

# ACCOUNT TAKEOVER FRAUD LIFECYCLE

Understanding the account takeover fraud lifecycle allows financial institutions to better prevent and detect it. The lifecycle, summarized below, has three distinct phases:



## Harvest Phase

Storing and retrieving credentials and sensitive Personally Identifiable Information (PII).

- **Betrayal of Trust:** Impersonation Scams
- **Direct Deception:** Phishing, Smishing and Vishing
- **Indirect Deception:** Fake Websites and Apps
- **Malicious Software:** Malware and Keyloggers
- **Outside Threats:** Third-Party Breaches and Public Data



## Access Phase

Gaining entry, gathering intelligence and establishing control over victim accounts using automated tools, social engineering tactics, and strategic manipulation.

- **Initial Access:** Credential Stuffing, SIM Swapping
- **Reconnaissance:** Check Balances, Review Spending/Deposit Patterns, Identify Transaction Limits
- **Lockout:** Secure the Profile, Initiate Account Detail Changes, Lock Out Account Holder



## Monetize Phase

Seizing control and turning the account into a source of revenue.

- **Unauthorized Transactions:** Wire Transfers, Online Purchases, Moving Funds Between Accounts
- **Account Linking:** Connect Compromised Account to Other Accounts or Wallets
- **Mimicking Normal Behavior:** Stay Within Normal Transaction Patterns, Avoids Triggering Alerts, The Most Challenging to Detect

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, use of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.