

During the past year the banking industry has seen significant changes regarding threats to online banking. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Bank of McCrory is providing the below security awareness information for your use and action to help protect your online account and transaction information.

## ***Protections and Liabilities for Consumer Transactions using Bank of McCrory Online Banking***

To access our Online Banking service, you must use the ID you provided Bank of McCrory, select your Personal Image, and provide your Password. If you are not on a computer that you have defined as trusted, you will be asked to answer one of your Challenge Questions. It is YOUR responsibility to safeguard the ID, Personal Image, Challenge Questions & Answers, and Password. Anyone to whom you give your Online Banking authentication information, will have FULL access to your accounts, even if you attempt to limit that person's authority.

You, or someone you have authorized [by giving them your Online Banking authentication information], can instruct us to perform the following transactions:

- Make transfers between your qualifying accounts to the extent authorized;
- Obtain information that we make available about your qualifying accounts;
- Obtain other services or perform other transactions that we authorize.

You must have enough money or credit in any account from which you instruct us to make a payment or transfer. You also agree to the Terms & Conditions of your deposit account that you received when you opened your deposit account.

## ***Statements***

Your Online Banking payments and transfers will be indicated on the monthly or quarterly statements we provide. Please notify us promptly if you change your address or if you believe there are any errors or unauthorized transactions on any statement, or statement information.

## ***Unauthorized Transactions or Loss/Theft of Your Online Banking Authentication Information***

If you believe your Online Banking authentication information has been lost or stolen, call us

immediately at 870-731-2521, during normal business hours. After hours you may e-mail us at [info@bankofmccrory.com](mailto:info@bankofmccrory.com) or write us at Bank of McCrory, P. O. Box 370, McCrory, AR, 72101. Immediately contacting us by phone is the best way of reducing your possible losses, since not all e-mail may arrive at their destinations. We will send an e-mail back to you as confirmation that we did receive it. Because e-mail is not secure, do not include any of your account or social security numbers with your e-mail. Your name, address, and a brief message as to what the problem might be is all we will need. If you have given someone your Online Banking authentication information and want to terminate that person's authority, you should change your password and/or other means of access, to prevent further access by that person.

You may terminate your Online Banking Agreement at any time upon giving the Bank written notice of the termination. If you terminate, you authorize us to continue making transfers you have previously authorized until we have had a reasonable opportunity to act upon your termination notice. Once we have acted upon your termination notice, we will make no further transfers or payments from your Online Banking account. If we terminate your use of your Online Banking account, we reserve the right to make no further transfers of payments from your account including any transactions you have previously authorized.

YOU are responsible for all transfers authorized using the Online Banking services under this Agreement. If you permit other persons to use your authentication information, you are responsible for any transactions they authorize or conduct on any of your accounts. However, tell us at once if you believe anyone has used your authentication information and accessed your accounts without your authority. Telephoning is the best way of keeping your possible losses down.

For Online Banking transactions, if you tell us within 2 business days, you can lose no more than \$50 if someone accessed your account without your permission. If you do not tell us within 2 business days after you learn of the unauthorized use of your account, and we can prove that we could have prevented the unauthorized transaction if you had told us in time, you could lose as much as \$500 or more. Your liability for unauthorized loan transactions through the Online Banking service will not exceed \$50.

Also, if your statement shows Online Banking transfers that you did not make, tell us at once. If you do not tell us within sixty (60) days of the mailing date of your statement, you may be liable for the full amount of the loss if we can prove that we could have prevented the unauthorized transactions if you had told us in time. Should some emergency such as extended travel or hospitalization prevent you from contacting us, a reasonable extension of time will be allowed.

### ***Limitation of Liability for Online Banking Services***

If we do not complete a transfer to or from your consumer account on time or in the correct

amount according to our agreement with you, we will be liable and used primarily for personal, family, or household purposes.) Our sole responsibility for an error in a transfer will be to correct the error. You agree that neither we nor the service providers shall be responsible for any loss, property damage or loss, whether caused by the equipment, software, Bank of McCrory, or by Online browser providers such as Netscape (Netscape Navigator browser) and Microsoft (Microsoft Internet Explorer browser), or by Internet access providers or by online service providers or by an agent or subcontractor of any of the foregoing. Neither we nor the service providers will be responsible for any direct, indirect, special or consequential economic or other damages arising in any way out of the installation, download, use, or maintenance of the equipment, software, the Bank of McCrory Online Banking services or Internet Browser or access software. In this regard, although we have taken measures to provide security for communications from you to us via the Bank of McCrory Online Banking Services and may have referred to such communication as "secured," we cannot and do not provide any warranty or guarantee of such security. In states that do not allow the exclusions or limitation of such damages, our liability is limited to the extent permitted by applicable law.

