Proposal: 1670 - Federal Reserve Actions to Support Interbank Settlement of Faster Payments
Description:

Comment ID: 136970
From: Bottomline Technologies, Mark Ranta, CTP
Proposal: 1670 - Federal Reserve Actions to Support Interbank Settlement of Faster Payments
Subject: Federal Reserve Actions to Support Interbank Settlement of Faster Payments

Comments:

Date:Nov 07, 2019

Proposal:Federal Reserve Actions to Support Interbank Settlement of Faster Payments [OP-1670]
Document ID:OP-1670
Revision:1
First name:Mark
Middle initial:A
Last name:Ranta, CTP
Affiliation (if any):Bottomline Technologies
Affiliation Type:Other (Oth)
Address line 1:325 Corporate Drive
Address line 2:
City:Portsmouth
State:New Hampshire
Zip:03801
Country:UNITED STATES
Postal (if outside the U.S.):
Your comment:Dear Ms. Misback,

Bottomline Technologies is thankful for the opportunity to comment on the notice and request for public comment on Docket No. OP-1670, Federal Reserve Actions to Support Interbank Settlement of Faster Payments. The Following is our response.

In order to operate a secure 24x7x365 real-time payment ecosystem, Bottomline believes that all participants must adhere to a minimum set of security related standards to protect the integrity of the system itself as well as the participants in the system from both known threats and evolving risks. Our response sought out global best practices and regulations (e.g. PSD2) and it is Bottomline's recommendation that there should be four key areas of focus taken into consideration when designing the operating rules of the system:

1) Real-time risk mitigation best practices
2) Malware protection capabilities
3) Endpoint protection capabilities
4) Strong Customer Authentication (SCA) requirement

1) Real Time Capabilities &ndash; Features and functions needed to meet the demands of a Real Time Payment Ecosystem:

I. The ability to support a real-time risk analysis of every electronic payment by the transaction monitoring solution employed by the network participant, aka the payment service provider (PSP).

II. The ability to detect changes in a payer's spending or "normal" behavioral patterns.

III. The ability to detect/identify the geographic location of the payee and validate that it is not blacklisted or identified as a high-risk location.

IV. The ability to identity that the actual provision of the payment service has been free of fraud.

2) Malware Protection Capabilities &ndash; Features and functions needed to mitigate the threat posed by malware to the payment network and its' participants:

I. All participants must deploy a solution with the ability to detect signs of being compromised by

malware.
II. The ability to identify anomalous activity such as account takeover, credential stuffing, or man in the middle attacks.
III. The ability to validate that no malware infection in any session of the authentication procedure has been identified.
3) Endpoint Protection Capabilities &ndash; Features and functions needed to mitigate the threat to the ecosystem posed by devices or terminals:
I. The solution needs to be able to validate that the device or "point of initiation" is secure, that we know where it is, and that it hasn't been compromised in any way (see malware).
II. The ability to detect endpoint or device risks with emphasis on identifying and mitigating the threat of a device security compromise, such as DNS or message re-routing, rooting/jail breaking, impersonation (e.g. cookie theft), third party unauthorized access, or sideloading attacks.
III. The ability to detect that no unusual information about the payer's device/software access is present.
IV. The ability to validate that the location of the payment initiator (i.e. the payer) is not abnormal (at the device level).
4) Strong Customer Authentication Requirement - Multi-factor/step-up/or "Strong Customer Authentication (SCA)" should be a mandatory requirement for the ecosystem.
I. The goal is to secure and maintain baseline controls for all network participants and allow for user accessible and fair market authentication means.
II. Authentication should always require at least two of three minimum elements: what you know, what you have, and what you are. These standards should also be required every time a new device or endpoint is used to initiate a session.
III. SCA should be applied when there is a risk-based reason for validating a user when a user accesses a payment account online, initiates a payment product transaction, or carries out any action via a remote channel that carries risk.

These areas of focus apply to the initial system rollout as well as all future enhancements to the system.
Thank you again for the opportunity to comment.
Regards,
Mark A. Ranta, CTP
Strategic Payment Solutions
Bottomline Technologies