



Lake Ridge
Bank™

Go Far. Go Together.

A GUIDE

TO NAVIGATING BANK ACCOUNT FRAUD



Financial fraud attempts and the financial impact on victims continues to grow. Fraud can happen to anyone, at any time, and anywhere. The best way to protect yourself is to be fraud savvy. As your financial partner, Lake Ridge Bank wants to help you be better prepared with the tools and resources you need to combat fraud before it happens. And if you've already been a victim of bank account fraud, this guide can help you understand what to expect, from start to finish.



FILING A FRAUD DISPUTE WITH LAKE RIDGE BANK

If you believe you have had fraud on your account(s), you should file a formal dispute and sign an affidavit to initiate the fraud process. We're here to help you – **contact your banker to begin your fraud dispute.**

- Your banker will help determine what type of dispute to file. Types of disputes include:
 - **Altered Item** – this is an existing check where details such as the payable amount or the payee's name was changed after it was written.
 - **Counterfeit** – A fabricated check or a copy of a real check with altered details. This is a new check that is created based off an original version, without the account holder's authorization.
 - **Fraudulent Endorsement** (signature on the back of the check) – this is an endorsement that is forged or made without the authorization of the rightful payee.
 - **Forged Drawer/Signer** (signature on the front lower right corner of the check) – this involves a forged signature of the owner of the checking account. This can include lifting a valid signature off another check and adhering it to the forged check, or simply someone else signing the account owner's name on the check.
- After signing your dispute, your banker will help you close any existing accounts affected by the fraud and open your new account(s). Once the fraudsters use an account, they are likely to attempt fraud again until the account is closed.

REGULATORY TIMEFRAMES FOR FILING DISPUTES

DISPUTE REASON	EXAMPLE	CONSUMER TIMEFRAME TO DISPUTE	BUSINESS TIMEFRAME TO DISPUTE
Altered Check	Originally issued check payee or dollar amount altered	1 year from date of statement	1 year from date of statement
Counterfeit Check	A copy of a legitimate check, created without your approval	30 days from date of statement	1 business day after posting
Fraudulent Endorsement (signature on back of check)	Endorsement is forged or not authorized	3 years from date of statement	3 years from date of statement
Forged Check Signer	Someone forged your signature on the front of the check	30 days from date of statement	1 business day after posting
ACH Error	You sent an electronic payment for products or services to the wrong vendor	30 days from date of statement	1 business day after posting



ACCOUNT FRAUD STEPS TO RESOLUTION

If you believe fraud has occurred on your bank account, contact your banker immediately or call the bank at **(608) 223-3000** to begin the fraud resolution process (below) to help minimize any further impact on your accounts.

We are here to help you get resolution. A personal banker can assist you with completing and submitting a Fraud Dispute form for the fraudulent activity on your account. They can also close any affected accounts and open your new accounts to prevent any additional fraud. As part of the process, a new check card and checks will be ordered to ensure you can continue to access your accounts for other payments. We can also help you switch all your automatic payments and deposits into your new account to make sure your bills continue to be paid.

Our experienced team will work closely with you to help make the process as easy as possible.





FILING A POLICE REPORT

After you have completed and submitted your Fraud Report, we strongly recommend that you file a police report. If you choose not to file a police report, Lake Ridge Bank will file one if there was a monetary loss due to fraud, however, we may also file a police report in circumstances that didn't result in a monetary loss.

- Contact the police department in the city where the fraudulent activity took place (if known) or contact your local police department to file a police report. Use the non-emergency number for the police.

WHAT HAPPENS AFTER YOU FILE YOUR DISPUTE?

Unfortunately, filing a dispute does NOT guarantee that you will receive the money you lost due to the fraudulent activity back. Like most banks, Lake Ridge Bank DOES NOT provide provisional credit or reimbursement of any money you lost due to fraud outside of the dispute time limits shown on page 1.

