Opt In for Service to Transfer To/From Another Financial

You must apply to use he Automated Clearing House (ACH) network in order to be able to transfer funds to/from Caro to/from another financial institution.

Member Name	Member Number	SSN

Member Email Address

I (We) understand that this authorization will remain in full force and effective until I (we) notify Caro (in writing, by phone, or in person at 4480 Rosewood Drive, Columbia, SC 29209) that I (we) wish to revoke this authorization. I (we) understand that Caro requires at least five (5) business days notice to cancel.

Signature: _____ Date: _____

Signature: _____ Date: _____

IN-OFFICE USE ONLY

Staff Member Initials: _____ Date: _____

Member has been taken off of opt-out of External ACH list: _____

Member has already logged into Online Banking: _____

If yes, added member to External ACH list: _____

Mail or deliver to:
4480 Rosewood Dr • Columbia, SC 29209 | 710 Pulaski Street • Columbia, SC 29209
803.227.5555 • www.smartcaro.org

IMPORTANT INFORMATION

The Automated Clearing House (ACH) network is a way of transferring money from one bank account to another. Supporting both credit and debit transfers, payments and withdrawals are sent to the clearing house where they await authorization before arriving at their final banking destination

What is ACH Fraud?

ACH fraud occurs when funds are stolen through the ACH network. A criminal needs two things to carry out ACH fraud:

- A bank account number
- A bank routing number

With this information, they can transfer money from the victim's account, either as a lump sum or as recurring payments. They can also make unauthorized payments for goods or services. The time delay with ACH payments is a key vulnerability that financial criminals exploit. Criminals use a range of technological and psychological tactics to obtain these details.

Types of ACH Fraud

- **Data breaches**: Criminals often gain access to customer credentials via a data breach. In this scenario, fraudsters log into bank accounts with bought or stolen information from the dark web before withdrawing funds through the ACH network.
- **Check kiting**: In this type of ACH fraud, criminals move money back and forth between accounts at different banks. When the transfer is approved by the clearing house, it looks like the money is in the account, but it has already been moved.
- **Email phishing**: One of the most common methods, phishing involves sending fake emails or texts that appear to be from legitimate organizations. These messages trick victims into revealing sensitive account details by mimicking the look and feel of communications from trusted sources.
- **Loss or theft of debit card**: If the loss or theft of a debit card is not immediately reported, criminals can use this window of time to carry out an unauthorized ACH withdrawal.
- **Malware**: Botnets install malicious software on victims' devices without their knowledge. The malware then steals account numbers and login credentials stored on the infected system.
- **Skimming**: Skimmers are physical devices illicitly installed on ATMs, gas pumps, and other card readers. They copy card data, which can then be used to generate or access account numbers.
- **Social Engineering**: This method involves manipulating authorized users into making unauthorized transfers, often by exploiting their trust and lack of awareness.

IMPORTANT INFORMATION

Who's At Risk?

Any business or consumer with a checking, savings, credit union, or peer-to-peer payment account may be at risk. ACH fraud impacts many victims, each with unique vulnerabilities and consequences. The list of victims most at risk includes:

- **Individuals**: Particularly at risk are elderly individuals who may be more prone to falling for social engineering tactics. These tactics often involve manipulating the victim into divulging account information, either through confidence tricks or deceptive requests that seem legitimate.
- **Small Businesses**: Small companies frequently lack the advanced cybersecurity measures that larger corporations might have. This makes them more susceptible to phishing attacks and malware. Small business accounts often carry sufficient funds to be attractive targets for fraudsters.
- **Non-Profits and Charities**: The charitable nature of these organizations can make them targets for fraud. They may be tricked into making unauthorized transfers under the guise of genuine requests for donations or funding.
- **Government Entities**: Public sector bodies are not immune to ACH fraud. Those involved in collecting payments or distributing benefits, such as tax authorities or social welfare agencies, can be targeted for their substantial financial transactions.

Each of these groups faces unique risks in the context of ACH fraud. The consequences can range from financial loss to damage to reputation and trust, highlighting the importance of awareness, risk analysis, and preventative measures.

ACH Fraud Protection and Prevention

The widespread use of ACH payments and the sophistication of criminal tactics demand a robust approach to information security and fraud prevention. Here are several key technologies and strategies that can significantly reduce the risk of ACH fraud:

- **Employee Education**: Educate staff about phishing and social engineering tactics so they recognize and avoid schemes aimed at extracting sensitive account information.
- **Transaction Monitoring**: Use transaction monitoring and fraud detection tools to identify anomalies and unauthorized payments. Continuous monitoring helps in the early detection of suspicious activities.
- **Data Encryption and Secure Transmission**: Encrypt stored account details and ensure data is encrypted when sent over networks.
- **Limited Access Control**: Restrict account access to employees on a need-to-know basis. Limit privileges and monitor who has access to sensitive account information.
- **Periodic Risk Assessments**: Conduct regular risk assessments to identify and address vulnerabilities in your ACH transaction and account security processes. By understanding where their systems might be susceptible to fraud, you can implement targeted strategies to strengthen those areas.
- **Regular Security Updates**: Keep security software, firewalls, and antivirus programs current. Regular updates help to protect businesses from malware infiltration and security compromises that leak account details.

If you suspect fraud on your account, please contact us immediately.

Mail or deliver to:
4480 Rosewood Dr • Columbia, SC 29209 | 710 Pulaski Street • Columbia, SC 29209
803.227.5555 • www.smartcaro.org