OMB Control No. 3064-0198
Expiration Date: March 31, 2021

Topics for Presentations and Discussions

at the FFIEC 2020 Authentication Forum

The FFIEC is interested in presentations and discussion on the below customer and employee authentication topics.

PRA Burden Statement

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number. The FFIEC 2020 Authentication Forum constitutes a collection of information under the Paperwork Reduction Act which has been cleared by OMB under Control Number 3064-0198 (expiration date March 31, 2021). Public reporting burden for this information collection is estimated to average 6 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and reviewing and completing the information collection. You can send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing the burden, to the Paperwork Reduction Act Clearance Officer, Legal Division, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429; and to the Office of Management and Budget, Paperwork Reduction Project (Re: Control Number 3064-0198), Washington DC 20503.

Part 1. Customer Authentication Topics

The topics in Part 1 each relate to electronic banking services accessible by consumer and business customers by means of a smart phone, Internet banking or other electronic channel. The topics are focused on authentication practices for customers that have previously been identity proofed. These topics do not relate to customer identity proofing or verification (e.g. know your customer) as part of the account-opening process.

1. *Views on Current FFIEC Guidance on Customer Authentication*. Discuss aspects of the current FFIEC authentication guidance that could be updated or changed to better reflect current risks and authentication controls.

2. *Trends in Customer Account Compromise*.

    a) *Trends.* Identify current trends in the compromise of authentication controls for consumer and business customer accounts. Consider emerging hacking/compromise trends/risks.

    b) *Credential Stuffing Attacks*. Identify reasons financial institutions' information systems and authentication controls have not been successful in safeguarding against credential stuffing attacks.

- o For example, discuss why layered security controls have not been effective against some publicly-known credential stuffing attacks.
- o Identify any authentication controls that can better protect against credential stuffing attacks.

c) *Business Email Compromise (BEC)*. Identify customer authentication controls that can more effectively address BEC hacking/compromise risk. Discuss to what degree the risk of account compromise is related to the customer, as opposed to the authentication control implemented by the financial institution.

d) *Social Engineering Based Attacks*. Identify customer authentication controls that have been reported as effective against social engineering based attacks.

e) *Metrics*. Identify metrics that financial institutions or trade associations have regarding trends (e.g. volume of incidents, losses, etc.) of attempted and successful attacks on authentication controls for electronic banking services. Discuss if these metrics are viewed as informative for future trends in losses and attacks.

3. *Current Authentication Controls*.

a) *General*. Identify authentication controls for consumer and business accounts that are now viewed as industry standard practices. Distinguish between (i) controls that uniquely authenticate the customer (such as biometrics) and (ii) controls or layered security that reduce fraud but do not uniquely identify the customer (such as geo-location).

b) *Perimeter versus Risk-Level Authentication*. Identify trends and relative merits of single authentication control at the perimeter entry to electronic banking services, as opposed to secondary authentication controls when customer seeks to execute a high dollar transaction.

c) *Role of Two Factor Authentication (aka MFA) in Electronic Banking*. Identify current and future role for implementing two factor authentication in electronic banking authentication.

- o Consider the benefits and challenges from business, technology or customer experience perspective associated with two factor authentication.
- o Discuss if there are any lingering technical or adoption impediments to financial institutions implementing two factor authentication with customers? For any impediments identified, discuss whether or not there are possible solutions on the horizon.

d) *SMS Messages in Customer Authentication*. Identify trends in security and compromise threats for SMS messaging used as part of customer authentication. Discuss whether these threats limit SMS messaging as an effective customer authentication control. Consider NIST and FTC statements regarding the deprecation of SMS messaging as authentication factor.

e) *SMS Alternative – Use of One Time Passcodes Via Secure Application to Satisfy Two Factor Authentication*. Address the prevalence/trend of financial institutions offering consumer and business customers the option to authenticate with one time passcodes

(OTP) via a secure application as one of two factors for MFA. Consider security risks, consumer acceptance, and operational/implementation issues associated with OTP via secure application.

f) *Challenge Questions and Other Low Reliability Controls*. Address the current use of challenge-response questions as an authentication factor. Consider whether this approach or other authentication controls are viewed by industry as having a low reliability.

g) *Device Authentication and Device Fingerprinting*. Comment on similarities and differences between device or machine to machine authentication and device finger-printing.

