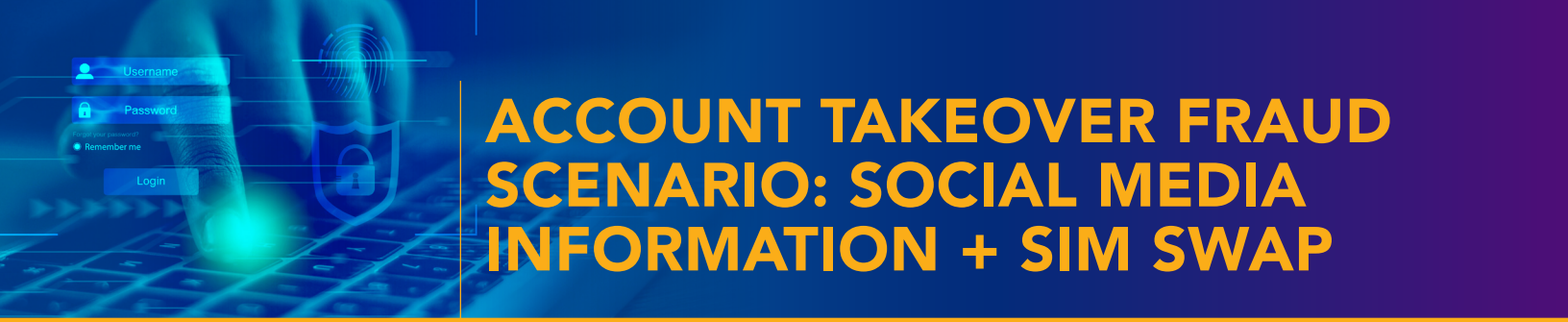




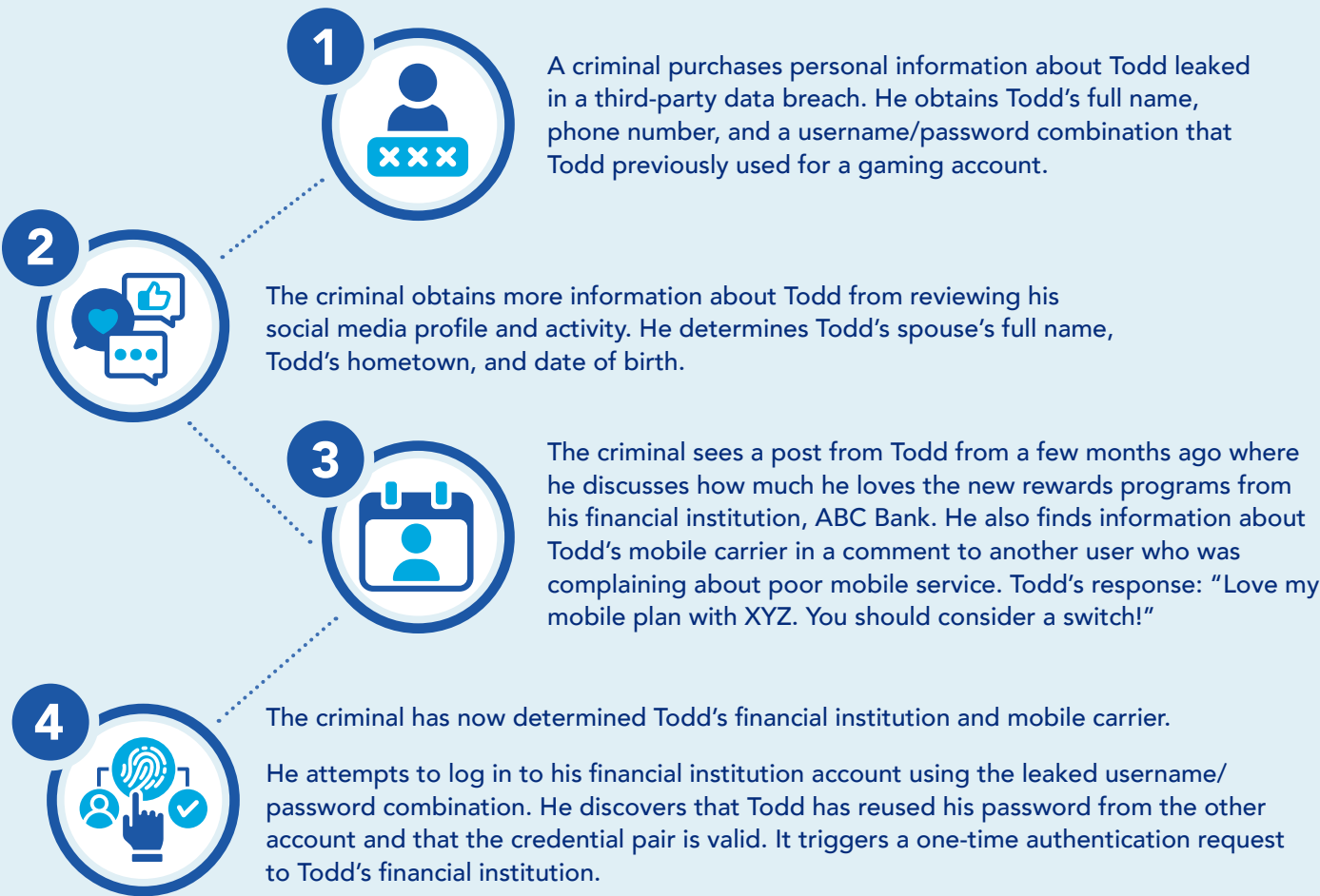
ACCOUNT TAKEOVER FRAUD SCENARIO: SOCIAL MEDIA INFORMATION + SIM SWAP

Scenario Overview

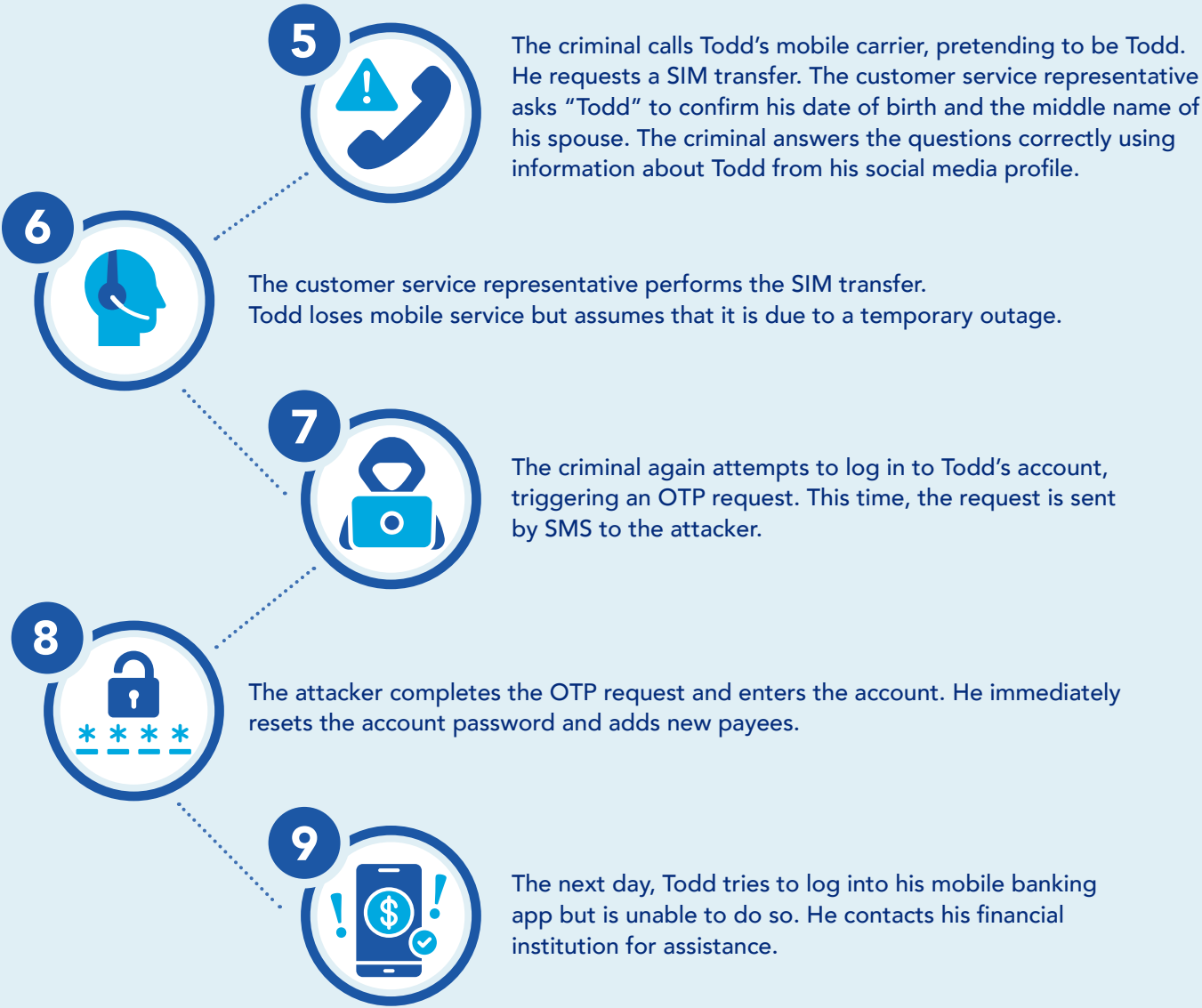
In this scenario, a criminal exploits personal information that Todd shared on social media to determine his mobile carrier and financial institution. The criminal uses this information to socially engineer a customer service representative at a mobile carrier to take control of Todd's phone number, allowing the attacker to complete the financial institution's SMS-based authentication.

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

SOCIAL MEDIA PROFILE IS USED FOR HARVESTING



SOCIAL ENGINEERING ENABLES SIM SWAP



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.