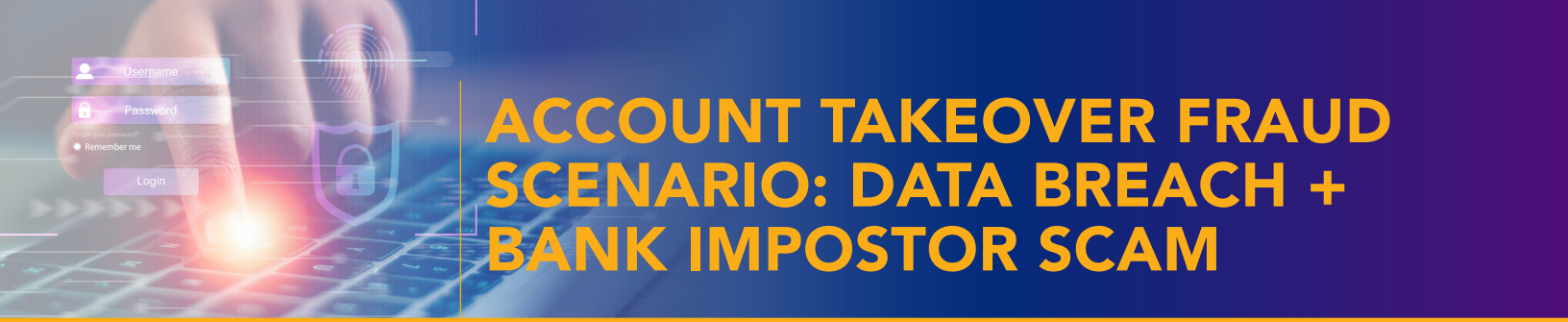




# ACCOUNT TAKEOVER FRAUD SCENARIO: DATA BREACH + BANK IMPOSTOR SCAM

## Scenario Overview

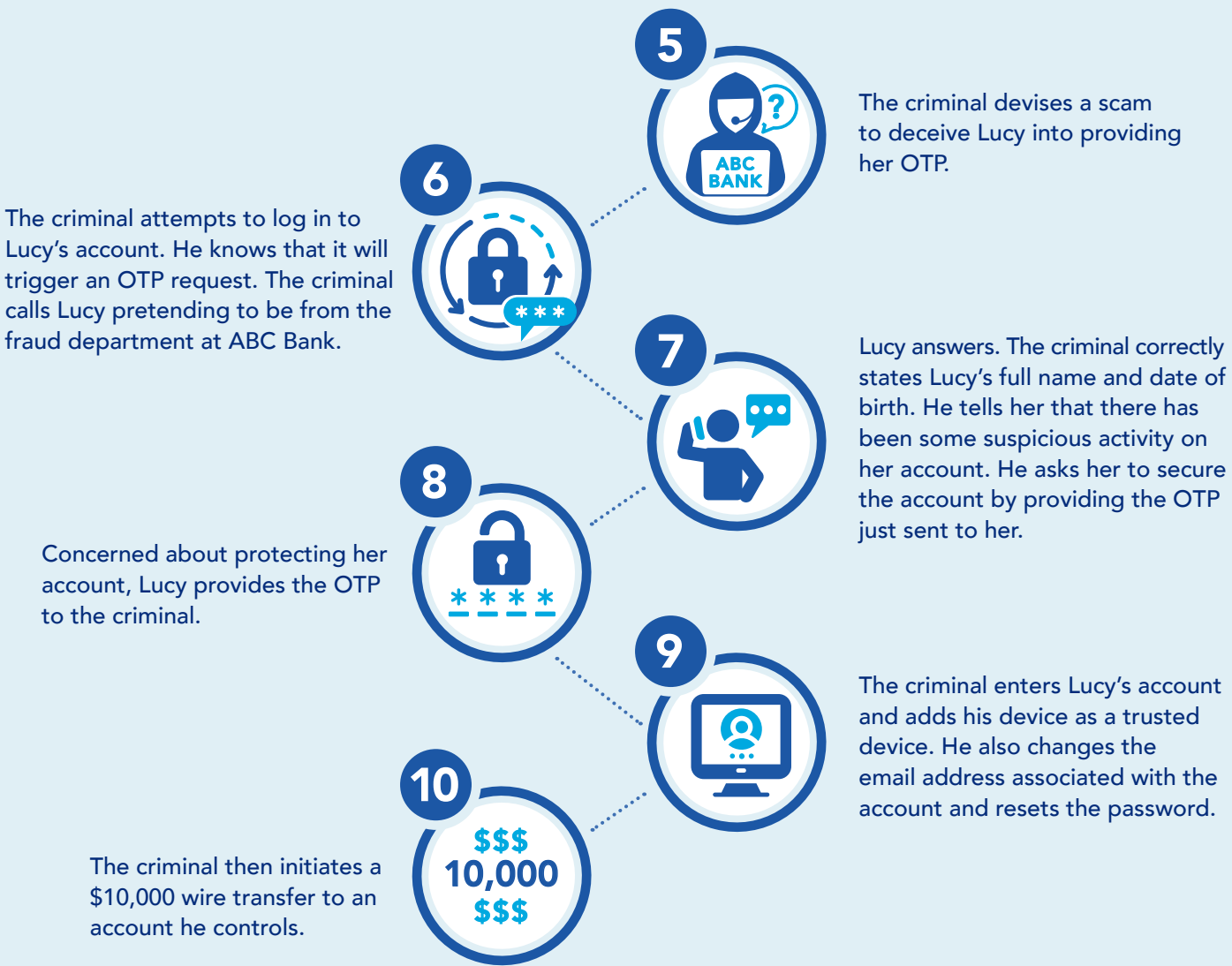
A large e-commerce retailer experiences a data breach. Criminals use automated tools to test the validity of leaked credentials on thousands of different financial institutions’ online banking portals. When a valid credential combination is attempted at ABC Bank, it triggers a one-time password (OTP) 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



### BANK IMPOSTOR SCAM USED TO COMPLETE ACCOUNT TAKEOVER



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.