

FSTC Monthly Highlights – June 2006

FSTC continues to provide an action-oriented, collaborative forum for our members to address shared business opportunities and challenges through technology-oriented projects and knowledge-sharing. Please contact me, Dan Schutzer at Dan.Schutzer@fstc.org, or the appropriate Managing Executive for more information.

Since our last update, we are:

Developing several new project initiatives (summarized below):

- Account-based Payments Convergence
- Better Mutual Authentication Phase II
- Data and Resource Sharing amongst FI's and partners

Launching a Vendor Advisory Council

Annual Conference planned for Oct 10-11, with SCOM meetings on Oct 12 at Columbia University, New York

Below is a short highlight of activities in our Standing Committees:

Enterprise Architecture Standing Committee

The second face-to-face meeting of the Enterprise Architecture Standing Committee (EA SCOM) was held on June 19-20 in Charlotte, hosted by Wachovia. This meeting was very well attended with 32 representatives from 15 FSTC member companies. Significant progress is being made toward our primary goal which is building a community of senior architects and technologists to facilitate collaboration towards industry goals. A primary agenda item was to review the results of the EA Profile survey which was completed by ten organizations. This proved to be an excellent vehicle for sharing information and experiences. The SCOM agreed to collaborate on the development of a version two of the survey which would provide more value to the involved organizations. Some things coming out of this area are:

- Two tracks: Management Track and Practitioner Track
- Enterprise Architecture Profile and Maturity Survey – round 1
- Services Oriented Architecture (SOA) Special Interest Group
- Standards Usage Initiative

The next face-to-face meeting of the EA SCOM will take place October 12 in NYC, after the Annual Meeting Oct 10-11

For more information, please contact Bill Barr at bill.barr@fstc.org

Business Continuity Standing Committee (BCSCOM)

Assisted with the development of the agenda for the first FSSCC Infectious Disease Forum – FSTC and interested Members to attend the first meeting is planned for July 11 in Washington DC

SCOM meeting to be held July 17 at 1 PM et – Federal Reserve Bank to provide an update Operational Risk Trends, Basil 2 and Sound Practices Activity

Continue to play a leadership role in FSSCC R&D Committee and other related activities

For more information, please contact Charles Wallen at charles.wallen@fstc.org.

Payments and Check Imaging Standing Committee

- Supported continuing meetings of:
 - Source Document Forum
 - will form a subgroup of X9 to define standards for business checks
 - Usability Definition SIG
- Kicked of Account-based Payments initiative
 - conducted 2 team formation calls
 - monthly bank-only meetings will be scheduled going forward
 - Partnering with BITS and other industry players to combat cross-channel payment fraud; FSTC is now a member of the Partner Group

For more information, please contact Chris Nautiyal at chris.nautiyal@fstc.org

Security and Infrastructure Standing Committee

- Held meetings on Biometrics, Secure email and Identity Access control of resource and information sharing.
- Kicked off Better Mutual Authentication follow-on
 - Held two formation meetings for a Better Mutual Authentication Project follow-on
 - Conducted a project survey
 - Project Prospectus is in preparation; look for it on our website.

For more information, please contact Steven Bellovin at Steven.Bellovin@fstc.org

Projects

We view our projects as our core activity, and one of the key benefits of FSTC membership is eligibility to participate in these projects. Below are some details on some of our recently completed and newly launched projects, as well as a description of some of our Projects in development.

ACTIVE PROJECTS

1. Image Capture System Benchmark

A potential root cause of image quality problems is uneven camera calibration and maintenance of image capture systems. While already an issue in bank processing centers both across centers and within the same center, the growth in distributed and remote capture amplifies the importance of consistent image capture, and the need for an industry standard benchmark to reduce related image quality problems.

During the project the team will run and test "benchmark" documents on project participants' image capture systems with the goal of establishing a standard benchmark deck to be used to "certify" new equipment and maintain current equipment.

The first in-person project meeting was June 27-28 hosted in Charlotte by Bank of America. Fun was had by all viewing hundreds of images that significantly varied due to the variety of capture platforms that captured the images; there was much more variation/less consistency than we expected!!

If you are interested in participating, please contact Chris Nautiyal at chris.nautiyal@fstc.org.

2. Resiliency Model: Phase II – launched December 2005 with a target completion date of August 2006

Current Activity Highlights:

Face to face working session was held in Milwaukee June 6 and 7 hosted by M&I Bank

Survey of Resiliency Practices questionnaires have been developed to support notional self assessments by participant organizations

Training to be held in mid-July on Resiliency Survey techniques and strategies to facilitate a standardized data gathering approach

Data base is being developed to store and manage resiliency benchmark data gathered during surveys

Capability documentation is ongoing to define resiliency competency goals, characteristics and practices

Working sessions are held every other week to focus on framework development

In-person working meeting are being scheduled in July and September; Participant Executive Resiliency Briefing is tentatively planned in September or October

Design, objectives and deliverables are being developed in conjunction with Carnegie Mellon for Phase 3 of the project

Resiliency Project Overview

FSTC defines "resiliency" as pro-actively managing risks and adaptively responding to disruptive events. The FSTC Resiliency Model Initiative Phase II will answer such questions as:

What constitutes resiliency?

How does an organization assess their resiliency/operational risk management capabilities against an accepted industry standard, and establish an ongoing process improvement methodology?

How can an organization identify where investments are needed, and where they are not, against an unbiased, vendor-neutral, and risk-based model?

How can a common, effective set of terms reduce the communication friction between the financial services industry, service vendors, and government regulators?

Over the past year, FSTC has been working with industry-leading financial institutions, technology vendors, and industry partners like the Carnegie Mellon SEI Network Systems Survivability Program to answer these questions, and to enable more efficient and effective resiliency management in the financial services industry through the development of the FSTC Resiliency Model.

The Model will serve both as a process improvement tool and a roadmap to refining resiliency capabilities for financial institutions and their partners. It creates unbiased common ground for organizations and vendors to develop cost-effective solutions. This project assumes at its core that true resiliency is a collaborative problem, and that in our increasingly global economy, the problem needs to be addressed as an industry, rather than in isolation. With the reality of increasing, devastating business interruptions due to hurricanes and other natural disasters, terrorist threats, regional infrastructure failures, and breaches in technology security, this initiative is re-defining what it takes for the financial services industry to stay in business, no matter what the circumstances.

If you are interested in participating, please contact Charles Wallen at charles.wallen@fstc.org.

3. Improving Information Security for Financial Services Processes

Background: Financial business processes create, carry or consume sensitive data. Sometimes, this data must be shared with trading partners, clients and customers. Unfortunately, implementations of information security controls that are intended to protect sensitive data vary among communicating parties. These variations can open opportunities for criminal exploitation or unplanned release of sensitive data leading to diminished public trust in participating financial institutions, revenue shortfalls and higher costs. In an effort to reduce this vulnerability, study is directed at:

- Developing standard reference models of key financial processes where information is exchanged and shared externally (Account-opening and Payments are initial use cases)
- Investigate how to reduce the amount of sensitive information that needs to be transmitted and shared with external parties
- Investigate how to remove obstacles to real-time information sharing
- Investigate how to reduce vulnerabilities by encrypting data and auditing access

This is a joint OMG-FSTC initiative aimed at examining key financial processes, such as Account Opening and Payments, with the goal of minimizing the amount of sensitive personal information exchanged and shared.

If you are interested in participating, please contact Dan Schutzer at dan.schutzer@fstc.org.

PROJECTS IN FORMATION:

1. Better Mutual Authentication Phase II

The Counter-Phishing project defined the problem, and the Better Mutual Authentication Phase 1 project, helped to shape and define the industry's requirements for solutions. As a result of successful completion of these projects, and as evidenced by the success of recent outreach efforts, the FSTC now has excellent credibility in this area. Recent phishing incidents point to the importance of a strong *mutual* authentication – providing the customer greater assurance that the website they are visiting, and the email they are reading, really comes from the Financial Institution they do business with. A follow-on project could draw in additional participants, build on work already completed, and result in significant forward progress toward influencing critical vendor initiatives and standards bodies, and lead to a successful operational deployment of enhanced *mutual* authentication.

We have held two formation meetings for a Better Mutual Authentication Project follow-on, conducted a project survey, and a Project Prospectus is in preparation. Look for it on our website.

If you are interested in participating in further development, please contact Dan Schutzer at dan.schutzer@fstc.org or Chuck Wade at chuck.wade@fstc.org

2. Account-based Payments Convergence

In general, the payment “networks” (e.g. credit, debit, merchant, consumer, ATM, corporate, check, mobile, clearing house etc.) are “converging” and this is leading to a number of issues and opportunities. During project formation participants will discuss the following issues and determine which topics to focus on and what to do about them!

Are current Payment and Technology Trends causing gaps in the payment infrastructure?

Is the conversion of checks making way for increased fraud, and customer confusion, or is it presenting new revenue opportunities and suggesting new product innovations:?

Can we move toward “real time” authentication and posting of check payments?

Will payment convergence allow for payment infrastructure convergence and cost savings or increased processing overhead?

What can we do to mitigate the effects of the image environment on fraud, the payment infrastructure, immediate conversion to ACH therefore bypassing image exchange and storage?

How does this convergence impact the various rules, regulations, security, and protection?

Can we design more flexibility into our payment systems to accommodate changes and increased flexibility in the rules and regulations?

Two kick off meetings were held in June; be on the look out for an invitation for regularly scheduled monthly meetings

Please go to [fstc.org](http://www.fstc.org) at <http://www.fstc.org/news/news051506.php> for more information.

If you are interested in participating in further development, please contact Chris Nautiyal at chris.nautiyal@fstc.org

3. Data Sharing and Rights Management

"Assessing the Potential for Technology and Standards to Better Protect Customer Data"

Most US financial institutions send and receive consumer data to and from third-party service and outsourced data providers such as Acxiom, Choicepoint, and Experian. They do so in a variety of business processes including customer registration, account enrollment, authentication, loan scoring, customer address cleansing, new hire

background checks, and others. In some cases, due to the confidential and sensitive nature of such data, it is generally encrypted in transmission.

However, aside from provisions contained in service agreements, financial firms have little direct control in protecting that data once its journey to the third party service is complete. As recent incidents highlight, service providers, many in unregulated industries, play a critical role in protecting consumers' private information. The US Congress is now poised to weigh and attempt to respond to this issue by extending the regulatory blanket to third-party businesses.

In light of both the concerns for protecting customer data and movement by regulators, now is the time for the industry to re-examine the data sharing and management processes in place today, and consider opportunities for technology and technology-enabled business process solutions to improve controls over customer data whether in storage, use or transmission.

If you are interested in participating in further development, please contact Steve Bellovin at steven.bellovin@fstc.org

4. Real-time Sharing of Information on Fraud Incidents

The goal of the project is to demonstrate how emerging data standards and tools can accelerate and improve the effectiveness of fraud-related information sharing in current and new information-sharing networks through a proof-of-concept.

Responding to the threats posed by modern fraud, or "phraud," requires unprecedented levels of cooperation and coordination between lines of business, organizations, industries, government agencies, and even nations. Information about fraudulent activities now comes from a variety of players, many operating outside of the financial services industry. At the same time, effective responses to shut down the machinery of fraud often requires cooperation with non-financial players, such as ISPs operating in other countries. However, much of this coordination is taking place through manual data entry, email, and phone, leading to limited use and effectiveness.

New standards are emerging for exchanging information about fraud incidents, and this Project proposes to produce a working demonstration of these new standards to demonstrate how reducing the friction associated with current information exchange mechanisms can lead to reduced fraud losses.

If you are interested in participating in further development, please contact Steve Bellovin at steven.bellovin@fstc.org

5. Secure Authenticated Messaging

The need for more secure, better authenticated, messaging is greater now than ever, and there are many related technology initiatives that need to be evaluated and influenced; such as. DKIM - Domain Key Identified Mail; SPF / SenderID. Similarly there are many available email encryption technologies and standards. Part of the issue lies in the need for solutions that are sufficiently easy to maintain and easy enough to use by consumers that they will be accepted for mainstream use.

If you are interested in participating in further development, please contact Steve Bellovin at steven.bellovin@fstc.org or Chuck Wade at chuck.wade@fstc.org

6. Shared Models for Fraud Detection

This is an intriguing project idea. A standard behavior based model would have value. If we can agree as an industry what behaviors to monitor (unusually large transfers, signing on from an unusual location, etc.) then each FI can set its specific thresholds within that framework.

If you are interested in participating in further development, please contact Steve Bellovin at steven.bellovin@fstc.org or Chuck Wade at chuck.wade@fstc.org