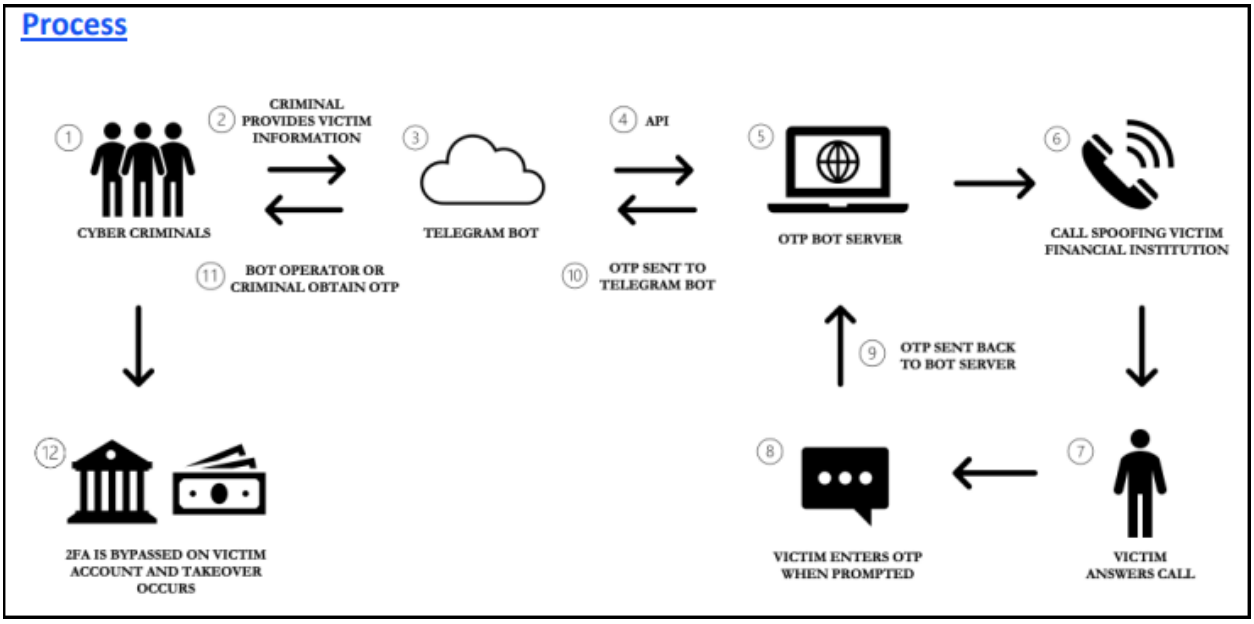
OBA FRAUD ALERT
ACCOUNT TAKEOVER/MOBILE WALLET FRAUD HITTING BANKS HARD

One-time password (OTP) bots are a form of crimeware-as-a-service that are used to bypass two-factor authentication (2FA) on victim accounts with the intention to commit account takeovers. Scammers are increasing their use of OTP bots to commit account takeover and mobile wallet fraud. The attacks we are aware of are targeting consumer BINs.

The bots facilitate a spoofed phone call impersonating a victim's financial institution, typically claiming that there is potential fraud on the account that needs to be verified and disputed. During the call, the bot deceives the victim into divulging their OTP, which is then passed back to the bad actor and ultimately input in conjunction with the email and password of the victim to gain access and take over the victim's account.



1) A bad actor obtains victim account login credentials and PII (including their phone number);
2) The bad actor then provides the victim's phone number and name to the OTP Bot of their choice to facilitate the call;
3) The OTP Bot makes a call impersonating the victims financial institution using the Telegram API to solicit their OTP;
4) While the bot is making the call, the bad actor is actively logging into the financial institution's website using the victim's credentials;

5) **If** the victim answers the call and provides their OTP, the OTP is sent back through the bot server to the bad actor who then uses it to successfully access the victim's account.

Before your bank customers get attacked with these calls, here's a few suggestions for pre-attack mitigation and post-attack triage! Yes, multiple banks in Oklahoma have been targeted recently. Loss per card/account can exceed $10,000 per day. So far, the ATMs used outside the state of Oklahoma are all Chase owned/located machines. CrimeDex alerts from around the country have stated the scammers may also use the tap-2-pay feature at retail stores for pre-paid card purchases, USPS stores for money orders, or online merchants for card-not-present sales.

Pre-Attack Mitigation Considerations:

- Educate your customers. The Banks Never Ask That campaign is easy to link to Protect Yourself - Banks Never Ask That!
- Educate your employees responsible for in-bound customer calls so they can notify fraud/security of any increase in phone calls regarding phishing or higher value unauthorized card transactions
- Raise the risk score or block digital wallet ATM transactions outside your customer footprint
- Raise the risk score (greater than 35 was suggested) for all Visa 3-D Secure or Mastercard SecureCode transactions
- Suspend or remove the PIN change feature on your online banking app
- Suspend or remove phone number change feature on your online banking app
- Disable push provisions on your online banking app
- Review your customer authentication processes for in-bound calls that request a change for PIN, phone number, or online banking app password
- Review daily logs of customer phone number changes – does the new number make sense i.e. changed from AC 580 to AC 645 (FL)
- Review daily logs for daily card limit increase requests – if the increase is requested via online banking channels, check the IP address used to submit the request
- Have a prepared Response Action Plan in place that is developed with your vendors so you know ahead of time what the vendor can assist with and what they can't
- Ensure your cyber insurance policy covers this type of event

Post-Attack Mitigation Considerations:

- Close any affected card
- Temporarily suspend customer online banking services for affected customers
- Close any accounts whose information may have been compromised by fraudulent online banking access
- Affected customers should have their devices checked for malware
- Block all digital wallet transactions outside your customer footprint
- Block all digital wallet ATM transactions
- Block all NICE network transactions outside your main customer base area
- Temporarily suspend P2P services on your online banking app
- Query card transaction logs for any other transactions conducted at the same terminals or if unique, the same geographic area. For example: Plantation FL. Then take pro-active loss mitigation measures on additional cards found