ACCOUNT TAKEOVER FRAUD SCENARIO: DATA BREACH + BANK IMPOSTOR SCAM

Scenario Overview

A large e-commerce retailer experiences a data breach. Criminals use automated tools to test the validity of leaked credentials on thousands of different financial institutions' online banking portals. When a valid credential combination is attempted at ABC Bank, it triggers a one-time password (OTP) to authenticate account holder access. The criminal then socially engineers the victim to solicit the OTP, gaining access to her account.

Let's take a more detailed look at what happened in this scenario:

DATA BREACH ENABLES CREDENTIAL STUFFING

1. A large e-commerce retailer experiences a data breach. Millions of username/password combinations and personally identifiable information (PII) are exposed.

2. Months later, a criminal purchases the breached data on the dark web. Using automated tools, the criminal tests the stolen email-password combinations on thousands of online banking portals, looking to exploit instances where victims reused passwords for their online banking.

3. The criminal finds a valid login using Lucy's credentials at ABC Bank. The attempt to log in to Lucy's account triggers a multi-factor authentication (MFA) request from the financial institution because a new phone was detected.

4. By triggering an MFA request, the criminal confirms that Lucy has an account at ABC Bank.

BANK IMPOSTOR SCAM USED TO COMPLETE ACCOUNT TAKEOVER

5. The criminal devises a scam to deceive Lucy into providing her OTP.

6. The criminal attempts to log in to Lucy's account. He knows that it will trigger an OTP request. The criminal calls Lucy pretending to be from the fraud department at ABC Bank.

7. Lucy answers. The criminal correctly states Lucy's full name and date of birth. He tells her that there has been some suspicious activity on her account. He asks her to secure the account by providing the OTP just sent to her.

8. Concerned about protecting her account, Lucy provides the OTP to the criminal.

9. The criminal enters Lucy's account and adds his device as a trusted device. He also changes the email address associated with the account and resets the password.

10. The criminal then initiates a $10,000 wire transfer to an account he controls.

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, utilization 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.