4. *Emerging Authentication Controls*. Identify emerging authentication controls implemented at some financial institutions, but which are not yet wide-spread in the industry.

5. *New Payment Services Impact on Customer Authentication*. Identify impacts on customer authentication risks and controls arising from new developments in payment systems, such as the use of mobile phone payments and real time P2P payments.

6. *Non-Bank Payment Companies*. Discuss whether non-bank payment companies (such as P2P wallet companies) offer the same security level for customer authentication, as required for banks under current FFIEC guidance. Consider similar or different risks for banks and non-bank payment companies.

7. *Impact of Consumer Permissioned Parties*. Discuss the impact of data aggregators and consumer permissioned parties (CPP) on financial institutions' authentication risks and controls. Address impact on both on financial institutions and their consumer customers.
   - Identify if and how authentication at the financial institution may impact a consumer's ability to access or share his or her data by means of a CPP/data aggregator.
   - Address authentication challenges in the context of (i) the data screen scraping process, and (ii) the process under a data sharing agreement with a financial institution. For example, discuss how CPPs/data aggregators navigate MFA controls at the financial institution.
   - Discuss how the authentication for customers, CPP/data aggregators and financial institutions is managed through application programming interfaces (APIs).
   - Discuss authentications controls being employed by CPP/data aggregator when a customer accesses data stored at the CPP/data aggregator which was previously downloaded from a financial institution.
   - Discuss if CPPs/data aggregators impose customer authentication standards on downstream entities that may subsequently access customer data derived from financial institutions.

   [*Note: Please limit presentations on this topic to issues associated with technology authentication risks and controls. This project is not considering or addressing other issues associated with consumer permissioned parties or open banking, such as customer agency authority, liability allocations, data quality, or Bank Service Company Act, etc.*]

8. *Regulatory Trends*. Discuss the impact of new laws and regulations on financial institutions' implementation of customer authentication controls, from both a potential liability perspective and minimum standards perspective. Possible topics include, the EU's General Data Protection

Regulation (GSPR), the California Consumer Privacy Act, NY Cyber Regulations, Consumer Financial Protection Act Section 1033, and the FTC Proposed Amendments to its Safeguards Rule.

9. *Experience with Strong Customer Authentication under European Union PSD2*. Discuss EU banks' experience with the implementation of EU Payment Services Directive #2 (PSD2) requirement for "strong customer authentication." Consider customer experience, implementation cost, complexity and fraud loss reduction for financial institutions operating in the EU.

10. *Role of Service Providers*. Identify unique customer authentication issues that regional banks, community banks, and credit unions may have as a result of the use of a third party service provider to support customer authentication for electronic banking.
    - Discuss whether service providers provide customer authentication options for different types of customers and/or business lines.

Part 2. Financial Institution Employee Authentication

1. *General*. Identify industry standard and emerging authentication factors/tools that financial institutions utilize for their employees.

2. *Comparison with Customer Authentication*. Discuss similarities and differences in authentication standards and technologies used for financial institution employees, as compared to customers.

3. *Remote Access.* Identify unique or enhanced authentication factors/tools for employee authentication when remotely (offsite) accessing financial institution networks.

4. *Privileged Access*. Identify unique or enhanced authentication factors/tools for privileged employee access. Consider types of positions that typically require stronger authentication. Discuss whether or not financial institutions are using NIST/NCCoE guidance specifically for financial institutions' access rights management (SP 1800-9, Privileged Account Management SP 1800-18).

5. *Trends in Compromise of Employee Access*. Discuss typical and emerging threats targeting financial institutions' employees' access.

Part 3. Authentication of Third Party Access

1. *General*. Identify industry standard and emerging authentication factors/tools utilized by financial institutions for permitting third party service providers to access financial institutions' managed systems.

2. *Comparison with Customer Authentication*. Discuss and compare authentication factors/tools used for third party access with those factors/tools used for financial institution customers and/or employees.

3. *Trusted Connections*. Discuss circumstances under which financial institutions utilize trusted connections for third party service providers. Consider the impact of a trusted connection on a financial institution's authentication expectations for a third party service provider.