

# Fraud Prevention for Account Opening

While financial institutions should grow their bottom line through new accounts, the digital landscape opens up doors for account opening fraud. With the increased ability to open an account online many fraudsters are preying on the opportunity to steal information and money. It is imperative to implement risk mitigation measures in the account opening process. Review this checklist for best practices for new accounts.

Often times, financial institutions are publicly displaying processes for opening and servicing new accounts. Often, scammers will use this public information to fraudulently open a new account and apply for a loan, a debit card, or a product offered by the financial institution to access secure information and steal funds. However, your financial institution can help prevent fraud activity on new accounts with these best practices:

- Validate all new accountholder information and watch for any type of immediate wire, ACH or new loan requests.
- Be aware of withdrawals at a branch location or an ATM immediately following a deposit at an ATM.
- Limit the dollar amount on outgoing wires, ACH, and debit card transactions for new (and existing) accountholders.
- Educate all accountholders to be cautious when accessing their online account and use hard-to-guess information for passwords and security questions.
- Consider requiring new accountholders to create a password or passcode that would be required for any type of activity performed on their account.
- Implement layers of multi-factor and dynamic authentication that includes strong passwords/passcodes, biometrics, and tokenization for verifying information and allowing online account access.
- Perform extensive authentication prior to approving loans requested by new accountholders.
- Institute a waiting period for new accountholders to apply for a loan, debit card, or product and consider limiting the dollar amount of loans requested by new accountholders.
- Require multi-factor authentication and strong passwords – also consider the use of biometrics, security tokens, etc. – before providing online access to account information.
- Review each new applicant’s credit reports in detail before opening their account to catch any warning signs of past financial crimes..
- Train and educate employees about red flags of new account fraud and loan fraud on an ongoing basis.

*Visit our website for more  
risk education:  
[alliedsolutions.net/resources](https://alliedsolutions.net/resources)*

**Subscribe to receive more risk education: [alliedsolutions.net/enews](https://alliedsolutions.net/enews).**

