Debit Scams

Fast Facts

Do not give out your checking account information over the phone **unless** you know the company and understand why the information is necessary.

If someone says they are taping your call, **ask why**. Do not be afraid to ask questions.

Do not give out checking account information over the phone.

Legitimate companies will **not** ask for your bank account information unless you have expressly agreed to the automatic debiting of your checking account.

Fraudulent telemarketers have found yet another way to steal your money, this time from your checking account. A debit card is an electronic card issued by a bank which allows bank clients access to their accounts to withdraw cash or pay for goods and services. Consumers across the country are complaining about unauthorized debits from their checking accounts.

Automatic debiting of your checking account can be a legitimate payment method; many people pay mortgages or make car payments this way. But fraudulent telemarketers are abusing this method of payment. Therefore, if a caller asks for your checking account number or other information printed on your check, you should follow the same warning that applies to your credit card number – do not give out checking account information over the phone unless you are familiar with the company and agree to pay for something. Remember, if you give your checking account number over the phone to a stranger for "verification" or "computer purposes," that person could use it to improperly take money from your checking account.

How the scam works

You either get a postcard or a telephone call saying you have won a free prize or can qualify for a major credit card, regardless of past credit problems. If you respond to the offer, the telemarketer often asks you right away,

"Do you have a checking account?" If you say "yes," the telemarketer then goes on to explain the offer. Often it sounds too good to pass up.

Near the end of the sales pitch, the telemarketer may ask you to get one of your checks and to read off all of the numbers at the bottom. Some deceptive telemarketers may not tell you why this information is needed. Other deceptive telemarketers may tell you the account information will help ensure that you qualify for the offer. And, in some cases, the legitimate telemarketer will honestly explain that this information will allow them to debit your checking account.

Once a telemarketer has your checking account information, it is put on a "demand draft," which is processed much like a check. The draft has your name, account number, and states an amount. Unlike a check, however, the draft does not require your signature. When your bank receives the draft, it takes the amount on the draft from your checking account and pays the telemarketers' bank. You may not know that your bank has paid the draft until you receive your bank statement.

What you can do to protect yourself

It can be difficult to detect an automatic debit scam before you suffer financial losses. If you do not know whom you are talking to, follow these suggestions to help you avoid becoming a victim:

- Do not give out your checking account number over the phone unless you know the company and understand why the information is necessary.
- If someone says they are taping your call, ask why. Do not be afraid to ask questions.
- Companies do not ask for your bank account information unless you have expressly agreed to this payment method.

It is the law

Under Wisconsin's Direct Marketing Law (Wis. Admin. Code s. ATCP 127.10) seller or telemarketer is required by law to obtain your verifiable authorization to obtain payment from your bank account. That means whoever takes your bank account information over the phone must have your express permission to debit your account, and must use one of three ways to get it. The person must tell you that money will be taken from your bank account. If you authorize payment of money from your bank account, they must then get your written authorization, tape record your authorization, or send you a written confirmation before debiting your bank account. If they tape record your authorization, they must disclose, and you must receive, the following information:

- The date of the demand draft;
- The amount of the draft(s);
- The payees' (who will receive your money) name;
- The number of draft payments (if more than one);
- A telephone number that you can call during normal business hours; and
- The date that you are giving your oral authorization.

If a seller or telemarketer uses written confirmation to verify your authorization, they must give you all the information required for a tape recorded authorization and tell you in the confirmation notice the refund procedure you can use to dispute the accuracy of the confirmation and receive a refund.

What to do if you are a victim

If telemarketers cause money to be taken from your bank account without your knowledge or authorization, they have violated the law. If you receive a written confirmation notice that does not accurately represent your understanding of the sale, follow the refund procedures that should have been provided and request a refund of your money. If you do not receive a refund, it is against the law. If you believe you have been a victim of fraud, contact your bank immediately. Tell the bank that you did not okay the debit and that you want to prevent further debiting.

You also should contact Consumer Protection. Depending on the timing and the circumstances, you may be able to get your money back.

The Federal Fair Credit Billing Act (FCBA) (15 USC § 1601) and Electronic Fund Transfer Act (EFTA) (15 USC § 1693), also known as Regulation E, offers protection if your credit, ATM, or debit cards are lost or stolen.

- Your liability for unauthorized use of your lost or stolen ATM or debit card is as follows:
- $50 if you notify the bank within 2 days.
- Up to $500 if you notify the bank more than 2 days after the loss or theft, but less than 60 days after your statement is sent to you.
- Unlimited if you fail to report the fraud within 60 days after you receive your bank statement.
- Your liability for unauthorized use of your lost or stolen credit card tops out at $50.

Check your statements and report any unauthorized activities to your bank immediately.

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

DebitScams259 (rev 10/23)