



Digital banking is making account fraud easier for criminals. Scammers use publicly available information combined with stolen or synthetic identities to open and leverage fraudulent accounts. This kind of fraud will only escalate without proactive measures in the account opening process.

Answer the following questions to help you better understand any areas of vulnerability related to account opening.

POLICY & COMPLIANCE OVERSIGHT

Focus: Regulatory adherence, KYC/CIP standards, and financial crime compliance

Does your financial institution...

Have a designated BSA (Bank Secrecy Act) team?	Yes	No	Unsure
Utilize KYC/CIP verification per established regulatory frameworks, including:			
• Identity verification: Real-time, multi-source correlation?	Yes	No	Unsure
• Document verification: ID validation (e.g., passport, driver's license) and selfie comparisons?	Yes	No	Unsure
• Watchlist screening: Screening against OFAC, global sanctions, and politically exposed persons (PEP) lists?	Yes	No	Unsure
• Fraud screening: Use scorecards and behavior-based rules to detect fraud?	Yes	No	Unsure
• Device and behavior profiling: Analyze device, SIM, IP, GPS, VPN, and fingerprinting?	Yes	No	Unsure
• Multi-factor authentication (MFA): OTPs or knowledge-based questions to verify identity?	Yes	No	Unsure

INTERNAL PROCESSES & ACCOUNT CONTROLS

Focus: Employee training, account monitoring,
and transaction limitations

Does your financial institution...

Ensure employees are trained on when and how to validate accounts?	Yes	No	Unsure
Conduct ongoing training on synthetic identity red flags?	Yes	No	Unsure
Authenticate account access with more than just KBA (knowledge-based authentication) questions?	Yes	No	Unsure
Require new accountholders to create strong passwords/passcodes for account activity?	Yes	No	Unsure
Watch for immediate wires, ACH transfers, or loan requests on new accounts?	Yes	No	Unsure
Place check holds on newly opened accounts until funds are verified?	Yes	No	Unsure
Review remote deposit capture policies for suspicious check behavior?	Yes	No	Unsure
Limit outgoing transaction amounts (wires, ACH, debit) for new accounts?	Yes	No	Unsure
Authenticate extensively before approving loans for new accountholders?	Yes	No	Unsure
Institute a waiting period before allowing loans, debit cards, or product access for new customers?	Yes	No	Unsure
Set dollar limits for loans requested by new accountholders?	Yes	No	Unsure
Encourage accountholders to place credit freezes at bureaus?	Yes	No	Unsure
Encourage regular monitoring of accounts by both staff and consumers?	Yes	No	Unsure
Review new accountholders' credit reports to identify red flags of identity theft?	Yes	No	Unsure

TECHNOLOGY & DIGITAL ACCESS SECURITY

Focus: Authentication layers, access control,
and fraud detection tools

Does your financial institution...

Require MFA, strong passwords, and biometrics for account access?	Yes	No	Unsure
Implement dynamic, layered authentication using:			
• Passwords/passcodes	Yes	No	Unsure
• Biometrics	Yes	No	Unsure
• Tokenization	Yes	No	Unsure
Use centralized technology that integrates vendor tools through configurable workflows?	Yes	No	Unsure
Partner with vendors offering immersive fraud monitoring services (e.g., dark web, SSN, address change monitoring)?	Yes	No	Unsure
Invest in fraud detection tools that catch and report potentially counterfeit checks at deposit?	Yes	No	Unsure

Review your responses to identify
areas of confidence and those
needing further investigation.

For more risk education, visit:
alliedsolutions.net/resources