesting is bound to happen."

This 16-page illustrated pamphlet addresses many questions that the public may have regarding electronic fund transfers, such as what record or evidence of transactions will be available, what are the procedures for correcting errors, what is the potential risk of lost or stolen cards, and how will one resolve complaints.

The publication is being distributed by the New York Federal Reserve Bank in conjunction with its Consumer Credit Information (CCI) program. Additional copies are available, free of charge, from our Public Information Department (Tel. No. 212-791-6134). Requests for more than 500 copies should be made in writing to that department.

CCI materials are intended as a resource to help both creditors and borrowers. Comments are always welcome and may be directed to Peter Bakstansky, Vice President.

ANTHONY M. SOLOMON,  
*President.*



# Alice in Debitland

---

CONSUMER PROTECTIONS AND THE ELECTRONIC FUND TRANSFER ACT

---

---

## ALICE'S ADVENTURE

---

*It's 1980. Alice has pushed through a revolving glass door into the department store and selected several items. Reaching into her wallet, she pulls out a debit card with such beautifully printed letters it seems to say, "Use Me."*

*"Curiouser and curiouser," remarks Alice. But she has already adjusted easily to the change credit cards have made in her life. So, reasoning from her experience in a childhood adventure, Alice supposes it's simply a question of opposites: "If a credit card postpones payment, then a debit card probably speeds it up. It's sure to make SOME change in the size of my bank account, and either way I shall have my purchases."*

*Alice hands her debit card to the clerk, who inserts it into a computer terminal. At the press of a button, electronic impulses fly to the Wonderland Bank, where Alice keeps her checking account. Automatically and instantaneously, funds are transferred from her account to the merchant's.*

*Alice gathers her parcels just fast enough to side-step the White Rabbit, who is hurrying by with his pocket watch and fretting, "No time, no time." "Yes," reflects Alice, "That seems to be the whole point."*

*Indeed it is. Instant money. EFT.*



---

## CAN ALICE ADJUST?

---



Alice's debit card is just one way to use EFT, electronic fund transfer systems that effect payment between parties by substituting an electronic signal for cash or checks.

Are we heading for a "checkless society?" Probably not. But putting a dent in the pile of paper checks in the payments system—or reducing the rate it has been growing—is clearly one advantage to electronic banking.

Today, the cost of clearing each check through the banking system is estimated at between 30 to 50 cents per check, to which must be added the costs of paper, printing, and mailing. Moreover, checks—except your own check presented at your own bank—take time to cash: time for delivery, endorsement, presentation to another person's bank, and circuitous travel through various stations in the clearing system. The technology now exists to lower the costs of the payments mechanism and make it more efficient and convenient by reducing paperwork.

---

In fact, a number of steps have already been taken toward a payments mechanism that moves money between accounts in a fast, paperless way. These are some examples of EFT systems in operation:

- ♦ **Automated Teller Machines (ATMs).** Consumers can do their banking without the assistance of a teller—using these machines to get cash, to make deposits, to pay bills, or to transfer funds from one account to another electronically. First the consumer inserts a plastic “debit” or EFT card into the machine; next, using a number keyboard, enters a code, presses the appropriate transaction button, and authorizes a debit or credit of the desired amount; then—in the case of a withdrawal—waits for cash to be dispensed. (The code is often called a personal identification number, or “PIN.”)

- ♦ **Point of Sale Terminals (POS).** In some communities—like Alice’s—electronic terminals located in shopping areas allow the transfer of funds from the consumer’s account to the merchant’s. To pay for a purchase, the consumer inserts an EFT card into the terminal and punches in an amount. Money is taken out of the consumer’s account and credited to the merchant’s account electronically.
- ♦ **Preauthorized Payments.** This is a method of automatically withdrawing or depositing funds to an individual account, under authority given to the financial institution or to a third party (an employer, for example) by the account holder. For example, consumers can authorize direct electronic deposit of wages, social security or dividend payments to be made to their accounts. Or, they can authorize finan-

---

cial institutions to make regular, recurring payments of insurance, mortgage, utility or other bills.

- ♦ **Telephone Transfers.** Consumers can transfer funds from one account to another—from savings to checking, for example—or can order payment of specific bills by phone.

Despite these developments, for many of us the world of electronic money is still a wonderland. Alice, encountering change, is satisfied that *something* interesting is bound to happen. But most of us need to understand EFT in order to adjust to it. Recognizing this, Congress passed the Electronic Fund Transfer Act.



---

## THE CONSUMER ASKS QUESTIONS

---



The EFT Act, and Regulation E issued by the Federal Reserve Board to carry it out, give the consumer answers to several basic questions about EFT.

Most questions center on this issue: a check is a piece of paper with information that authorizes a bank to withdraw a certain amount of money from one person's account and pay that amount to another person. EFT transmits this information without the paper, but:

- ♦ What record—what evidence—will I have of my transactions?
- ♦ How easily will I be able to correct errors?
- ♦ What if someone steals money from my account?
- ♦ Do I have to use EFT?