- Once the dispute is filed with our bank, a message is sent to the "Bank of First Deposit" (BOFD) which is the bank where the initial transaction took place. For example, if someone fraudulently endorsed a check you had issued and cashed it at Chase Bank, Chase Bank would be the BOFD.
- Be sure to contact anyone who was expecting a payment from you but may not have received it due to the fraudulent activity to make other arrangements to pay them.
- Depending on the situation, the BOFD may not have a time limit in which they are required to respond to your dispute by, and instead may utilize a "first come, first served" system to process disputes.
 - This type of dispute processing can take a substantial amount of time before we hear back from the BOFD which means you may not know the outcome of your dispute for several months.
 - o If we have not received a response within 60 days of initially sending the dispute, we reach out to the BOFD again.
 - o If we have not received a response within 120 days of initially sending the dispute, we will determine other actions we may be able to take.
- Assuming you notified our bank of your fraudulent transaction(s) and signed the dispute affidavit within the dispute time limits shown on page 3, your account will be reimbursed for any fraudulent activity identified during the dispute time frame.
 - For fraudulent transactions disputed outside of the dispute time limits shown on page 1, there will be no reimbursement of funds unless funds are received from the BOFD.
- Once we receive the results of the BOFD's fraud investigation, we will email you these results, including any monetary reimbursement you will receive, if applicable.
 - Once we receive the funds from the BOFD, we will credit your account within three (3) business days.



OTHER THINGS TO CONSIDER WHEN YOU'VE BEEN A VICTIM OF FRAUD

- If the fraud took place through a computer, cell phone, tablet or other internet enabled device, make sure you **immediately** change your logins, passwords and PIN numbers and have your computer scrubbed for viruses by a professional. Visit **www.IC3.gov** for more information.
- Continue to monitor your account activity to ensure no additional fraudulent activity occurs on your account(s). If it does, report it to your banker immediately.
- Consider placing a freeze on your ChexSystems report. This report is used by financial institutions whenever you open a new account to determine if you have unpaid bank accounts.
 - To place a freeze call **(800)428-9623** or visit **chexsystems.com/security-freeze**
- If you are a victim of identity theft, visit **IdentityTheft.gov** or call **(877) 438-4338** to file a report with the Federal Trade Commission (FTC).
- Regularly review your credit report for accuracy. To obtain a free copy of your credit report go to **annualcreditreport.com** or call **(877) 322-8228**.
- If you would like to place a fraud alert, or freeze your credit report, we recommend you contact all three credit bureaus. There is no cost to place fraud alerts.
 - To place a **fraud alert**, contact all three of the following companies:
TransUnion.com/fraud or **(800)680-7289**
Experian.com/fraudalert or **(888)397-3742**
Equifax.com/CreditReportAssistance or **(888)766-0008**
 - To place a **freeze** on your credit report, contact all three of the following companies:
TransUnion.com/freeze or **(888)909-8872**
Experian.com/freeze or **(888)397-3742**
Freeze.Equifax.com or **(800)349-9960**
- You may want to perform an Electronic/Computer Scrub on your computer/tablet/phone to check for, and remove, any malware and malicious viruses. There are a variety of companies in the area that perform malware/virus check and removal. Be sure to ask about the costs associated with their services.



FRAUD PREVENTION TOOLS

Our **Consumer Accounts** offer a variety of fraud prevention tools, including:

- **Account Alerts:** With account alerts, you know the moment something important happens with your account(s). Choose from dozens of account activity alerts and receive notifications via email, text, online banking or push notifications through your mobile app.
- **eDocuments:** Don't fall victim to identity theft from stolen paper documents, sign up to receive and access your account statements and notices securely online.
- **Credit Sense:** Monitor your credit report through your online or mobile banking app.
- **Card Control:** Provides a central hub for managing your cards – view your transactions and stay informed in real time.
- **Bill Pay:** Offers you a secure and easy way to manage your bills and make payments directly from your Lake Ridge Bank account.

Our **Business Accounts** offer numerous fraud prevention services, including:

- **Check Positive Pay:** An image based fraud prevention service which compares and confirms all checks presented for payment against the actual checks you upload into our system.
- **ACH Fraud Protection:** Your ACH activity can be filtered or blocked, giving you full control of your funds.
- **Online Banking Protection:** Additional layers of security to your company's login process using hard tokens, soft tokens, or RSA authentication.
- **Account Alerts:** Lets you know the moment something important (or suspicious) happens to your account. You choose the alerts you need to stay informed in real time.
- **Cardvalet:** Turn your cards on or off instantly, whenever you want, from wherever you are. Allows you to control transactions by category, or by dollar amounts.

