INFORMATION SECURITY TIPS for SAFE ONLINE BANKING

Here are some ways that can help safeguard your personal and financial information

KEEP PERSONAL INFORMATION PRIVATE

- Be cautious when sharing personal information, such as your social security number (SSN).
- Do not share personal information over the phone or online unless you have initiated the contact. US Metro Bank will never initiate an email, link, text message or phone call and ask you to reveal any private information, including your account information.
- Memorize your personal identification number such as your ATM PIN including your Online Banking User ID and Password.
- Do not write or keep your PIN in an easily found place, such as on your card, or in your purse or wallet.

PROTECT YOUR COMPUTER

- Make sure every computer you own has up to date software installed including operating system, personal firewall, anti-virus, anti-spyware and current browser. Be cautious of "fee" antivirus software offers and get your software from reputable companies.
- Regularly back up your computer files to media you can store elsewhere, such as CD's, thumb dives or external USB hard drives. Store these back up file in a secure place.

NAVIGATE ONLINE BANKING SAFELY

- Verify your Online Banking session is secure:
  - A closed, or locked, padlock, usually located in the lower right corner of your browser window, indicates a secure connection.
  - Look for "https://" at the beginning of the Web Site address or URL in your Web browser. The "s" means secure.
- Create a strong password for online accounts:
  - Use a combination of numbers, letters, and special characters.
  - Pick a password at least 8 characters or longer.
  - Change your password every 90 days.
  - Do not use your online password as the password for other websites, including your email.
- Use the "Sign Off" feature when you're done using Online Banking or when you are away from your computer for an extended period of time. Close your browser to prevent others from using your session.

BE CAUTIONS WITH EMAIL AND DOWNLOADS

- Be aware of email scams and phony websites. Use a critical eye and feel free to contact us if you have a question about something that appears to be from the Bank.
- Learn as much as possible about anything you're downloading to your computer, including email attachments. Programs from unknown sources can compromise the security of your computer.
- Follow these guidelines to decide whether or not to open and read an email message:
  - Do you know the person who emailed you?
  - Has this person emailed you before?
  - Does the subject line make sense?
  - Did you expect to receive an attachment from this person?
  - Does the message harbor a virus? Use an anti-virus program to verify that it does not.
- Do not send personal and financial information over the Internet via email, as it is typically not secure and could be intercepted.

SAFEGUARD YOUR ACCOUNT

- Shred financial documents, including old bank statements and invoices that you no longer need.
- Store new and cancelled checks in a secure place.
- Keep records of your financial transactions.
- Do not write your account number on items that may be thrown away later.

SAFEGUARD YOUR ACCOUNT

- Send mail from a post office or secured mailbox, rather than from your home mailbox.
- Collect incoming mail promptly.
- Shred all unwanted pre-approved offers for financial products and services, like credit cards or loans.

If you have any questions regarding security of your US Metro Bank accounts, please contact us at 714-620-8888

Member FDIC

EQUAL HOUSING LENDER