

FSTC Monthly Highlights – May 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 have:

Launched two new projects (brief write-ups included below):

- Resiliency Model Phase II project
- Image Capture Benchmarking

Initiated a joint study with OMG

Improving Information Security for Financial Services Processes (more detail is covered below under projects)

Completed three projects (summaries of these projects will be posted shortly):

- Interoperable Verification of Check Security Features
- Better Mutual Authentication Phase I projects
- Image Quality and Usability Assurance Phase II project.

Developing several new initiatives (summarized below):

- Account-based Payments Convergence
- Better Mutual Authentication Phase II
- Data Sharing and Rights Management
- Secure messaging
- Real-time Sharing of Information on Fraud Incidents in security.

Launched a new Standing Committee on Enterprise Architecture

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

Enterprise Architecture Standing Committee

The organizing meeting was held April 24-25 in New York City; hosted by Citigroup. The meeting was well attended with twelve financial institutions, seven technology suppliers and two non-profits represented.

The EA SCOM initially has organized itself into two tracks; a Management Track and an Applied EA Track. Each is developing a set of topics to pursue. The next meeting will be held June 19-20 in Charlotte; hosted by Wachovia.

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

Business Continuity Standing Committee

- Panel discussion of Pandemic Preparations - JPMC, MasterCard, US Bank and Wachovia provided an overview of their activities and discussion was held on challenges, planning strategies and sources of pandemic information;
- A meeting was held where Members provided feedback on the proposed Financial Services Sector Coordination Council (FSSCC)- Strategic Objectives for 2006-2007

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
 - Usability Definition SIG
- Worked on defining the Account-based Payments initiative

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

Security and Infrastructure Standing Committee

- Hosted meetings discussing Better Mutual Authentication, Secure messaging, and the OMG/FSTC initiative on Data Sharing
- Plan to launch special interest groups on:
 - Secure messaging
 - Better Mutual Authentication Phase II
 - Data Sharing and Protection
 - Review state of biometrics

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.

RECENTLY COMPLETED PROJECTS

1. Interoperable Verification of Survivable Check Security Features IV-SCSF (completed Feb 2006)

As the financial services industry moves to image exchange, and loses the paper-based security features and controls in place today, survivable features can play a critical role in maintaining the integrity of check payments. With a standard in place that enables interoperable verification, banks can better protect their customers, merchants, and other check receivers from potential losses due to check fraud. This five-month project developed the core elements of a standard for interoperable verification of survivable

security features. When formally codified by X9, it will enable the interoperable verification of survivable security features at the point of payment.

For a more detailed summary, please visit:

<http://www.fstc.org/projects/ivcsf.php>.

The press release is available at:

<http://www.americanbanker.com/article.html?id=20050908E8C35A7K&from=home>

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

2. Image Quality and Usability Assurance: Phase II (completed Nov 2005)

This project framed the groundwork, removed major technical obstacles and set in motion the acceleration of the historic shift from exchange of paper checks to exchange of electronic images. The shift is significant because it brings new efficiencies and benefits to banking, and it changes the way every American consumer and business receives and stores the most basic financial document - proof of payment.

The results of the Image Quality and Usability Assurance project provide the first vendor-independent industry-standard way to approach check image quality. Lacking this standard approach, banks have no way to trust the quality of images captured outside of their direct control. The project results have changed that. By focusing on the metrics that best predict check image usability, banks can improve the effectiveness of their manual review while reducing the number of images reviewed, speed up their review times, and reduce their risk and liability. This is a tremendous gain for the industry and offers the prospect of reducing the workload for assuring image quality.

For a more detailed summary, please visit:

http://www.fstc.org/projects/image_quality_summary.php.

The press release is available at: <http://fstc.org/press/img121506.php>

You can request the full report from Chris Nautiyal at chris.nautiyal@fstc.org

3. Better Mutual Authentication (completed April 2006)

A summary of the project and its findings is still being completed, but briefly, BMA produced:

- Identification of relevant use cases, vulnerabilities, and threats
- Updated terminology used to define authentication practices
- Surveyed available technologies and solutions
- Produced “Financial Industry Requirements and Recommendations for BMA”
- Developed tools for evaluating combinations of authentication techniques
- Developed a high level architecture of authentication systems that employ multiple authentication techniques
- Created a roadmap for evolving BMA to meet future needs
- Identified key standards organizations and vendor initiatives that the Financial Services community should be working with in order to ensure a satisfactory Better Mutual Authentication Solution emerges

Some related findings include:

- Authentication in a retail financial context must address the inherent asymmetry of a *real person* communicating with *machinery*
- *Mutual authentication* is vital to bolstering consumer confidence and trust — consumers must be able to confirm authenticity of financial service providers
- *Multiple authentication techniques* need to be available to financial institutions and their customers—not just multi-factor authentication
- *Multiple channels* must be supported by new authentication schemes, although the Web is the channel of greatest immediate concern
- *Different applications* require *different approaches* to authenticating the parties—there are *no* one-size-fits-all solutions
- New authentication techniques will not *displace*, but must *complement* traditional techniques—passwords will be needed for some time to come
- Customers will *delegate authority* to other parties to act on their behalf with financial services, so new authentication systems must support delegation
- Effective *customer support* is essential if consumers are going to adopt new authentication measures

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.

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:

- Specialized working groups have been formed to address three key areas of the project – Framework development, Practices review/analysis and Taxonomy refinement;
- Capability documentation is ongoing to define resiliency competency goals, characteristics and practices;

- Assessment questionnaires are being developed in conjunction with the capability write-ups that will facilitate notional self assessments by participant organizations;
- Working sessions are held every other week to focus on framework development;
- The third face to face working session is scheduled for June 6 and 7 hosted by M&I Bank in Milwaukee.

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 Resiliency Model Initiative: Phase 2 (RM-2) continues the ground-breaking work of Phase 1, which created a new common taxonomy of terms, and a framework that facilitates benchmarking, self-assessments, process improvement and measurement. The RM-2 project proposes the continued development of a Resiliency Model that defines capabilities, characteristics, goals and activities across virtually all of the key processes of an organization, including: technology, infrastructure, facilities, information assets, people and third-parties.

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

This is a joint study with OMG.

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

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

PROJECTS IN FORMATION

1. 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. For example, as merchants, consumers and many other players in the payment value chain get savvier, and technology advances, the various players are cleverly figuring out how to transact what should be a check payment over the ACH network, how to avoid credit and debit card interchange fees, how to bypass the ATM network, how to use “phone” networks and the Internet for payments and information businesses derived from payment and bank account information, and many more such innovations. These “innovations” often lead to increased risk of fraud and Identity Theft. Examples of increased risk include fraudsters “stealing” account numbers, possibly compromising the check image infrastructure, finding ways to by-pass online payment authentication, etc.

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 Trends causing gaps in the payment infrastructure?
- Is the conversion of checks to ARK, POP, BOC, etc. making way for increased fraud, customer confusion and difficult back office research?
- Can we move toward “real time” authentication and posting of check payments and charge a premium?
- Will payment convergence allow for payment infrastructure convergence and cost savings?
- 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?
- Why don't credit card numbers, debit card numbers and checking account numbers have the same rules, regulations, security, protection and flexibility?

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

2. 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

3. 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

4. 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. 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 authentication.

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

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 Keyes 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