SCAM SCENARIO:BANK IMPOSTOR

SCAM SCENARIO: BANK IMPOSTOR



An individual receives a phone call from someone pretending to be from her financial institution, who states that her account has been compromised and she needs to take steps to protect it.

In order to "protect" the account, the caller asks the customer to verify her online banking credentials, obtain a one-time verification passcode, and provide this code during the phone call with the "financial institution."



After the call, the customer is unable to access her account using online banking and contacts her financial institution. A representative from the real financial institution said they did not call the customer and multiple payments for \$9,500 were sent from the account that day. The customer confirms she did not authorize these payments.

CLASSIFICATION: SCAM

UNAUTHORIZED PAYMENT

RELATIONSHIP AND TRUST

BANK IMPOSTOR



The scams 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.