Let us help you protect your accounts from fraud. Contact your banker today for more information about how we can help you prevent fraud in your accounts. Why wait? We make it easy to add our fraud prevention tools and start protecting your accounts today.



TOP 5 SCAMS WE'RE CURRENTLY SEEING

While we continue to see a growing number of financial frauds and scams, here are the top five frauds you should be aware of and how you can avoid them:

1. Grandparent Scams - Scammers call and pretend to be a family member in danger (they've been arrested, have been in an accident or are ill), and asks you to send them funds immediately to get them out of the "crisis."

- We recommend all families create a "password" to share with all family members to use if they are truly in a dangerous situation.
- Always hang up and call the family member who contacted you back directly using the phone number you usually reach them at to see if they are really in a dangerous situation.

2. Romance Scams - New "love interests" gain your trust, then tell you that someone they know needs money urgently. They then ask you for money to purchase items on the scammer's behalf. The scammers tend to ask for payment in gift cards, Venmo, Zelle,® Paypal™ or cryptocurrency. These types of payments are requested because they are difficult to track.

- Talk to your friends or family about your new "love interests" and pay serious attention if they have any concerns.
- Don't share personal information, usernames, passwords, or one-time codes with anyone, especially someone you just met recently.
- If you just met someone online and they start asking you to send them money, it's probably a "romance" scam!

3. Cryptocurrency Scams - This investment fraud is the costliest type of financial fraud we see. Scammers use crypto currency because there are no legal protections and payments using cryptocurrency are usually irreversible.

- If you meet someone online and they want to show you how to invest, have opportunities for you to make money quickly, or just offer to show you how to send cryptocurrency, assume it is a fraud!
- A legit business or government entity will never ask you for money through email, text, or social media. They will also never demand you buy or pay in cryptocurrency.

4. Employment Scams - Scammers will lure their victims into interviewing for a company that may seem legit. This fake company then starts to collect personal information from you which they then use to obtain your banking and personal information, apply for loans and credit and more. Other job frauds promise guaranteed or easy income if you purchase a program, give them money to obtain the job, or required training, to the scammer.

- Look up the name of the company or person hiring you, along with the words scam, review, or complaint. Are other people being scammed by this company or person?
- Never click on an unexpected link they send you, even if it seems to come from a reputable company.
- Never pay a fee for a job or training program without doing your research.

5. Online Account Tax Scams - Tax related scammers may pretend to be a "helpful" third party who offers to help you create an IRS online account to pay your taxes. These scammers then use your name and personal information to file fake tax returns to your tax refund sent to them or use your information to commit other financial fraud or identity theft.

- Never use a third-party vendor to set up an online account with the IRS. Our team can help you if you would like assistance.
- Don't store your financial records or other important information in your saved emails, or on your desktop.

OTHER RESOURCES

For more information on how to prevent fraud and/or what to do if you are a victim of fraud, contact any of the entities listed below:

- Federal Trade Commission (FTC):
www.ftc.gov or **1-877-FTC-HELP**
- Office Of Comptroller of the Currency Fraud Resource:
www.occ.treas.gov
- Consumer Financial Protection Bureau:
www.consumerfinance.gov/consumer-tools/fraud/
- Financial Crime Resource Center:
www.victimsofcrime.org
- AARP Fraud Watch Network:
www.aarp.org/money/scams or **1-877-908-3360**

If you have any questions about fraud in your accounts, or how Lake Ridge Bank can help you prevent fraud from happening on your accounts, please contact a banker at any of our 20 offices or call our Client Support Team at **(608) 223-3000** today.

You can prevent most fraud by keeping a close eye on your accounts and staying up to date on the latest scams and frauds. As your financial partner, Lake Ridge Bank is always available to assist you with any fraud questions you may have or with any of the steps in the Fraud Process.

FRAUD RESOLUTION CHECKLIST

- ☐ Contact your bank immediately to alert them of the fraudulent activity.
- ☐ Fill out the required Fraud Dispute Form completely.
- ☐ File a police report.
- ☐ Close any affected accounts.
- ☐ Open new accounts, order new checks and check cards.
- ☐ Change any automatic payments and deposits to the new accounts.
- ☐ Continue to closely monitor your accounts for suspicious activity.



**Lake Ridge
Bank™**

Go Far. Go Together.