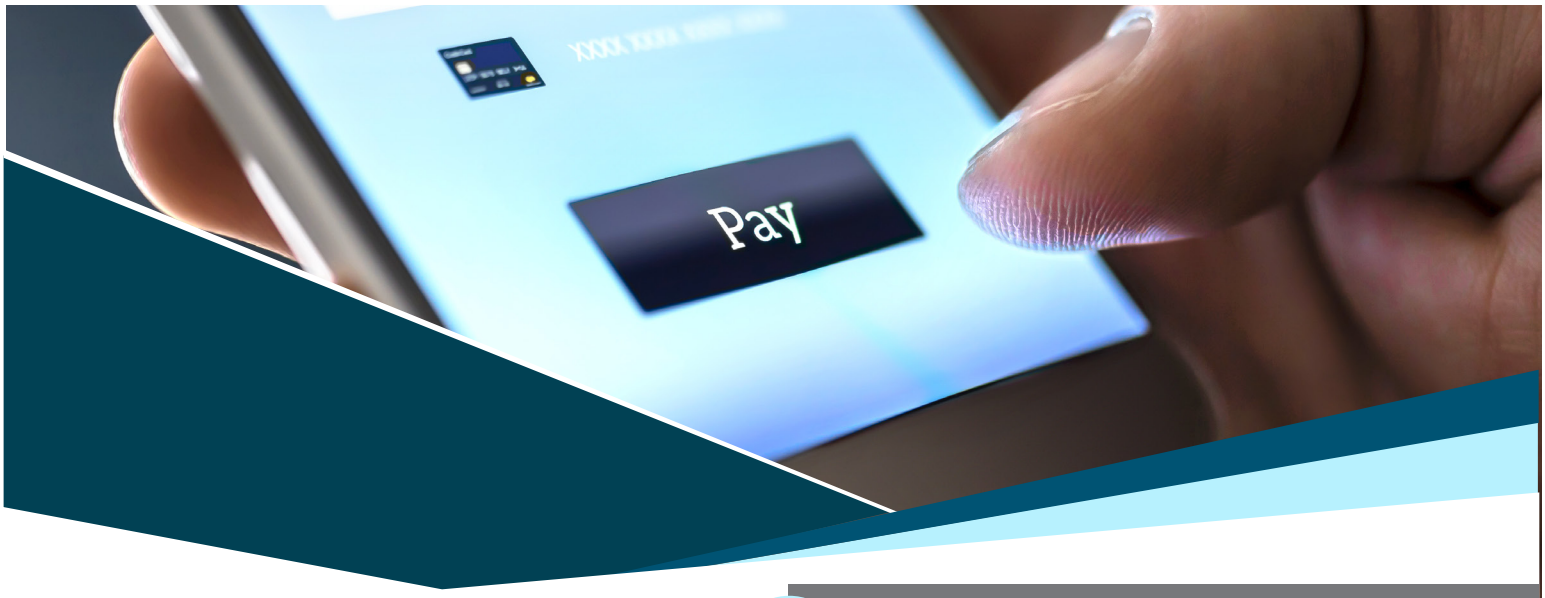

10 DO'S AND DON'TS TO PROTECT YOURSELF FROM P2P FRAUD

Digital payments such as peer-to-peer payments, or P2P payments, allow consumers to transfer money using their bank accounts, debit cards, or credit cards through a website or mobile app such as Cash App, Google Pay, Paypal, Venmo, and Zelle®. It's like sending cash and the transfer usually requires just a few clicks. At Piedmont Federal, we offer Zelle® which is a real-time P2P payment platform and money is sent in a matter of minutes to friends or family.

Be prepared to protect yourself and family by following the tips listed here:

If you are a victim of a P2P payment scam:
- **Contact us at 336-770-1000.**
- **File a complaint with the Federal Trade Commission or call 1-877-FTC-HELP (382-4357).**

DON'T Don't send money to someone you don't know or have never met in person.

DON'T Don't fall for these common and urgent scams such as relatives are in trouble, computer support, job/employment, dating/romance, sweepstakes or pay for a product until you receive it.

DON'T Don't fall for a scammer saying they "accidentally" sent you money on a P2P service and asks you to send the money back.

DON'T Don't do a Google search for customer service phone numbers. Scammers create fake websites with toll free numbers that connect to them.

DON'T Don't share bank authentication, verification numbers, or your personal information with anyone who contacts you, even if caller ID indicates it's a familiar company. Keep your account usernames/passwords, Social Security number, bank account, debit, and credit card information to yourself. If you're pressured or have any concerns, hang up and contact us directly.

DON'T Don't let anyone you don't know borrow your phone.

DO Do be sure to know and trust the other party who's receiving your money. Confirm the name, email and phone number. If you make a mistake, even one wrong digit, you will send your money to someone else who may not give it back. Just like handing someone cash, your bank can't get it back for you.

DO Do set up alerts to notify you of any transaction on your account.

DO Do enable multi-factor authentication — a step to verify who you are, like a text with a code — for all accounts and do not share the verification codes with anyone, including anyone claiming to be the bank.

DO Do be wary of accessing any financial or personal information on public Wi-Fi or mobile hotspots. They often lack security and hackers can capture sensitive personal information on these open servers.