First National Bank of Waynesboro, building customer awareness... Internet Banking Security Tips

The Internet has made it easier for criminals to deceive individuals into revealing confidential information and clicking on links or attachments that will compromise the security of their computers which ultimately have an impact on Internet banking security. These criminals have continued to use increasingly sophisticated, effective, and malicious methods to fraudulently gain unauthorized access to consumers' Internet banking accounts.

At First National Bank we understand that security measures are a top priority and of utmost importance for Internet banking. First National has implemented a significant level of security features to mitigate the risk of fraudulent Internet activity however we strongly encourage both our consumer and business customers using Internet banking services to be aware of current threats to the security of their Internet banking accounts, and to implement internal preventative and monitoring controls to reduce the risk of compromised access and account takeover.

First National is required under Regulation E: Electronic Fund Transfers to provide certain protections to our customers relative to electronic fund transfers (EFT). As applicable to Internet access, this regulation covers transactions initiated through First National's Internet banking and cash management channels, to either order, instruct, or authorize the financial institution to debit or credit an account. Transactions may include but are not limited to ACH payments, external transfers, and bill payments. For specific applicability and provisions, please refer First National's EFT disclosure which is located on the back of this notification.

First National will NEVER request a customer's personal information (debit card number, account number, social security number, personal identification number or password) through email or by phone. If you ever receive an unsolicited phone call or email claiming to be from First National requesting your personal and confidential information, please DO NOT respond. Contact us immediately by calling (706) 554-8100. As an additional monitoring control, you should review account statements and online account transaction history to ensure all transactions are correct and authorized.

Fraudsters will commonly use a type of Internet piracy called "phishing." In a typical Phishing case, you'll receive an e-mail that appears to be from First National. In some cases, the e-mail may appear to come from a government agency, including the FDIC. The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the Bank's web site. In a phishing scam, you could be redirected to a fictitious web site that may look exactly like the Bank's site. In other situations, it may be the Bank's actual web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your login authentication credentials. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth. If you provide the requested information, you may find yourself the victim of identity theft which can lead to malicious activity such as Internet banking account takeover.

First National is required through its banking regulators to conduct regular periodic risk assessments of their electronic banking products and services to identify security threats, and controls in place related to internal and external security, changes in customer functionality offered through electronic banking, and actual incidents of security breaches, ID theft, or fraud experienced internally or within the industry. As a proactive measure, we strongly suggest to our business or commercial customers to also perform a periodic risk assessment and controls evaluation related to security of their Internet banking / cash management environment. Special attention should be directed to high risk transactions which involve access to personal financial information or the movement of funds to other parties such as ACH, wire transfers, and bill payment.

First National has implemented strong preventative and monitoring controls within its Internet banking and bill payment system however in order to enhance our customer's internal security we recommend our customers implement their own controls to mitigate risks. Examples of controls you may want to consider implementing to mitigate the risks of account takeover and fraudulent account activities are as follows:

• Maintain up-to-date operating system security patches and have installed updated virus/spyware protection software. Viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus and anti-spyware software will help to keep your computer safe from malicious software that could install itself or may try to install itself on your computer.

• Install a Firewall, either software or hardware. A firewall will prevent attacks on your computer through the Internet using established rules to determine if a requested connection is malicious or not.

• Implement intrusion detection/prevention software or services

• Safekeeping and confidentiality of Internet banking authentication credentials

• For business customers, implement dual control for initiating and approving high risk Cash Management transactions such as ACH origination and wire transfers

• Daily account activity monitoring via Internet banking account transaction history review

• Review and monitor your checking account, debit card, and credit card statements for unauthorized transactions.

• Refrain from opening unsolicited email and attachments

• Refrain from providing authentication credentials to callers claiming to be representing the financial institution and from responding to emails requesting information or re-directing you to a website.

• Prior to disposing, shred all confidential information on hardcopy and on electronic media.

If you notice any suspicious or unauthorized account activity, experience a breach in security of personal information, your login credentials or computer security have been compromised, or for more information please contact Lynn Meeks at bookkeeping@fnbwaynesboro.com or call (706) 554-8100.

MEMBER FDIC

ELECTRONIC FUND TRANSFERS
YOUR RIGHTS AND RESPONSIBILITIES

Indicated below are types of Electronic Fund Transfers we are capable of handling, some of which may not apply to your account. Please read this disclosure carefully because it tells you your rights and obligations for the transactions listed. You should keep this notice for future reference.

Electronic Fund Transfers Initiated By Third Parties. You may authorize a third party to initiate electronic fund transfers between your account and the third party's account. These transfers to make or receive payment may be one-time occurrences or may recur as directed by you. These transfers may use the Automated Clearing House (ACH) or other payments network. Your authorization to the third party to make these transfers can occur in a number of ways. For example, your authorization to convert a check to an electronic fund transfer or to electronically pay a returned check charge can occur when a merchant provides you with notice and you go forward with the transaction (typically, at the point of purchase, a merchant will post a sign and print the notice on a receipt). In all cases, these third party transfers will require you to provide the third party with your account number and bank information. This information can be found on your check as well as on a deposit or withdrawal slip. Thus, you should only provide your bank and account information (whether over the phone, the Internet, or via some other method) to trusted third parties whom you have authorized to initiate these electronic fund transfers. Examples of these transfers include, but are not limited to:

- **Preauthorized credits.** You may make arrangements for certain direct deposits to be accepted into your checking or savings account(s).
- **Preauthorized payments.** You may make arrangements to pay certain recurring bills from your checking or money market account(s).
- **Electronic check conversion.** You may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills.
- **Electronic returned check charge.** You may authorize a merchant or other payee to initiate an electronic funds transfer to collect a charge in the event a check is returned for insufficient funds.

First Connection Telephone Transfers - types of transfers - You may access your account by telephone 24 hours a day at (706) 437-9300 using a touch tone phone, your account numbers and your password, to:

- transfer funds between checking and savings
- make payments from checking or savings to loan accounts with us
- stop payment on a check
- get information about:
  - the account balance of checking or savings accounts

ATM Transfers - types of transfers and dollar limitations - You may access your account(s) by ATM using your ATM card and personal identification number or debit card and personal identification number, to:

- make deposits to checking or savings account(s)
- get cash withdrawals from checking or savings account(s)
  - you may withdraw no more than $500.00 per day with an ATM card or non-photo debit card
  - you may withdraw no more than $750.00 per day with a photo debit card
- transfer funds from savings to checking account(s)
- transfer funds from checking to savings account(s)
- get information about:
  - the account balance of checking or savings account(s)

Some of these services may not be available at all terminals.

Types of Debit Card Point-of-Sale Transactions - You may access your checking account(s) to purchase goods (in person, online, or by phone), pay for services (in person, online, or by phone), get cash from a merchant, if the merchant permits, or from a participating financial institution, and do anything that a participating merchant will accept.

Point-of-Sale Transactions - dollar limitations and charges - Using your card:

- you may make no more than 20 transactions per day
- you may not exceed $750.00 in transactions per day with a non-photo debit card
- you may not exceed $1,500.00 in transactions per day with a photo debit card

Currency Conversion. When you use your Visa®-branded Debit Card at a merchant that settles in currency other than US dollars, the charge will be converted into the US dollar amount. The currency conversion rate used to determine the transaction amount in US dollars is either a rate selected by Visa from the range of rates available in wholesale currency markets for the applicable central processing date, which rate may vary from the rate Visa itself receives, or the government-mandated rate in effect for the applicable central processing date. The conversion rate in effect on the processing date may differ from the rate in effect on the transaction date or posting date.

Advisory Against Illegal Use. You agree not to use your card(s) for illegal gambling or other illegal purpose. Display of a payment card. logo by, for example, an online merchant does not necessarily mean that transactions are lawful in all jurisdictions in which the cardholder may be located.

Non-Visa Debit Transaction Processing. We have enabled non-Visa debit transaction processing. This means you may use your Visa-branded debit card on a PIN-Debit Network* (a non-Visa network) without using a PIN.

The non-Visa debit network(s) for which such transactions are enabled are: STAR Network.

Examples of the types of actions that you may be required to make to initiate a Visa transaction on your Visa-branded debit card include signing a receipt, providing a card number over the phone or via the Internet, or swiping the card through a point-of-sale terminal.

Examples of the types of actions you may be required to make to initiate a transaction on a PIN-Debit Network include initiating a payment directly with the biller (possibly via telephone, Internet, or kiosk locations), responding to a logo displayed at a payment site and choosing to direct payment through that network, and having your identity verified using known information derived from an existing relationship with you instead of through use of a PIN.

The provisions of your agreement with us relating only to Visa transactions are not applicable to non-Visa transactions. For example, the additional limits on liability (sometimes referred to as Visa's zero-liability program) and the streamlined error resolution procedures offered on Visa debit card transactions are not applicable to transactions processed on a PIN-Debit Network.