Additionally, Bank of McCrory will NOT be liable for the following:

- a. If, through no fault of ours, you do not have enough money in your account to complete a transaction, your account is inactive or closed, or the transaction amount would exceed the credit limit on your line of credit.
- b. If you used the wrong authentication information or you have not properly followed any applicable computer, Internet, or Bank of McCrory user instructions for making transfer and bill payment transactions.
- c. If your computer fails or malfunctions or the Online Banking service was not properly working and such problem was or should have been apparent when you attempted such transaction.
- d. If, through no fault of ours, a bill payment or funds transfer transaction does not reach a particular creditor and a fee, penalty, or interest is assessed against you.
- e. If circumstances beyond our control (such as fire, flood, telecommunications outages or strikes, equipment or power failure) prevent the transaction.
- f. If the funds in your account are subject to legal process or other claim, or if your account is frozen because of a delinquent loan, overdrawn account, or suspected fraud.
- g. If the error was caused by a system beyond the Bank of McCrory's control such as a telecommunications system, or Internet service provider.
- h. If you have not given the Bank of McCrory complete, correct, or current information so Bank of McCrory can process a transaction.

## ***Billing Errors***

In case of errors or questions about your Online Banking transactions, telephone us at the phone numbers or write us at the address set forth above as soon as you can. We must hear from you no later than sixty (60) days after we sent the first statement on which the problem appears.

- a. Tell us your name and account number.
- b. Describe the transaction you are unsure about, including the transaction confirmation or reference number if applicable, and explain as clearly as you can why you believe it is an error or why you need more information.
- c. Tell us the dollar amount of the suspected error.

## ***Consumer Accounts***

**(an account belonging to a natural person and used primarily for personal, family, or household purposes)**

If you tell us orally, we may require that you send us your complaint or question in writing within ten (10) business days. We will tell you the results of our investigation within ten (10) business days after we hear from you and will correct any error promptly. For errors related to transactions occurring within thirty (30) days after the first deposit to the account (new accounts), we will tell you the results of our investigation within twenty (20) business days. If we need more time, however, we may take up to forty-five (45) days to investigate your complaint or question (ninety (90) calendar days for new account transaction errors, or errors involving transactions initiated outside the United States). If we decide to do this, we will re-credit your account within ten (10) business days 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 ten (10) business days, we may not re-credit your account.

If we decide after our investigation that an error did not occur, we will deliver or mail to you an explanation of our findings within three (3) business days after the conclusion of our investigation. If you request, we will provide you copies of documents (to the extent possible without violating other members' rights to privacy) relied upon to conclude that the error did not occur.

## ***Precautions You Should Take***

- **Bank of McCrory will never** contact any customer and request electronic banking credentials. If you get a call asking for your credentials, hang up and call us!
- **If you are a Bank of McCrory commercial online banking customer:** we suggest you periodically evaluate the possible risks to your account. Some key areas to check are:

- Who has access to the online banking PC and credentials?
- Is (Are) the online banking PC or PCs secured after normal business hours?
- Do you have up to date antivirus and antimalware software on the PC?
- How often do you change the online banking password and who knows the password?
- Is there a firewall active on your PC?
- **Block cookies on your Web browser:** When you surf, hundreds of data points are being collected by the sites you visit. These data get mashed together to form an integral part of your “digital profile,” which is then sold without your consent to companies around the world. By blocking cookies, you’ll prevent some of the data collection about you. Yes, you’ll have to enter passwords more often, but it’s a smarter way to surf.
- **Don’t put your full birth date on your social-networking profiles:** Identity thieves use birth dates as cornerstones of their craft. If you want your friends to know your birthday, try just the month and day, and leave off the year.
- **Don’t download Facebook apps from outside the United States:** Apps on social networks can access huge amounts of personal information. Some unscrupulous or careless entities collect lots of data and then lose, abuse, or sell them. If the app maker is in the U.S., it’s probably safer, and at least you have recourse if something should ever go wrong.
- **Use multiple usernames and passwords:** Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate. Having distinct passwords is not enough nowadays: if you have the same username across different Web sites, your entire romantic, personal, professional, and e-commerce life can be mapped and re-created with some simple algorithms. It’s happened before.
- **Online Banking Problems, Concerns, or Something doesn’t look right?** Call us at 870-731-2521.