Ambassador Courier

Upcoming Important Dates & Seminars

Monday, May 26
All locations closed in observance of Memorial Day

Tuesday, May 27
Three Transitions to Retirement Virtual Seminar, 6pm

Tuesday, June 3
Rollover Planning Virtual Seminar, 6pm

Thursday, June 19
All locations closed in observance of Juneteenth

Tuesday, June 24
Women and Investing Virtual Seminar, 6pm

Friday, July 4 and Saturday, July 5
All locations closed in observance of Independence Day

Register for upcoming virtual seminars on the events calendar at firstffcu.com

How to Protect Personal Information on Your Phone

Smartphones are like digital vaults. They hold our conversations, banking information, emails, passwords, photos, and more. But all that convenience comes with risk—if your phone falls into the wrong hands or gets hacked, your personal information could be compromised.

At First Financial, we know how important it is to keep your information safe. Follow the steps below to protect the personal data stored on your phone.

1. Lock Your Phone with a Strong Passcode

Start with the basics: Set a secure lock screen. Whether it's a passcode, fingerprint, facial recognition, or a combination – this is your first line of defense against unauthorized access. If you use a numeric passcode, make sure it's at least six digits long, and avoid obvious choices like 123456 or your birthdate.

2. Keep Your Phone and Apps Updated

Software updates aren't just for new features, they're critical for patching security vulnerabilities. Enable automatic updates for your phone's operating system and all installed apps when new versions become available. Updates often include fixes that block hackers from exploiting weaknesses. It's one of the easiest — and most important — ways to protect your device.

3. Use Two-Factor Authentication

Many apps on your phone, like banking, email, or shopping – contain sensitive information. Enable two-factor authentication (2FA) on those accounts whenever possible. This adds an extra layer of security by requiring a second verification step, like a temporary code sent to your phone, in addition to your password. Even if someone manages to steal your password, they won't be able to access your account without that second factor.

4. Create Strong, Unique Passwords

Strong passwords are a must, but they can be hard to remember. Consider using a password manager app to generate and store unique passwords for all your accounts. That way, you're not relying on the same one or two passwords for everything. When creating a password, aim for at least 15 characters with a mix of letters, numbers, and symbols. Avoid using easy to guess information, like birthdays or pet names.

5. Be Cautious with Public Wi-Fi

Free Wi-Fi is convenient, but it's also risky. Hackers can intercept data on unsecured networks. Avoid accessing sensitive accounts like your bank or credit card when using public Wi-Fi at a coffee shop, airport, hotel, etc. Consider using a virtual private network (VPN) to encrypt your connection and add a layer of privacy when on public networks.

6. Turn On Phone Tracking and Remote Wipe Features

If your phone is ever lost or stolen, tracking and remote wipe tools can help. Enable "Find My iPhone" (Apple) or "Find My Device" (Android) so you can locate your phone, lock it, or even erase the data remotely if needed. This ensures your private information stays out of the wrong hands — even if your phone doesn't make it back to you.

7. Be Selective About App Permissions

When you download a new app, it may request access to your contacts, location, camera, or other sensitive areas. Only grant permissions that are necessary for the app to function, and/or only when the app is being used. Review your existing apps regularly and revoke any permissions that seem excessive.

8. Watch Out for Phishing Messages

Scammers can send text messages or emails that look like they're from a trusted source. These messages may include links that install malware on your device or ask for personal information. Avoid clicking on suspicious links, and never provide personal details unless you're absolutely sure of the sender. Check out our Important Alerts & Scams blogs at blog.firstffcu.com to learn more about phishing and how to protect yourself.

Stay Secure with First Financial

Your phone holds a lot of personal information — do everything you can to keep it secure. Taking just a few simple steps can greatly reduce your risk of identity theft and fraudulent activity.

Need help protecting your finances or setting up First Financial mobile banking security features and alerts? We're here to help. **Call us at 732.312.1500 or visit your local branch.**

Spring Greetings

We hope that you are enjoying the warmer temperatures and longer days of spring with your family and friends!

If your organization is planning a *sizzling* in-person or virtual event this summer, please let us know and we would be happy to attend or send materials. Feel free to pass this newsletter along to your employees too. We are here to answer any questions they might have or provide financial advice when they need us!

If you're interested in bringing us to your school or business, contact Business Development at business@firstffcu.com.

We are grateful for the opportunity to continue supporting you and your employees in achieving financial wellness.

Sincerely,
Samantha Colella,
Business Development Representative

Community Spotlight

Despite the frigid temperatures, we stayed *warm* and connected with our Monmouth and Ocean County community partners at various winter-friendly events. Let's take a look at where our travels have taken us over the last few months!

