

Institution _____

Date of Exam _____

Charter# _____

OFFICER’S QUESTIONNAIRE - ACCOUNT TAKEOVER RISK

Instructions for Completing the Questionnaire

The Officer’s Questionnaire - Account Takeover Risk (Questionnaire) contains questions covering significant areas of the Texas Bankers Electronic Crimes Task Force *Best Practices for Reducing the Risk of Corporate Account Takeover* (Best Practices). Your responses to these questions will help determine the scope of the examination; provide insight into the composition of the institution’s account takeover (ATO) risk management program; and may be relied upon to form conclusions as to the condition of the institution’s ATO program. Therefore, accurate and timely completion of the Questionnaire is expected. Examiners may request additional supporting documentation to assess the validity of the answers that are provided and to further assess the quality and content of the financial institution’s ATO program. At the bottom of this page is a signature block, which must be signed by an executive officer attesting to the accuracy and completeness of all provided information.

Please answer the questions as of the pre-determined examination date. The majority of the questions require only a “Yes” or “No” response; however, you are encouraged to expand or clarify any response as needed directly after each question or after each section in the “Clarifying or Additional Comments” area. Please do not leave blank responses.

Many questions contain a reference to the FFIEC’s *Supplement to Authentication in an Internet Banking Environment* (FFIEC Supplemental Guidance) and the Best Practices help document that may aid you in completing the Questionnaire. Please note that these references may not encompass the entirety of the published information.

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.		
Officer’s Name and Title	Institution’s Name and Location	
Officer’s Signature	Date Signed	As of Date
This is an official document. Any false information contained in it may be grounds for prosecution and may be punishable by fine or imprisonment.		

PART 1: PROTECT: Bank Awareness, Services Offered and Risk Profile

To help us assess your awareness of account takeover risk, the types of electronic banking services you offer, and your risk profile, please answer the following questions. Tools and resources are available at www.ectf.dob.texas.gov to assist your institution in implementing a strong ATO Protection program.

YES	NO	
		a) Does your institution have any customers that use Internet Banking or cash management systems for ACH origination, outgoing wire transfer requests, external funds transfers, or person-to-person pay? If "No", you have finished completing the questionnaire.
		b) Has enhanced authentication or layered security for consumer as well as business accounts been implemented? (<i>FFEIC Supplement to Authentication in an Internet Banking Environment</i>)
		If "No", do you have plans to implement enhanced authentication or layered security?
		Describe authentication methods implemented or planned. (Include both manual and automated methods.)
		c) Has the Board been informed of the issues surrounding ATO?
		If "Yes", please provide the date that ATO was last discussed and reviewed by the Board of Directors:
		d) Have corporate on-line banking customers been educated on <u>basic</u> online security practices? [<i>FFEIC Supplement to Authentication in an Internet Banking Environment, Best Practices P4</i>]
		e) Has advanced security awareness education been provided to retail and high risk customers through a website, personal contacts, group meetings, or other methods? [<i>Best Practices P5</i>]
		f) Are signed written agreements in place with corporate customers using Internet Banking services? [<i>Best Practices P7</i>]
		g) Has your institution contacted vendors to receive information regarding reducing the risk of ATO? [<i>Best Practices P8</i>]

Clarifying or Additional Comments:

Part II. DETECT: Monitoring Systems, Employee Awareness, Notifications From Customers

To help us assess your ability to detect electronic theft through monitoring systems, employee awareness, and notifications from customers, please answer the following questions.

YES	NO	
		a) Have automated or manual monitoring systems been established? [<i>FFEIC Supplement to Authentication in an Internet Banking Environment, Best Practices D1</i>]
		Please indicate the anomaly detection methods the bank uses:
		b) Have bank employees been educated on ATO warning signs? [<i>Best Practices D2</i>]
		If "Yes", please indicate the last date training was provided:
		c) Have account holders been educated on the warning signs of a potentially compromised computer system and fraudulent account activity? [<i>FFEIC Supplement to Authentication in an Internet Banking Environment, Best Practices D3</i>]
Clarifying or Additional Comments:		

Part III. RESPOND: Incident Response and Notification

To help us assess your incident response plans and procedures, please answer the following questions.

YES	NO	
		a) Describe methods the bank would use to contact customer in the event of a suspected fraudulent activity:
		b) Does your ATO program contain formal policies, procedures and guidelines for the following:
		1. Immediately reverse fraudulent transactions? [<i>Best Practices R5</i>]
		2. Notification of the receiving bank(s)? [<i>Best Practices R5</i>]

Part III. RESPOND: Incident Response and Notification

To help us assess your incident response plans and procedures, please answer the following questions.

YES	NO	
		3. Suspension any compromised systems? [<i>Best Practices R5</i>]
		4. Contingency plan to recover or suspend compromised systems? [<i>Best Practices R6</i>]
		5. Contacting law enforcement and regulatory agencies? [<i>Best Practices R7</i>]
		6. Customer relations and documentation of recovery efforts? [<i>Best Practices R8</i>]

Clarifying or Additional Comments:

Part IV. Previous Incident(s)

YES	NO	
		a) Have any of the institution's customers been victim to an account takeover or attempted takeover?
		b) If "Yes", was a SAR filed? A SAR must be filed on any ATO theft or attempted theft (past, present, or future) per <u>FinCEN Advisory 2011-A016</u> issued December 19, 2011.

Clarifying or Additional Comments: