

## **Q&A Document – Bank Systems & Technology Web Seminar January 25, 2007**

### **WEBSTER BANK QUESTIONS**

**Q: How long was the project to test and rollout single sign on successfully?**

A: It is an on-going process as new applications come on-line. I would say that the initial few applications took a few months mainly due to our inexperience with the product and process. Now, depending upon the application and the information we obtain from the application owners, we can add some in as few as a few hours. Third party vendors, i.e. especially web apps, can be challenging as we don't control when the application may change.

**Q: Could you expand on how you enforce stronger passwords "behind the scenes"?"**

A: We now have the ability to enforce strong passwords without the user knowing it and also enforce frequent password changes. This means that the single sign-on product is the one changing the password, not the user.

**Q: Do you have a single vendor for core ancillary banking applications? Is SSO difficult in a multi-app, multi-vendor environment?**

A: We have one primary vendor for most of our core applications, however, the applications vary (web based, fat clients, etc) so the effort differs based upon that. The main difficulties are with third party managed applications as we may not be aware of slight changes to the application or how it is presented which could cause issues with single sign-on functionality.

**Q: How does your institution monitor employee access/activity of non-public personal information (i.e an internal breach of data)?**

A: We have strict policies surrounding data handling, storage, and transport. We also log all activity to a central repository.

**Q: What is the staffing at Webster for continuing SSO integration and system maintenance?**

A: Right now I pretty much have 1 primary and 1 backup person that have responsibility for ongoing SSO integration and maintenance. Maintenance today requires about 5% of one person's time. Keep in mind as new applications need to be added it would spike up. We have it down that some new applications can be added in a couple of hours.

**Q: Is two factor authentication used for single sign-on solutions?**

A: Single Sign-On (SSO) solutions are meant to make it convenient for the end users to reduce the number of sign-on required to access the necessary IT systems. Often, this is considered as a security weakness. In our view, implementing SSO solutions provides us an opportunity to implement stronger / complex password policies since we have reduced the number of sign-ons required. Organizations consider, Two-Factor / Multi-factor Authentication as an approach to mitigating potential security risks associated with single sign-on (SSO) solutions. Multi-factor authentication is based on the concept of using two or more methods to authenticate an identity of a user. This is generally something the user knows (a password or PIN), something the user owns (such as smart card or token), and something that only the user can present (a biometric ID such as from a fingerprint or retina scan). Any good single sign-on implementation should have the flexibility to offer the integration of multi-factor authentication systems for increased security.

**Q: Explain SSO again, please?**

A: Historically, Single Sign-On (SSO) is quite an old concept that was developed to reduce the number of sign-on between various systems. As the name suggests, single sign-on is designed to take the various number of sign-on that a user has to perform and reduce them to a single operation. In practice this will probably never be the case, but ideally a user should be able to log on once and further authentication requests would then be serviced automatically by the software rather than the user. This means that data required during a login, such as user name and password are presented to an application without the user having to remember these values themselves.

When you consider the many passwords a user regularly has to remember --such as for server access, email, or intranet proxy logins-- a single sign-on solution sounds like a great way to reduce the burden of memorizing multiple passwords, also called credentials. Research studies by analysts such as Gartner have shown that large corporations will, on average, have in excess of 70 applications or systems that require a person to login and present some credential such as a password as to their identity.

One can look at single sign-on solution as something that presents a user's credentials on their behalf to perform the login. This does not refer to systems that synchronize multiple user passwords to the same value. For more information on SSO and Novell's solution offering for Secure Login please visit: <http://www.novell.com/products/securelogin/>

**Q: What do I have to implement first an SSO solution or identity management solution?**

A: It depends on the needs and challenges of your organization. If your organization is faced with the challenge of making bank branch employees productive and focus on customer service then SSO may be an appropriate starting point. If your needs are around automating manual and paper based security and access control processes then identity management may be a good starting point.

**Q: Which piece of IT architecture is the most 'breachable' and insecure? O/S? Databases? Applications? Web Servers? Mail servers?**

A: Web Servers that are usually located inside the DMZ. Usually the Database, Applications and Mail Servers are located within the trusted network.

**FINANCIAL INSIGHTS QUESTIONS**

**Q: Which industry standards need to be paid attention to in the ID federation, entitlements and provisioning spaces? (E.g. SAML, SPML, XACML, WS Policy?)**

A The concept of federated identity really encompasses any and all industry standards in relation to identity access management. Federated identity is a single user identity that can be used to access a group of web sites bound by the ties of federation, and websites become federated by coordinated efforts of the financial institution and those connected by service agreement (ie service partner providers). Without federated identity, users are forced to manage different credentials for every site they use, and this collection of IDs and passwords becomes difficult to manage and control over time, offering inroads for identity theft.

**Q: Do you see banks issuing a 'federated' accepted online identity? Such identity would allow consumers to use a bank issued ID to access accounts at several banks or even non-bank firms or government."**

A: I don't see that happening, primarily because I don't think banks could collaborate to manage a single user ID across a group of institutions, and a government issued ID brings us back to a similar issue we are facing today - the social security number. Banks will want to maintain control of their identity and access management because to relegate that responsibility across a collection of institutions would open them up to security concerns that may be well beyond their control.

**Q: What are the specific regs and compliance rules that govern security...by name? glba and?**

A: There are more than 30 rules and regs that address security that originate from the FDIC, FRB, NCUA, OCC, OTS, SEC, US congress and international authorities. If you are interested in understanding all the security requirements for your bank, I would suggest starting first with the FFIEC website as a resource as they provide documentation tools for both the banks and the examiners.

**Q: What is Basel II?**

A: For more information on Basel II you can visit: <http://www.bis.org/publ/bcbsca.htm>

**Q: What are the new regulations banks need to be concerned about? What do they impact?**

A: The most recent guidance is related to customer authentication in an online banking environment, issued by the FFIEC in October 2005. This guidance stated that banks must assess their current online banking authentication practices, conduct a risk assessment, and strengthen measures to mitigate these risks. Otherwise, the compliance landscape has remained relatively steady for the last few years, and banks are absorbing existing compliance initiatives.

**Q: Is there empirical data on acceptance rates (costs) of credit protection subsequent to the offer due to**

**a breach announcement?**

A: There is no clear data from the institutions on their financial losses as the result of a breach announcement. As you can imagine, banks do not make this information public because it would be damaging to their brand and business.