Identity Theft and Fraud Prevention

Steps You Can Take to Project Yourself.
You can protect yourself and your accounts by recognizing and preparing for fraud and online banking threats. Anyone can fall prey to fraud and identity theft. Below are some tips on ways to minimize your risk.

- Before you sign into websites where you are entering personal or financial information make sure the website displays a secure lock icon has https in the URL address. (https://www.floridacapitalbank.com)
- Check all personal and business accounts frequently. Review financial accounts and statements regularly for charges you did not make.
- Inspect your credit report and financial statements. Credit reports contain information about you, including what accounts you have and your bill paying history.
- Be alert and take immediate action when:
  - Your bills do not arrive as expected
  - You receive unexpected credit card or account statements
  - You receive unexpected denials of credit when you have not applied for credit
  - You receive calls or letters about purchases you did not make.
- Keep your account information up-to-date. Be sure to notify us as soon as possible about any changes to identifiable information we may need to verify account information.
- Don't give your account numbers or any personal or financial information over the phone, through email, through mail, or over the Internet unless you initiate the conversation and you know the person or organization.
- Don't print your driver's license, phone or Social Security number on your checks.
- Report lost or stolen checks immediately and we'll stop payment on the check numbers you report. When you receive new checks, look through them to make sure all check numbers are accounted for.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write you Social Security number on a check. Give it out if only absolutely necessary.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done to your house. At work, make sure to lock up all confidential information in a filing cabinet before you leave the office.
- Store your new and canceled checks in a safe place.
- Call us right away if you receive any suspicious phone inquiries asking for your account information, or if you see anything suspicious in your account activity or on your statement.
- Shred financial documents and paperwork with personal information before you discard or store financial information securely (including bank statements, invoices, ATM and credit card receipts).
- Guard your PINs and passwords (Don't store them on your phone or write them on your card).
- Use a unique username and password for Online Banking that you never use anywhere else, i.e., webmail, social networking or any other online accounts. If hackers get the password for one of your online accounts, they will often try to use it to access other accounts.
- Be careful when you use your device in public areas. If you use flcb.com or one of our apps in public or on a public or shared computer, make sure you sign out when you're done, and delete all cookies.
- Keep your computer operating system, internet browser, and other software up to date. These updates often address security concerns. The same is true for cell phones and cell phone applications.

- Configure any new device with security in mind. Be sure to change default passwords, and beware that default settings are often intended more for an ease of use than to secure the device. Enable security settings that are made available and give extra consideration to those that control information sharing.
- Educate yourself about Identity Theft and other signs of fraud

For Business Banking Customers

Safeguard your business

If you own a business, it's important to:

- Maintain appropriate internal controls, including separation of duties. For example, be sure that the people who reconcile accounts are different than the people who make payments.
- Perform regular risk assessments and evaluate your internal controls to determine any potential exposure you may have related to online banking activities with a focus on “high risk” transactions, like wires.
- Periodically review your users and the permissions you give them. Your system administrator can establish user permissions and online transaction limits for each of your users.
- Regularly check your transactions and statements for any unauthorized activity.
- Take advantage of our online **Positive Pay Service** to help you monitor and control checks clearing against your accounts.
- Customize your Account Alerts so you’ll get notified when certain account activity takes place.

Maintain accurate account information

Keeping your account information up-to-date is very important in protecting yourself against fraud and helping us when we need to use identifiable information to verify account information. If you need to update your information or if you believe that our information about you is incomplete, out-of-date, or incorrect, you may review or update certain account information by logging into your account online. If you cannot change the incorrect information online, or you prefer to request changes offline, please contact your branch or Business Relationship Banker, or call our customer service center at 1-800-318-3159, and they will be able to help you

Set-up free Account Alerts

We're always looking for ways to help you keep your accounts safe. Free Account Alerts are a great way to keep track of your finances to detect withdrawals you didn’t authorize or other suspicious account activity. You can sign up to get all types of alerts by text, phone or email.

Get paperless statements

Paperless statements are an easy way to stay clutter-free and avoid losing statements in the mail. If you sign-up to go paperless, you’ll get an email alerting you that a new statement is available online. You can see these statements anytime, from virtually anywhere, when you log into online banking.

Card Controls

Prevent fraud and control spending on your Debit Card with our Card Valet service. Protect your business card through your mobile device by receiving alerts and defining when, where and how your payment cards are used - with CardValet®. Payment cards offer convenience and risk prevention. CardValet manages the risk by allowing you to define when, where, and how your cards can be used.

Review your credit reports
At least once a year, read through your credit reports carefully. Look out for credit inquiries from unfamiliar companies, accounts you never opened and unexplained debts. This can be a warning sign of fraud or identity theft.

You can request a free annual credit report from each of the 3 national credit reporting agencies, even if you don't suspect any unauthorized activity on your account. You can request all three reports at once or you can order one report at a time.

You can request and review your free report through one of the following ways:

- **Online**: Visit AnnualCreditReport.com
- **Phone**: Call (877) 322-8228
- **Mail**: Download and complete the Annual Credit Report Request form. Mail the completed form to:
  Annual Credit Report Request Service
  P.O. Box 105281
  Atlanta, GA 30348-5281

Effective Passwords

Your identity is one of your most valuable resources. We recommend you help safeguard your identity and personal information by using effective password protection. Here are some suggestions for creating safer passwords and some cautions against weaker ones.

Tips for choosing more-secure passwords:

- Create original passwords that contain a combination of letters, numbers, and even special characters (#, &, %) if allowed
- Use both capital and lowercase letters (if your password can be case sensitive)
- Ensure your passwords are at least eight characters
- Use a unique password for each service. Avoid using:
  - Your Social Security number
  - Account numbers
  - Phone numbers or addresses
  - Birth dates or anniversaries
  - Obvious or common nicknames
  - Names of relatives or pets
  - Common words from the dictionary
- Choose a password you can easily remember, so you don't have to write it down
- Avoid using software that saves or remembers your passwords
- Change your passwords at least twice a year

Protect and update your equipment
Install anti-virus and firewall software on your computer and keep it up to date. Be cautious about offers for free anti-virus software; make sure you get your software from a reputable company. Look for anti-virus software that scans incoming communications and files for viruses, removes or quarantines viruses and updates automatically.

A firewall is software or hardware designed to block unauthorized access to your computer. It's especially important to run a firewall if you have a cable modem or DSL line or other broadband connection, because they're often targeted. Many current operating systems come with a built-in firewall, which you have to turn on.

Mobile Device Security
Configure your mobile device to require a passcode to gain access and with auto lock features. Avoid storing sensitive information. Mobile devices have a high likelihood of being lost or stolen so you should avoid using them to store sensitive information such as passwords, and bank account numbers. If sensitive data is stored then encryption should be used to secure it.

To prevent unauthorized access to your mobile device, configure your settings to have the device locked after a set number of failed passcode attempts. Consider installing security software to prevent malware from infecting your mobile device.

Report fraud immediately
Contact us immediately if you think your FLCBank account has been put in jeopardy. The sooner we know what has happened, the sooner we can begin helping you. Please call your **Business Relationship Banker or contact a Relationship Banker at one of our branches at 1-800-318-3159.**

If you have disclosed sensitive information to a fraudster, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name.

- Equifax: 1.888.766.0008
- Experian: 1.888.397.3742
- TransUnion: 800.680.7289

If it sounds too good to be true, it probably is.
If you have become a victim of identity theft, immediately take the following actions

- Contact your banker.
- Notify anyone with whom you have a financial relationship.
- File a police report.
- Request accounts to be tagged “closed due to fraud”
- Notify credit bureau fraud units.
- Establish new passwords for inquiries on credit card accounts.
- Place a fraud alert statement on your credit report.
- Request bi-monthly copies of your credit report until your case is resolved (Free to fraud victims)
- Report check theft to check verification companies.
- Check the post office for unauthorized change of address requests.
- Follow-up contacts with letters and keep copies of all correspondence.

What is Identity Theft

Identity theft occurs when someone uses your identity or personal information—such as your name, your driver's license, or your Social Security number—without your permission to commit a crime or fraud. There are many different types of identity theft that can occur as criminals are always looking for new ways to exploit consumer information.

How Identity can be Compromised?

Your identity and personal information is always at risk and can be stolen long before you realize you're a victim. In most cases of identity theft, you don't find out you are a victim until you review your credit card statement or receive notices in the mail about new accounts you didn't open, charges you didn't make, or until you're contacted by a debt collector.

Here are some common ways identity theft happens:

- **Dumpster Diving**. Thieves rummage through your trash to find bills, credit card offers, and other paperwork with personal information on it.
- **Skimming**. Thieves steal credit and debit card numbers by affixing special storage devices on ATMs and gas pumps. Inspect all card readers before using them.
- **Phishing**. Thieves pretend to be financial institutions or companies and send spam or pop-up messages linking to fraudulent sites that ask for personal information.
- **Changing your address**. Thieves can divert your mailed statements to another location by completing a "change of address" form. FLCBank and other companies request customers to switch to electronic billing to help prevent this.
- **"Old-Fashioned" stealing**. Thieves steal phones, wallets and purses; mail; pre-approved credit card offers; checks and tax information.

Learn how to protect yourself from identity theft and fraud with some of our tips or through the resources below.

- FTC ID Theft Website
- FDIC ID Theft and Fraud Information
- Internet Crime Complaint Center

Different Types of Identity Theft and Fraud

Phishing

Email, phone and text messages are all popular places for scams. Fraudsters can spoof a sender's email address or phone number to appear to be from someone you trust.

Phishing is when an imposter tries to trick you into providing your personal information. They might impersonate a trustworthy entity, such as a bank, insurance company, retailer, or regulatory agency, in an email, phone call or text, asking you to confirm your information or saying you've won something—and it might look legitimate.

Don't open an email attachment, even if it appears to be from a friend or co-worker, unless you're expecting it or you're absolutely sure you know what it contains. Watch out for email subject lines or emails with a generic message like "check this out" or "thought you'd be interested in this." Make sure you know who sent the email before you open an attachment or click any links.

Beware of any unsolicited emails that request personal information of any kind. Do not respond to any such emails, texts, instant messages, pop-ups, or links.

The following tips will help you spot fraudulent messages:

- The email appears to be from a reputable company you know or do business with and asks you to reply or go to a website that looks familiar, where you'll be asked to give your username, password, account number, personal identification number (PIN), Social Security number or other personal information; some may use pop-up windows to ask for confidential information.
- The message title tries to create a feeling of urgency or general concern that requires your immediate attention; threatens to close or suspend your account if you don't take immediate action.
- The sender's name is usually generic, such as "Customer Service Department," or is just the company's name, such as "ABC Bank.
- The message may look professional and official, often displaying the look and feel of a website that you know, giving the appearance of legitimacy, but there are misspelled words or sentence structure that doesn't read correctly.
- The email address it came from or the one to reply to doesn't have the company's standard email domain identifier after the @ symbol.
- The message may point you to a domain name that is spelled very close to or appears to be related to the legitimate domain name.
- The message may point you to a web page that isn't protected by Secure Socket Layer (SSL), better known as https.
- It invites you to answer a survey that asks for personal or account information.
- States your account has been hacked, then asks for personal or account information.
- Indicates there are unauthorized charges on your account, then asks for personal or account information.
- Asks you to confirm, verify or update your account or billing information.
- Asks you to provide account information because someone wants to send you money.
- Claims you're getting a refund.
- States you've won a contest.

The best way to verify calls or emails received regarding your finances is to contact your financial institution directly. Locate the contact information on one of your statements or other materials from the company.

FLCBank wants you to know it is not our practice to ask for your pin or password by phone, text or email. However, if you initiate the call, a bank employee may ask you to give private information for them to assist you with any questions or concerns you have about your account.

Further, you can be assured that it's not our practice to:

- Send email that requires you to enter personal information directly into the email
- Send email threatening to close your account if you do not take the immediate action of providing personal information
- Send email asking you to reply by sending personal information
- Our bank, other financial institutions and regulatory agencies (i.e. FDIC, OCC, etc.) will never request sensitive information via text messaging (SMS).

With those things in mind, please exercise caution when reading emails that may appear to have been sent by us. If you see anything suspicious or something just doesn't seem right, give us a call immediately.

Social Engineering

In a social engineering attack, an attacker uses human interaction to manipulate a person into providing them information. People have a natural tendency to trust. Social engineering attacks attempt to exploit this tendency in order to steal your information. Once the information has been stolen it can be used to commit fraud or identify theft.

Social networking has changed the way we interact with friends and associates. While social networks, like Facebook, Twitter, YouTube, Instagram, and Snapchat, and others play a significant role in our lives, they are also a high risk for security threats.

It's better to be cautious about the information you share on social media. Don't use information from your social media accounts for your user ID or password. Take these precautions to protect yourself:

- **Have a strong password**. Use special characters like symbols and capital letters when creating your password. Also, don't use "common" passwords, like your birthday or your child's name.

- **Be careful with status updates**. We innocently post status updates that would give information needed to steal your identity. For example, you may post "Happy birthday to my mother!" and then tag her in the post. Likely, your mother's maiden name will be associated with that tag. Your mother's maiden name is a popular security question, which you just shared online.

- **Don't reveal to much about you.** Be cautious with how much personal information you share on social media profiles. Fraudsters can use these sites to collect your personal information to commit fraud. Common security questions are where you live. Consider leaving this section blank or use a fake location or make one up from another city and state.

Website Spoofing
Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different address. If you are suspicious of a website, close your browser and contact the company directly by phone. Do not click links on social networking sites, pop-up windows, or non-trusted websites.

Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative. Only give sensitive information to websites using a secure connection. Verify the web address begins with https:// (the "s" is for secure) rather than just http://

Spyware
Spyware, which includes keystroke loggers, screen and mouse recorders, and other types of malware, allows distant hackers to extract sensitive data from your computer. These programs often slow down your computer and send harvested information to criminals.

Follow the tips below to protect your computer and private information from these dangerous programs

- Never open any email attachments, web links, or files if the sender or source is not trustworthy or cannot be confirmed. This will help prevent spyware (which is designed to secretly access information) from being installed on your computer.
- Use the automated update wizards in your operating system to download and install the latest security patches.
- Install a firewall and anti-virus software with spyware protection on your computer. Use the automatic update options, and keep your subscriptions current, as fraudsters continue to develop new malware and viruses.
- Use email spam-filtering software.
- Avoid using public computers shared by many individuals to pay your bills, check your account balance, or transact business. If you do have to use a public computer, remember to log out of any websites completely and log off the computer.
- Always use encryption for wireless access.