Here are the answers the EFT Act gives.

---

## WHAT RECORD WILL I HAVE OF MY TRANSACTIONS?

---

A cancelled check is permanent proof that a payment has been made. Can an electronic terminal give this proof?

The answer is yes. If you use an ATM to withdraw money or make deposits, or a point-of-sale terminal to pay for a purchase, you can get a written receipt—much like the sales receipt you get with a cash purchase—showing the amount of the transfer, the date it was made, and other information. This receipt is your record of transfers initiated at an electronic terminal.

Your periodic statement must also show all electronic transfers to and from your account, including those made at electronic terminals, or under a preauthorized arrangement, or ordered by telephone. It will also name the party to whom payment has been made, and show any fees and your opening and closing balances.

Your monthly statement is proof of payment to a third party, your record for tax or other purposes, and your way of checking

and reconciling EFT transactions with your account balance.



**Remember** when you're paying bills that EFT transactions may take place **IMMEDIATELY**. When you write a check you enter the amount on your checkbook stub and deduct it to keep a running account of your balance. Be sure to keep the same kind of accurate, day-to-day record of your EFT transactions.

---

## HOW EASILY WILL I BE ABLE TO CORRECT ERRORS?

---

The procedure for reporting errors is somewhat different with EFT than it is with credit cards. But, as with credit cards, financial institutions must investigate and correct promptly any EFT errors you report.

If you believe there has been an error in an electronic fund transfer:

1. Write or call your financial institution immediately if possible, but no later than 60 days from the time the first statement that you think shows an error was mailed to you. Give your name and account number and explain why you believe there is an error, what kind of error, and the dollar amount and date in question. If you call, you may be asked to send this information in writing within 10 business days.

2. The financial institution must promptly investigate an error and resolve it within 45 days.



- ◆ However, if the financial institution takes longer than 10 business days to complete its investigation, it must re-credit your account for the amount in question while it finishes the investigation. In the meantime, you will have full use of the funds in question.

3. The financial institution must notify you of the results of its investigation:

- ◆ If there was an error, the institution must correct it promptly—for example, by making a recredit final.
- ◆ If it finds no error, the financial institution must explain in writing why it believes there was no error and let you know that it has deducted any amount recredited during the investigation. You may ask for copies of documents relied on for the investigation.



On a credit purchase, you usually resolve an error **BEFORE** making payment. With EFT an error will show up on your statement **AFTER** funds have been taken out of your account. So examine your statements carefully and report errors promptly.

---

## WHAT ABOUT LOSS OR THEFT?

---

It's important to be aware of the potential risk in using EFT, which differs from the risk on a credit card.

On lost or stolen credit cards, your loss is limited to \$50 per card. On an EFT card, your liability for unauthorized withdrawals is also limited to \$50 if you notify the financial institution within 2 business days after learning of loss or theft of your card or code.

But—

- ◆ You could lose as much as \$500 if you do not tell the card issuer within 2 business days after learning of loss or theft.
- ◆ If you do not report an unauthorized transfer that appears on your statement within 60 days after the statement is mailed to you, you risk *unlimited* loss on transfers made after the

60-day period. That means you could lose all the money in your account plus your maximum overdraft line of credit.

Here's an example of the rules:



*The Knave of Hearts stole Alice's debit card and secret code. The next day he withdrew \$250, all the money Alice had in her checking account. Five days later, he with-*

---

drew another \$500, triggering Alice's overdraft line of credit.

Alice did not realize her card was stolen until she received a statement from the Wonderland Bank, showing withdrawals of \$750 she did not make. She called the bank right away.

Alice's liability is \$50.

Now suppose that when Alice got her bank statement she didn't look at it and didn't call the bank. Seventy days after the statement was mailed to her, the Knave withdrew another \$1,000, reaching the limit on Alice's line of credit. In this case, Alice would be liable for \$1,050 (\$1,000 for transfers made more than 60 days after the statement was mailed; \$50 for transfers before the end of the 60 days).



1. Report AT ONCE if you believe an EFT card has been lost or stolen. The best way to report is by telephone. Keep the phone number for reporting loss or theft handy. If you write about a loss, your notice will be effective on the day you mail your letter.

2. You will usually have a separate code or "PIN" without which your EFT card can't be used. Do NOT keep your card and code together in your wallet. A card without a code can't be used by a thief. And don't give out your code to anyone or let anyone see the numbers you punch in.

