

Implications of FFIEC Guidance and Proposed Solutions

Balancing Risk Mitigation and Customer Experience

Anomaly Detection with Passive Authentication

Prepared By:

**Sunil Bhargava, VP Product Strategy
Business Signatures Corporation
Redwood Shores, CA**

June 2006

A White Paper prepared for Business Signatures Corporation

FFIEC Compliance: Choices for Financial Institutions

The recent FFIEC guidance requiring banks to implement some form of stronger authentication to protect highly sensitive transactions and external transfers by year-end 2006 has had the positive effect of mobilizing the banking industry and security vendors to search for effective solutions.

However, it has also caused concern and some confusion among Financial Institutions and security vendors as to what type of approaches will be effective and approved by the FFIEC.

Financial Institutions have legitimate concerns concerning the effectiveness and customer impact of various proposed solutions currently being discussed in the marketplace.

Taking into consideration effectiveness, customer impact and a risk-based approach, an ideal solution for a Financial Institution would have the following characteristics:

1. Effective at detecting and or preventing potential fraud
2. Built upon a proven fraud prevention approach
3. Transparent to the customer experience
4. Easy, fast and cost-effective to implement by Financial Institutions
5. Flexible enough to evolve detection and prevention rules without impacting website
6. Ability to evolve into online interdiction

A Proposed Solution – Multi-factor Authentication with Active Behavioral Authentication

This paper proposes that the use of Multi-factor Authentication with Active Behavioral Authentication to be one of the FFIEC-complaint approaches available to Financial Institutions to meet the FFIEC guidance requirements.

How it works

A Real Time Fraud Monitoring System, installed at the Financial Institution's website, in conjunction with client-side JavaScript, transparently monitors all web traffic for anomalies in Geo-location information, ISP access point information (including suspect ISPs and Anonymizers), Device characteristics, Browser characteristics, and User-settings on a per customer basis. Based on a flexible rule-based anomaly detection engine, when "out of the ordinary access patterns" are detected in any of these dimensions, the system immediately notices the anomaly, and authentication escalation can be accomplished by challenging the user to enter a One Time Password (OTP) value sent via email or SMS to a pre-registered address.

The combination of Device and Behavioral Authentication is key to reducing false positives and negatives. This combination yields a system that has the fewest authentication

challenge requirements and also is resistant to session hijacking or device spoofing attacks.

Benefits of This Approach

Effective and built upon a proven fraud prevention approach in call centers

Transparently monitoring access and behavioral characteristics has been used for years as part of call center security checks. It is true that Internet access provides special challenges for reliable device monitoring because of aspects like non-persistent IP addresses, or the use of different ISPs at home and at work.

However a well-designed Real Time Fraud Monitoring System that is capable of transparently building up access and behavioral profiles for individual users can self-learn the characteristics of multiple access devices and normal behavior patterns per customer. Once an initial self-learning phase is complete, access anomalies can be detected from this baseline.

Transparent to the customer experience

This approach does not require the customer to modify their behavior, remember a second password, go through a lengthy registration process, or carry a token etc. The customer experience of the financial institution website remains largely the same.

The only requirement is to have a current email or SMS address registered for each individual customer. Only when the Real Time Fraud Monitoring System detects anomalous access or behavior characteristics, will the user be challenged to enter an OTP value sent to their pre-registered email or SMS address.

Easy, Fast and Cost-effective to implement by Financial Institutions

When used with state of the art systems that can derive the behavior directly from the network this approach does not require any modifications to the actual website the Online Fraud Monitoring system can be installed transparently and quickly: usually within weeks.

Flexibility to evolve detection and prevention rules

Since the Real Time Fraud Monitoring System is separated from the FI's website and is built upon a fraud detection rules engine, detection rules can evolve and change easily over time in a heuristic way.

Ability to evolve into online interdiction with minimal website changes

While the initial implementation of this approach requires no FI website changes, this approach has the ability over time, with minor modifications to the financial institutions website, to also provide finer grain online interdiction of suspicious behavior.

This gives the FI the best of both worlds: an easy and quick-to-implement transparent monitoring approach, with the ability to evolve into online interdiction over time.

Summary: Rapid FFIEC Compliance Using a Proven Approach

Since many financial institutions are faced with a deadline of end 2006, which is unlikely to change, they may evaluate the approach proposed in this paper to meet the deadline and not only become compliant but set themselves on a path to combat fraud using a similar business process they probably already use in their call centers. Financial Institutions are encouraged to discuss this approach with their regulators and its applicability to FFIEC compliance.