

## NEW AND/OR CHANGE OF INFORMATION ASSET RISK ANALYSIS WORKSHEET

\* To be completed if new information assets and/or changes are considered to an existing information asset, prior to annual update to risk assessment process.

\*\* Complete the following to be transferred to each corresponding column in the ABRA Matrix. The completed RAW should then be retained with the completed Functional Area Worksheets.

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

Date: 8/1/2011

Data Type (Physical and/or Electronic):

Electronic

Responsibility:

Network Administration

### New Asset and/or Change in Existing Asset

Commercial Online Banking Services (JHA Netteller)

### Reasonably Foreseeable Internal and External Threats and Vulnerabilities to the Information Asset

Unauthorized access and disclosure potentially resulting in financial loss, loss of data integrity and confidentiality, resulting from malware, viruses, sharing of login credentials and social engineering attacks.

\*Using the above key, complete the following risk ratings:

Likelihood of Occurrence	Description of Security Controls (A) Administrative (T) Technical/Logical (P) Physical and Disposal/Retention Methods
Medium	(A)(T) Username and password required. (A)(T) Funds Transfer report viewed daily. (A)(T) Automated anomaly detection software in place. (A)(T) Customer locked out after three invalid login attempts. (A)(T) Password reset every 90 days. (A)(T) Automatic logout after five minutes of inactivity. (A)(T) Multifactor authentication: image confirmation and/or security question. (A)(T) Challenge questions contain "out of pocket" information (A)(T) Bank Administrators are unable to access customer passwords, multifactor answers or challenge question answers. If a customer forgets his/her credentials, an administrator enters a temporary one that the customer is required to change the next time they access commercial online banking. (A)(T) Customer ACH and Wire transaction limits are approved by Loan Officers and may not exceed these amounts. Bill Pay limits are fixed for all customers unless a higher limit is authorized by FI management. (A) (T) Dual authorization is required for account transfers and ACH and Wire initiations. (A)(T) Customers participate in a online educational course on the risks of online banking and how they can protect their business. (A) Network Administration is responsible for keeping up with new risks and vulnerabilities and other security issues related to Commercial Online Banking and will update the risk assessment accordingly.
Potential Damage to the FI	
Major	
Overall Risk	
Medium	
Residual Risk	
Acceptable	

### Testing Methods, Frequency and Control Issues

Utilize future audits to test for vulnerabilities.

### Recommendations/Strategy to Mitigate Residual Risk

Internet Banking Service Provider (JHA) is in process of assessing layered security controls against the 2011 FFIEC Authentication Guidance Objectives. Status update is expected by 1/1/2012. (See communication document)