In February, we had the pleasure of meeting the educators of Lakewood at Icarus Brewing. Later in the month, we attended a New Jersey Education Association Conference at the Ocean Place Resort and Spa, to showcase the benefits of credit union membership to the educators that help our local schools run.

March was full of meeting several community partners, from the faculty at Brookdale Community College, to the retired educators of Ocean County, and the staff of Ocean County Utilities Authority in Bayville.

We are ready to spring into action and take part in any upcoming events you may hold this year. If you would like us to visit your organization or send you virtual materials, please contact us today!

Meet Miguel Ramos, Owner of Unique Designs Constructions in Little Egg Harbor NJ

Meet Miguel Ramos, one of our valued business members and proud owner of Unique Designs Constructions. Miguel began banking with First Financial over two decades ago to fulfill his personal banking needs. When he embarked on the journey of becoming a business owner fifteen years later, bringing his business banking to First Financial was a no-brainer. **Watch his video interview at youtube.com/FirstFinancialFCU** to learn how the convenience and familiarity of First Financial led Miguel to explore our business banking options when he became a business owner.

New Lower Rates on Auto Loans

Lower rates on auto loans have bloomed at First Financial, which means you can drive into spring with a new ride! It's the perfect time to finance the car you've been dreaming of, refinance your vehicle from another lender to see if we can help you save on your monthly payments, or buy out your lease.* We also have same-day approval decisions, and a quick and easy online application.

**Visit our Auto Loans page at firstffcu.com for full terms & conditions, or to apply online.*

Debt After Death: What Happens to Debt When Someone Dies?

Losing a loved one is never easy. In addition to the emotional challenges you may face, you might also be worried about what will happen to their debt once they are gone. Generally, with limited exceptions, when a loved one dies you will not be liable for their unpaid debt. Instead, their debt is typically addressed through the settling of their estate.

How are debts settled when someone dies?

The process of settling a deceased person's estate is called probate. During the probate process, a personal representative (known as an executor in some states) or administrator if there is no will, is appointed to manage the estate and is responsible for paying off the decedent's debt before any remaining estate assets can be distributed to beneficiaries or heirs. Paying off a deceased individual's debt can significantly lower the value of an estate and may even involve the selling of estate assets, such as real estate or personal property.

Debts are usually paid in a specific order, with secured debt (such as a mortgage or car loan), funeral expenses, taxes, and medical bills generally having priority over unsecured debt, such as credit cards or personal loans. If the estate cannot pay the debt and no other individual shares legal responsibility for the debt (e.g., there is no cosigner or joint account holder), then the estate will be deemed insolvent and the debt will most likely go unpaid.

Estate and probate laws vary, depending on the state, so it's important to discuss your specific situation with an attorney who specializes in estate planning and probate.

What about cosigned loans and jointly held accounts?

A cosigned loan is a type of loan where the cosigner agrees to be legally responsible for the loan payments if the primary borrower fails to make them. If a decedent has an outstanding loan that was cosigned, such as a mortgage or auto loan, the surviving cosigner will be responsible for the remaining debt.

For cosigned private student loans, the surviving cosigner is usually responsible for the remaining loan balance, but this can vary depending on the lender and terms of the loan agreement.

If a decedent had credit cards or other accounts that were jointly held with another individual, the surviving account holder will be responsible for the remaining debt. Authorized users on credit card accounts will not be liable for any unpaid debt.

Are there special rules for community property states?

If the decedent was married and lived in a community property state, the surviving spouse is responsible for their spouse's debt as long as the debt was incurred during the marriage. The surviving spouse is responsible even if he or she was unaware that the deceased spouse incurred the debt.

What if you inherit a home with a mortgage?

Generally, when you inherit a home with a mortgage, you will become responsible for the mortgage payments. However, the specific rules will vary depending on your state's probate laws, the type of mortgage, and the terms set by the lender.

Can you be contacted by debt collectors?

If you are appointed the personal representative or administrator of your loved one's estate, a debt collector is allowed to contact you regarding outstanding debt. However, if you are not legally responsible for a debt, it is illegal for a debt collector to use deceptive practices to suggest or imply that you are. Even if you are legally responsible for a debt, under the Fair Debt Collection Practices Act (FDCPA), debt collectors are not allowed to unduly harass you.

Finally, beware of scam artists who may pose as debt collectors and try to coerce or pressure you for payment of your loved one's unpaid bills.

First Financial
Investment & Retirement Center

Questions about this topic or looking to get started with estate planning? Contact First Financial's Investment & Retirement Center by calling (732) 312-1534.

You can also email Mary.LaFerriere@lpl.com or Maureen.McGreevy@lpl.com

Protect Yourself From Check Fraud Scams

Despite the rise of digital banking, check fraud remains a prevalent financial scam. Scammers use sophisticated techniques to steal and manipulate checks, often leaving victims unaware until it's too late. Understanding how check fraud works and how to recognize suspicious activity can help protect your finances.