---

## DO I HAVE TO USE EFT?

---

A financial institution may send you an EFT card that is *VALID FOR USE* only if you ask for one, or in order to replace or renew an expired card. The financial institution must also give you the following information about your rights and responsibilities:

- ◆ A notice of your liability in case a card is lost or stolen;
- ◆ A telephone number for reporting loss or theft;
- ◆ A description of the error resolution procedures;
- ◆ The institution's business days;
- ◆ The kinds of electronic fund transfers you may make and whether there are limits on the frequency or dollar amounts of such transfers;

- ◆ Any charge by the institution for using EFT;
- ◆ Your right to receive records of electronic fund transfers;
- ◆ How to stop payment of a preauthorized transfer;
- ◆ The financial institution's liability to you for any failure to make or to stop transfers;
- ◆ The conditions under which a financial institution will give information to third parties about your account.

Generally, you must also be notified in advance of any change in terms of the account that would increase fees or liability or limit transfers.

A financial institution may send you a card you did not request only if the card is

---

**NOT VALID FOR USE.** An "unsolicited" card can be validated only at your request and only after the institution verifies that you are the person whose name is on the card. It must also be sent with a clear explanation of how to destroy or dispose of the card if you don't want to use it.

In addition, the EFT Act provides that no person can require you to repay an extension of credit by electronic means. And, although your employer or a government agency can require you to receive your salary or a government benefit by electronic transfer, you have the right to choose the financial institution at which you will receive the funds.



You can use cash, checks, credit cards, EFT or any combination of services. The choice depends, of course, on how you weigh convenience, fees, money management needs and other considerations. If you do use EFT, compare information about services and charges by financial institutions before you make your decision.

---

## SPECIAL QUESTIONS ABOUT PREAUTHORIZED PLANS

---



**Q. How will I know a preauthorized credit has been made?**

A. There are various ways you can be notified. Notice can be given by the payor that the deposit has been sent to your financial institution. Otherwise, a financial institution may provide notice that it has received the credit or will send you a notice only when it has not received the funds. Financial institutions also have the option of giving you a telephone number you can call to check on a preauthorized transfer.

**Q. How do I stop a preauthorized payment?**

A. You may stop any preauthorized payment by calling or writing the financial institution, so that your order is received at least 3 business days before the payment date. Written confirmation of a telephone notice to stop payment may be required.

**Q.** If the payments I preauthorize vary in amount from month to month, how will I know how much will be transferred out of my account?

**A.** You have the right to be notified of all varying payments at least 10 days in advance. Or, you may choose to specify a range of amounts and to be told only when a transfer falls outside that range. You may also choose to be told only when a transfer differs by a certain amount from the previous payment to the same company.

**Q.** Do the EFT Act protections apply to all preauthorized plans?

**A.** No. They do not apply to automatic transfers from your account to the institution that holds your account or vice versa. For example, they do not apply to automatic payments made on a mortgage held by the financial institution where you have your EFT account. The EFT Act also does not apply to automatic transfers among your accounts at one financial institution.

---

## COMPLAINTS AND PENALTIES

---



If you have a complaint about an EFT service, first try to resolve it directly with the financial institution. If that fails, you can contact the Division of Consumer and Community Affairs, Board of Governors of the Federal Reserve System, Washington, D.C. 20551. The Board supervises only State-chartered banks that are members of the Federal Reserve System; if your complaint is outside its authority, the Board will refer your inquiry to the proper regulatory agency. Or, you may write directly to the enforcement agency identified on page 16. You as an individual may also sue for actual damages plus a penalty of not less than \$100 or more than \$1,000. Class action suits are also permitted.

---

## FEDERAL ENFORCEMENT AGENCIES

---

### **National Banks**

Comptroller of the Currency  
Office of Customer and  
Community Programs  
Washington, D.C. 20219

### **State Member Banks**

Federal Reserve Bank serving the  
district in which the State member  
bank is located.

### **Nonmember Insured Banks**

Federal Deposit Insurance Corpora-  
tion Regional Director for the  
region in which the nonmember in-  
sured bank is located.

**Savings Institutions Insured by the  
FSLIC and Members of the FHLB  
System (except for Savings Banks  
insured by FDIC)**

The Federal Home Loan Bank  
Board Supervisory Agent in the  
district in which the institution is  
located.

### **Federal Credit Unions**

Division of Consumer Affairs  
National Credit Union  
Administration  
1776 G. Street, N.W.  
Washington, D.C. 20456

**Creditors Subject to Civil  
Aeronautics Board**

Director  
Bureau of Consumer Protection  
Civil Aeronautics Board  
Washington, D.C. 20428

### **Brokers and Dealers**

Division of Market Regulation  
Securities and Exchange  
Commission  
Washington, D.C. 20549

**Retail, Department Stores, Con-  
sumer Finance Companies, Certain  
Other Financial Institutions, and  
All Nonbank Debit Card Issuers**  
Federal Trade Commission  
Electronic Fund Transfers  
Washington, D.C. 20580

Additional copies of this handbook and other consumer pamphlets are available upon request from Publications Services, Division of Support Services, Board of Governors of the Federal Reserve System, Washington, D.C. 20551.

Board of Governors of the Federal Reserve System June 1980