Bank of Marin

# Wire and ACH Fraud Prevention

Businesses and consumers lose millions of dollars each year to wire transfer and ACH (Automated Clearing House) fraud - and that number is on the rise according to the Federal Trade Commission. Fraudsters disguise themselves as a trusted source by providing what appears to be legitimate information regarding a transaction and/or request for funds. The request may appear to be something you are expecting via an email, text message, or phone call.

To avoid being a victim of electronic fraud, here are a few simple steps you can take to verify that a request to send or receive funds is legitimate.

## Verify the Source of the Request

- Never initiate changes based only on email communication. Fake email addresses and phone numbers are the most common ways fraudsters request funds.
- Always investigate unusual requests. If you receive a request for payment that is out of your ordinary payment arrangement, confirm by phone with your vendor.
- Never use contact information provided by the requestor.
- Always verify changes to vendor information, including mailing address, bank routing number and bank account number.
- Always be suspicious of requests for secrecy or pressure to take action quickly.

**If you receive a request threating an action against you unless financial information or funds are provided, consult your banker, a trusted friend or expert immediately.**

## Compare Original Wire Information

- If this is a recurring transaction, confirm that **ALL** numbers and information match original wire documentation.
- Do not use account numbers or other private information that is provided by the requestor.
- Consult your banker if you see any discrepancies or have questions about the new information provided.

## General Precautions

- **Do not click on any links** provided to you by the requestor. Cyber-criminals can install malware to gain access to your login credentials without your knowledge.
- **Do not agree to receive money** to purchase gift cards, to send to another financial institution, or withdraw cash from your account to purchase cashier's checks or money orders to deposit into another person's account.
- **Beware of requests from unknown persons** asking you to purchase gift cards and then to provide the card and pin number electronically or over the phone.
- **Do not send money** in response to an unexpected or urgent request from a loved one. Scammers often pretend to be someone you know who is in distress. Verify the legitimacy of the request.

**TIP** **Bank of Marin will never ask for your debit card PIN or digital banking password.**

**If you suspect your Bank of Marin bank account has been compromised, contact your local branch or call Customer Support (866) 626-6004.**

**For more information about protecting yourself from fraud visit https://www.ftc.gov**

For additional Fraud Prevention Resources visit **WWW.BANKOFMARIN.COM/PREVENTFRAUD**