Preventing Account Takeover (ATO) Fraud

Below is a checklist of items and topics you may consider when reviewing your procedures and operational controls related to preventing account takeover ("ATO") fraud. The list is not exhaustive; we do not warrant its accuracy and alignment with all current legal and regulatory standards and it should not be relied upon as a formal decision-making document.

1. Account Holder Education & Awareness

- ☐ Accountholder communications warn about phishing, vishing, and smishing scams
- ☐ Educational materials provided: in branch, statements, email alerts, website, in-app notifications
- ☐ Guidance on creating strong, unique passwords
- ☐ Instructions not to share OTPs, PINs, or security codes

2. Multi-Factor Authentication (MFA)

- ☐ MFA required for all online banking logins
- ☐ Dynamic MFA methods implemented (push notifications, biometrics)
- ☐ Re-authentication required for high-risk transactions
- ☐ Exceptions to MFA are documented and justified

3. Login & Session Controls

- ☐ Monitoring for unusual login locations, IPs, or device fingerprints
- ☐ Alerts sent for new device or location logins
- ☐ Simultaneous session limits enforced
- ☐ Session timeouts for inactivity applied

4. Transaction Monitoring & Velocity Controls

- ☐ Thresholds set for transaction amounts, frequency, and destinations
- ☐ Suspicious or high-risk transactions flagged for manual review
- ☐ Behavioral analytics detect unusual account activity
- ☐ Alerts generated for sudden changes in transaction patterns

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.

5. Outbound Funds Verification

- ☐ Additional verification for large/unusual wires or ACH transfers
- ☐ Call-back verification to a trusted phone number
- ☐ Secondary authentication via mobile app or token
- ☐ Delayed processing applied for suspicious transfers

6. Account Recovery & Fraud Response

- ☐ Procedures in place to freeze accounts when fraud is suspected
- ☐ Rapid investigation and reversal of unauthorized transactions
- ☐ Dedicated fraud hotline for accountholders
- ☐ Incident documentation maintained for trend analysis and compliance

7. Device & Endpoint Security

- ☐ Accountholders encouraged to use up-to-date browsers and devices
- ☐ Access blocked from devices with known malware or unusual configuration
- ☐ Secure mobile banking apps with biometric login and encryption

8. Internal Controls & Staff Training

- ☐ Staff trained to recognize social engineering attempts
- ☐ Escalation protocols for suspicious accountholder-reported activity
- ☐ Regular review and update of fraud detection rules

9. Collaboration & External Resources

- ☐ Subscribed to shared fraud intelligence networks (e.g., FS-ISAC, Nacha)
- ☐ Fraud trends reported to regulators and law enforcement as required
- ☐ Third-party fraud prevention tools utilized for layered defense
- ☐ Name matching utilized, such as Advanced Fraud Solutions (AFS) TrueACH
- ☐ Visit Allied Solutions Fraud Prevention Center

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.