COMMERCIAL ONLINE BANKING SERVICES RISK ASSESSMENT AND CONTROLS EVALUATION

The Federal Financial Institutions Examination Council (FFIEC) has suggested that commercial online banking customers perform a related risk assessment and controls evaluation periodically. We are providing a template for your business to complete as an exercise to ensure optimal security is in place. Please go through and complete the following steps. Note that the yellow highlighted areas of the risk assessment need to be customized according to your business environment.

1. Page 2 - Fill out the Date, Responsibility and Business Name/Location fields. The Data Type is pre-populated for you.

2. Page 2 - Select in the Residual Risk box either Acceptable or Unacceptable risk. This indicates whether you have unmanaged risks in your internet banking environment that need additional controls.

3. Page 2 - Please select all the services that are used with your financial institution's Internet banking account that apply in the Internet Based Financial Transaction Types box.

4. Page 3 - Select all of the controls that apply to your business in the Controls in place to Prevent and Detect Fraud box.

5. Page 3 - Fill out your business' name in the Testing Methods, Frequency and Controls Issues box.

6. Page 4 - Complete the Recommendations/Strategy to Mitigate Residual Risk box if applicable. For example type, (P) Dedicated PC utilized for online banking services (not utilized for web browsing, emails and social networking).

Date: _____

Data Type (Physical and/or Electronic): *Electronic*

Responsibility: _____

Business Name/Location: _____

Loss of financial transaction data and personally identifiable information (PII) is an inherent risk of using Internet based banking services. Protecting the confidentiality, integrity and security of financial services transactions is shared by the financial institution and the business entity. This Risk Assessment outlines the recommended security controls essential to minimizing the risk of these transactions for the business entity.

Likelihood of Occurrence		Potential Damage		Inherent Risk		Residual Risk	
How likely is this threat to occur (without appropriate security controls in place)?	**Medium**	If the threat resulted in a security breach what kind of damage would result?	**Loss of funds, Identity Theft**	Likelihood of occurrence X Potential Damage	**Medium**	Remaining Risk- acceptable or unacceptable (unmanaged risk). Explain detail in mitigation strategy.	Acceptable or Unacceptable

Internet Based Financial Transaction Types				
ACH Transfers	**Wire Transfers**	**Mobile Banking**	**Remote Deposit Capture**	**Other**

Reasonably Foreseeable Internal and External Threats and Vulnerabilities to the Information Asset
Cyber-criminal attacks such as phishing, social engineering, interception of transaction data, stolen data, resulting in corporate account takeover and identity theft

Controls in place to (P)revent and (D)etect Fraud

(P) Business employees educated on use of application(s), IT security standards and best practices, common fraud schemes and procedures for contacting the FI in case of suspected security incident

(P) Segregation of Duties; separate approval process; dual control utilizing two separate PCs.

(P) (D) Real-time anti-virus and anti-spyware, desktop firewall, malware detection and removal software w/automatic updates and scheduled scans

(P) PC not used to surf the web or email

(P) Procedures for logging off and leaving online banking PC unattended or not in use

(P) Spam filters in place and updated

(P) Mgr. to understand responsibilities and liabilities per account agreement

(D) Monitor and reconcile accounts daily

(D) Discuss the options offered by the FI to detect or prevent out-of-pattern activity

(D) Note any changes in PC performance

(D) Pay attention to warnings

(D) Be on the alert for rogue emails

Testing Methods, Frequency and Control Issues

Financial Institution will conduct periodic analysis of the controls: or Internal analysis of the fraud controls will be conducted by

_____.

Business Name Here/ Acknowledgement Signature

Recommendations/Strategy to Mitigate Residual Risk