What is Check Fraud?

Check fraud occurs when criminals manipulate, forge, or steal checks to illegally access funds.

Common Types of Check Fraud

- **Check Washing:** Thieves steal legitimate checks — often from mailboxes, and modify key details, such as the recipient's name or the payment amount, before cashing or selling them.
- **Check Kiting:** Using multiple accounts to write and deposit bad checks, temporarily covering insufficient funds before withdrawing cash.
- **Forgery:** Criminals create counterfeit checks or forge signatures to access funds fraudulently.
- **Fake Checks:** Scammers trick victims into depositing fraudulent checks, often under the guise of prize winnings, job opportunities, or overpayment schemes. Once the check is cashed, the fraudster requests the money be sent back, leaving the victim responsible when the check bounces.

How to Recognize Check Fraud

Recognizing fraudulent checks early can help you avoid financial loss. Be on the lookout for these red flags:

- **Unexpected Checks**: If you receive a check from an unknown source, verify its legitimacy before depositing it.
- **Spelling and Formatting Errors:** Poor grammar, misspelled words, or inconsistent fonts can indicate a counterfeit check.
- **Unusual Check Amounts:** If the check amount exceeds what was agreed upon, it may be a scam.
- **Discrepancies in Mailing Address:** If the check was mailed from a different location than the issuing bank, proceed with caution.
- **Request for Money Transfers:** Be wary if someone asks you to deposit a check and send a portion of the money back. This is a common scam tactic.
- **Lack of Security Features:** Legitimate checks include watermarks and security threading. If these features appear altered or missing, the check may be fraudulent.

How to Prevent Check Fraud

While fraudsters are persistent, there are steps you can take to reduce your risk:

- **Use Secure Payment Methods:** Opt for electronic payments, online bill pay, or peer-to-peer payment apps (Zelle, Venmo, etc.) instead of checks when possible.
- **Write Checks with a Fraud-Resistant Pen:** Gel pens with permanent ink can make it harder for criminals to alter check details.
- **Check Your Mail Frequently:** Avoid leaving checks in your mailbox where they can be stolen and deposit them directly inside a bank or electronically right away.
  - If you deposit electronically, keep the check in a secure place and shred it once it clears.
- **Enroll in Informed Delivery:** The U.S. Postal Service offers a free service that notifies you of incoming mail, helping you detect missing mail sooner.
- **Monitor Your Bank Statements:** Regularly check your accounts for unauthorized transactions and report suspicious activity immediately.
- **Verify the Issuing Bank:** If you receive a check from an unfamiliar source, call the bank listed on the check using the contact information from their official website.

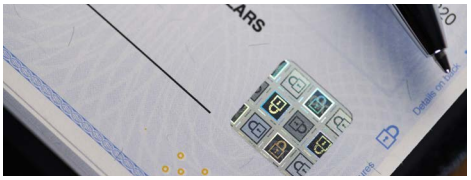
What to Do If You're a Victim of Check Fraud

If you suspect check fraud, take immediate action to minimize financial loss:

- **Notify Your Bank:** Report the fraudulent activity and request a hold on your account if necessary.
- **File a Police Report:** Document the fraud with your local law enforcement agency.
- **Report to Federal Agencies:** The FTC, U.S. Postal Inspection Service, and the FBI's Internet Crime Complaint Center accept reports of financial scams.
- **Monitor Your Credit:** Fraudsters who steal checks may also attempt identity theft. Consider using credit monitoring tools to detect future unauthorized activity.

Stay Protected with First Financial

Check fraud can happen to anyone, but awareness and preventative measures can keep your finances secure. By staying vigilant and following these best practices, you can reduce your risk of falling victim to check scams. If you suspect fraud or unusual transactions on any of your First Financial accounts, call us at 732.312.1500 or **visit your local branch today.**



Loan Connection
(732) 312-1500, Option 4

To Fax Loan Applications
(732) 312-1530 (24-hour)

Contact Us
Local Callers **(732) 312-1500**
Out of Area **(866) 750-0100**

info@firstffcu.com
firstffcu.com

Neptune Branch
783 Wayside Road

Toms River Branch
1360 Route 9 South
Corner of Routes 9 & 571

Freehold/Howell Service Center
389 Route 9 North
Next to Howell Park & Ride

First Financial FEDERAL CREDIT UNION

Contact Business Development

Samantha Colella
Business Development Representative
scolella@firstffcu.com
732.312.1421

First Financial's Supervisory Committee has the responsibility to investigate member complaints that cannot be resolved through normal channels. If you have a complaint or suggestion to improve our service to you or if you have an unresolved problem, please write to:

Supervisory Committee
P.O. Box 751
Neptune, NJ 07754