

### Multi-Factor Risk Assessment

Site Name:

Software Product:

Site Location:

Date of Review:

#### **Purpose:**

Identify high-Risk transactions that may require multi-factor authentication.

Existing authentication methodologies involve three basic “factors”:

- Something the user knows (e.g. password, PIN);
- Something the user has (e.g. ATM card, smart card); and
- Something the user is (e.g. biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include “out-of-band” controls for risk mitigation.

#### **Objectives:**

Use of the risk assessment methodology to identify those areas of the application that are of high risk and may require a multi-factor authentication strategy.

Compliance with the FFIEC’s Guidance document “Authentication in an Internet Environment”.

### Multiple-Factor Authentication Methodologies:

As described previous, there are several approaches to adding factors to the authentication process. Biometric methods provide a high level of certainty, but at a cost, and presumably would only be used in situations where the identified risk justified the cost. However, for banks, which require their Internet banking clients to be existing customers, and can initially authenticate the user with certainty, the use of an additional piece of information in addition to the logon ID and password would qualify as a multiple-factor authentication method and the cost would be reasonable. Answers to several security questions could be obtained during the initial authentication session for Internet banking. Examples of this "shared secret" could be:

- City of your birth
- Name of the First School attended
- Name of favorite High School teacher
- Name of a pet
- Mother's maiden name
- Fathers middle name

These questions could be presented at logon or when a customer attempts to execute a high risk transaction type. They can be rotated so that a different question is asked at each logon authentication procedure.

## Table of Contents

1. Application Description: .....	4
2. Identification of Transaction Types: .....	4
3. High Dollar Transaction Amounts .....	5
4. Customer Awareness: .....	5
5. Customer Typing: .....	6
6. Transaction Impact: .....	6

### 1. Application Description:

Provide an overview of the application description. Include customers, customer types, where the application is housed, and data flow between customers, application, and institution.

### 2. Identification of Transaction Types:

The risk assessment needs to identify the various levels of risk to a financial institution presented by individual transaction types. A sample matrix risk assessment is presented below.

Example:

<b>Transaction Type</b>	<b>Risk</b>	<b>Authentication Method Used</b>	<b>Additional Measures</b>
Balance Inquiry	Low	Single-Factor	None
Change in customer information	High	Multiple-Factor	Email notification that a change has been made and /or mailed notification to the client.
Bill Payment	High	Multiple-Factor	Activity reflected on monthly statement
Change in Bill Payment information	High	Multiple-Factor	Email notification that a change has been made.
Addition of Re-occurring payment to a Vendor	High	Multiple-Factor	Email notification that a change has been made.
Wire Transfer of Funds	High	Multiple-Factor	Email notification that a change has been made.
Transfer of Funds between client accounts	High	Multiple-Factor	Email notification that a change has been made.
Loan Origination	High	Multiple-Factor	Email notification that a change has been made.

Please complete the risk assessment for the various transaction types that you process:

Transaction Type	Risk	Authentication Method Used	Additional Measures

### 3. High Dollar Transaction Amounts

Do high dollar transactions require a second authentication factor?    What is the amount at which a second authentication factor is required?

### 4. Customer Awareness:

Financial institutions should also be able to demonstrate to an examiner their efforts in educating Internet banking customers on the risks. They should also be able to identify controls that have been put in place to mitigate those risks. The education and information presented to the customer could include:

- Informing them that writing down passwords is not advisable.
- Changing passwords on a frequent basis will decrease the likelihood the password is compromised.
- Sharing passwords with anyone is not a good idea.
- Reviewing monthly statements for account activity prior to the expiration of the review period for non-authorized transactions is their responsibility.

Has a customer awareness program been created for application?

### **5. Customer Typing:**

Do retail and commercial customers have different authentication requirements?  
(Large Dollar commercial transactions should require multiple employees and two-factor authentication)

### **6. Transaction Impact:**

How many "High Risk Transactions" transactions are processed per day? Would two factor authentication for each high risk transaction impact customer service?