*Visa Rules generally define *PIN-Debit Network* as a non-Visa debit network that typically authenticates transactions by use of a personal identification number (PIN) but that is not generally known for having a card program.

FNBanking Online

You may access your FNB account(s) by computer using your user identification, your password, and internet access at www.fnbwaynesboro.com to:

- Transfer funds from one of your FNB deposit accounts to another FNB deposit accounts, excluding certificates of deposits.
- Make payments from your FNB checking or FNB savings account to your loan accounts with us.
- Request stop payments on checks drawn on your FNB accounts.
- Get information about:
  - the available balance for all of your FNB accounts
  - for all of your FNB deposit accounts, all transactions information relating to transactions for the current month and previous month.

FEES

- We do not charge for direct deposits to any type of account.
- We will charge you $5.00 to issue a photo debit card.
- We will charge you $1.00 for a replacement debit card or $7.00 for a replacement photo debit card.

Payments Issued through FNBill Pay that are insufficient will be charged an additional $20.00 each.

Except as indicated elsewhere, we do not charge for these electronic fund transfers.

ATM Operator/Network Fees. When you use an ATM not owned by us, you may be charged a fee by the ATM operator or any network used (and you may be charged a fee for a balance inquiry even if you do not complete a fund transfer).

DOCUMENTATION

- **Terminal transfers.** You can get a receipt at the time you make a transfer to or from your account using an automated teller machine or point-of-sale terminal. However, you may not get a receipt if the amount of the transfer is $15 or less.
- **Preauthorized credits.** If you have arranged to have direct deposits made to your account at least once every 60 days from the same person or company, you can call us at (706) 554-8100 to find out whether or not the deposit has been made.
- **Periodic statements.**

  You will get a monthly account statement from us for your checking and money market accounts.

  You will get a monthly account statement from us for your savings accounts, unless there are no transfers in a particular month. In any case, you will get a statement at least quarterly.

PREAUTHORIZED PAYMENTS

- **Right to stop payment and procedure for doing so.** If you have told us in advance to make regular payments out of your account, you can stop any of these payments. Here is how:

  Call or write us at the telephone number or address listed in this brochure in time for us to receive your request 3 business days or more before the payment is scheduled to be made. If you call, we may also require you to put your request in writing and get it to us within 14 days after you call.

  We will charge you $26.00 for each stop-payment order you give.
- **Notice of varying amounts.** If these regular payments may vary in amount, the person you are going to pay will tell you, 10 days before each payment, when it will be made and how much it will be. (You may choose instead to get this notice only when the payment would differ by more than a certain amount from the previous payment, or when the amount would fall outside certain limits that you set.)
- **Liability for failure to stop payment of preauthorized transfer.** If you order us to stop one of these payments 3 business days or more before the transfer is scheduled, and we do not do so, we will be liable for your losses or damages.

FINANCIAL INSTITUTION'S LIABILITY

Liability for failure to make transfers. If we do not complete a transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will not be liable, for instance:

(1) If, through no fault of ours, you do not have enough money in your account to make the transfer.
(2) If you have an overdraft line and the transfer would go over the credit limit.
(3) If the automated teller machine where you are making the transfer does not have enough cash.
(4) If the terminal or system was not working properly and you knew about the breakdown when you started the transfer.
(5) If circumstances beyond our control (such as fire or flood) prevent the transfer, despite reasonable precautions that we have taken.
(6) There may be other exceptions stated in our agreement with you.

CONFIDENTIALITY

We will disclose information to third parties about your account or the transfers you make:

(1) where it is necessary for completing transfers; or
(2) in order to verify the existence and condition of your account for a third party, such as a credit bureau or merchant; or
(3) in order to comply with government agency or court orders; or
(4) as explained in the separate Privacy Disclosure.

UNAUTHORIZED TRANSFERS

(a) Consumer liability.

◆ *Generally.* Tell us AT ONCE if you believe your card and/or code has been lost or stolen, or if you believe that an electronic fund transfer has been made without your permission using information from your check. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account (plus your maximum overdraft line of credit). If you tell us within 2 business days after you learn of the loss or theft of your card and/or code, you can lose no more than $50 if someone used your card and/or code without your permission.

If you do NOT tell us within 2 business days after you learn of the loss or theft of your card and/or code, and we can prove we could have stopped someone from using your card and/or code without your permission if you had told us, you could lose as much as $500.

Also, if your statement shows transfers that you did not make, including those made by card, code or other means, tell us at once. If you do not tell us within 60 days after the statement was mailed to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time.

If a good reason (such as a long trip or a hospital stay) kept you from telling us, we will extend the time periods.

◆ *Additional Limit on Liability for Visa®-branded Debit Card.* Unless you have been grossly negligent or have engaged in fraud, you will not be liable for any unauthorized transactions using your lost or stolen Visa®-branded Debit Card. This additional limit on liability does not apply to ATM transactions or to transactions using your Personal Identification Number which are not processed by VISA®.

(b) Contact in event of unauthorized transfer. If you believe your card and/or code has been lost or stolen, call or write us at the telephone number or address listed in this brochure. You should also call the number or write to the address listed in this brochure if you believe a transfer has been made using the information from your check without your permission.

ERROR RESOLUTION NOTICE

In Case of Errors or Questions About Your Electronic Transfers, Call or Write us at the telephone number or address listed in this brochure, as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared.

(1) Tell us your name and account number (if any).
(2) Describe the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information.
(3) Tell us the dollar amount of the suspected error.

If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days (5 business days for Visa®-branded Debit Card point-of-sale transactions processed by Visa and 20 business days if the transfer involved a new account) after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days (90 days if the transfer involved a new account, a point-of-sale transaction, or a foreign-initiated transfer) to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days (5 business days for Visa®-branded Debit Card point-of-sale transactions processed by Visa and 20 business days if the transfer involved a new account) for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account. Your account is considered a new account for the first 30 days after the first deposit is made, unless each of you already has an established account with us before this account is opened.

We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation.

You may ask for copies of the documents that we used in our investigation.

FIRST NATIONAL BANK OF WAYNESBORO
BOOKKEEPING
P. O. BOX 647
WAYNESBORO, GEORGIA 30830
Business Days: Monday through Friday
Excluding Federal Holidays
Phone: (706) 554-8100

MORE DETAILED INFORMATION IS AVAILABLE ON REQUEST

NOTICE OF ATM/NIGHT DEPOSIT FACILITY USER PRECAUTIONS

As with all financial transactions, please exercise discretion when using an automated teller machine (ATM) or night deposit facility. For your own safety, be careful. The following suggestions may be helpful.

1. Prepare for your transactions at home (for instance, by filling out a deposit slip) to minimize your time at the ATM or night deposit facility.
2. Mark each transaction in your account record, but not while at the ATM or night deposit facility. Always save your ATM receipts. Don't leave them at the ATM or night deposit facility because they may contain important account information.
3. Compare your records with the account statements you receive.
4. Don't lend your ATM card to anyone.
5. Remember, do not leave your card at the ATM. Do not leave any documents at a night deposit facility.
6. Protect the secrecy of your Personal Identification Number (PIN). Protect your ATM card as though it were cash. Don't tell anyone your PIN. Don't give anyone information regarding your ATM card or PIN over the telephone. Never enter your PIN in any ATM that does not look genuine, has been modified, has a suspicious device attached, or is operating in a suspicious manner. Don't write your PIN where it can be discovered. For example, don't keep a note of your PIN in your wallet or purse.
7. Prevent others from seeing you enter your PIN by using your body to shield their view.
8. If you lose your ATM card or if it is stolen, promptly notify us. You should consult the other disclosures you have received about electronic fund transfers for additional information about what to do if your card is lost or stolen.
9. When you make a transaction, be aware of your surroundings. Look out for suspicious activity near the ATM or night deposit facility, particularly if it is after sunset. At night, be sure that the facility (including the parking area and walkways) is well lighted. Consider having someone accompany you when you use the facility, especially after sunset. If you observe any problem, go to another ATM or night deposit facility.
10. Don't accept assistance from anyone you don't know when using an ATM or night deposit facility.
11. If you notice anything suspicious or if any other problem arises after you have begun an ATM transaction, you may want to cancel the transaction, pocket your card and leave. You might consider using another ATM or coming back later.
12. Don't display your cash; pocket it as soon as the ATM transaction is completed and count the cash later when you are in the safety of your own car, home, or other secure surrounding.
13. At a drive-up facility, make sure all the car doors are locked and all of the windows are rolled up, except the driver's window. Keep the engine running and remain alert to your surroundings.
14. We want the ATM and night deposit facility to be safe and convenient for you. Therefore, please tell us if you know of any problem with a facility. For instance, let us know if a light is not working or there is any damage to a facility. Please report any suspicious activity or crimes to both the operator of the facility and the local law enforcement officials immediately.