

## **W3C Workshop on Transparency and Usability of Web Authentication**

March, 15-16, 2006

### **Digital Authentication for an Analog World: Why Authentication Processes Fail and How Do We Fix Them**

## **Contributors:**

**Robert W Capps II**

Chief Technologist  
Electronic Fraud Research  
World Savings Bank, FSB

+1 510 446-4274  
rcapps756@worldsavings.com

© 2006 World Savings Bank, FSB

The views expressed in this position paper are those of the author, and do not necessarily reflect those of the authors employer, World Savings Bank, FSB or its parent company, Golden West Financial.

## The Failure of Authentication Processes

Online authentication in its current form has failed to provide a reasonable level of assurance that the consumer is actually the one at the other end of the wire when requesting transactions online. This weakness has presented itself as an increase in fraud against the consumer and in turn the financial and commerce institutions.

The real risk in online fraud today is not the fraud itself; rather the risk is in the scale at which fraud can be performed. The use of computing resources to enable fraud schemes lies at the heart of the true danger it presents. Computing resources, in the right hands, can enable expeditious processing of stolen consumer identity credentials, automating the theft, sorting, validation and use of information, overwhelming existing anti-fraud solutions in place at most institutions.

The fraud issue is intensified by the fact that institutions have relied far too long on weak login and password authentication, enabling fraudsters to make easy marks of our consumers. Recent industry efforts to change the authentication paradigm have resulted in the weakening of an already shaky online authentication and trust system. This weakness, brought about by rapid changes to the authentication techniques used by institutions, as well as mass media attention to fraud attempts, has caused fear, uncertainty and doubt among many online consumers. This distrust of the online financial system will continue to present itself for the foreseeable future if we fail to change our course and do something about it.

The current consumer identification, authentication and fraud problems are not due to the failure of any one individual authentication component or industry sector; rather it is a failing of consumer access and operating system software developers, online financial and commerce applications developers, and the financial and commerce institutions to form partnerships to mitigate the outstanding risks.

Consumer access and operating system developers have treated consumer identification and authentication as an issue to be left to the developers of online financial transaction applications and the actual financial and commerce institutions to deal with. This lack of user friendly innovation and development of authentication technologies has fostered a vacuum in which phishing and pharming has become a malignant threat to consumers' acceptance of online channels. The first level of consumer protections must start with innovations driven by the developers of the consumer access and operating system software in partnership with other stakeholders.

The developers of online financial and commerce transaction systems themselves are not immune to responsibility for the threats we are currently facing. Lack of consistency and standardization within individual transaction systems presents the consumer with a labyrinth of dissimilar systems that they must master in order to navigate the financial services and commerce options presented to them on a daily basis. This lack of standardization creates confusion in the mind of the consumer, and prevents the industry from using a very powerful fraud detection feature present within the consumer population at large. Consumers that are accustomed to specific methods of performing transactions tend to pick up on minor changes to those action sets, potentially alerting consumers to potentially fraudulent transactions. When presented with a transactional anomaly in a financial context, the consumer could be conditioned to question the legitimacy of specific financial transaction and change their behavior based on perceived risk of the transaction.

The financial and commerce institutions maintain a majority of the responsibility in this area. The lack of standardization of process and procedures between institutions has created an environment in which the consumer rarely knows what is expected of them until actually attempt to perform a transaction. Each institution seems to want to place their own special signature on how transactions are structured in order to differentiate themselves from their competitors, others just fail to take consumer friendly functionality into account when designing their online systems. The end result is an inconsistent consumer experience

that benefits no one. To add insult to an already injured consumer, institutions often implement sudden, radical changes to process and procedure that are rarely communicated to consumers in a meaningful way. These sudden changes deny the consumer (and the institution) the benefit to use their reasoning skills to detect changes in process as potential threats, and modify their behavior based on the perceived risk of the anomaly.

Successful strong authentication mechanisms cannot be limited to online use. Much like a lightning strike, fraud will always follow the path of least resistance to a given result. Once we are successful in securing the online channel, the fraudsters will move back to poorly authenticated mechanisms such as telephone and person-to-person interactions in order to transact fraud.

In order to provide strong assurance of the consumer's identity, we must reach a higher level of technical sophistication with identification and authentication solutions. Currently deployed shared secret authenticators used almost universally online (login/password, social security number, mother's maiden name, date of birth, etc) have proven useful in providing a basic level of consumer authentication assurance for low risk transactions when utilized with an automated authentication process. Shared secret authenticators fail to provide an equivalent level of security for offline authentication processes and are completely inadequate for high risk transactions. Once a consumer's shared secret credential has been used as part of an offline human-to-human authentication process, the effective security of the disclosed shared secret is reduced due to the fact that another person now has knowledge of the authenticator. Continued use of shared secret authenticators between online and offline channels will put all authentication processes at risk of unauthorized access due to the disclosure issues inherent in offline authentication processes.

Alternative strong authentication solutions currently in use have many issues that preclude them from being successfully deployed to cross-channel consumer identification and authentication applications. Solutions such as hardware tokens with one-time-use passwords provide an adequate cross-channel authentication process that is easy to integrate, but fails to scale where customers have relationships with various institutions. Biometric techniques are showing progress in the lab, but are still less than reliable in practice and present major issues with credential acquisition online. Traditional knowledge based authentication solutions are simple to implement and are readily accepted by consumers, but rely on static authenticators that are easily stolen or obtained by the fraudster.

Addressing the shortcomings of current online authentication techniques, the Federal Financial Institutions Examinations Council recently issued guidance to financial services companies under regulation by FFIEC member agencies. This guidance required financial institutions to deploy some form of two-factor consumer authentication to protect consumer information and other assets. While this guidance was a positive step in moving the financial industry towards consistent consumer authentication, it has no impact on the commerce industry that will quickly become the weak link in the protection of consumer information. The lack of meaningful oversight of commerce institutions puts the consumers who do business with them at continued risk of financial and identity related fraud.

Any solution that has a hope of being successfully deployed in the consumer identification and authentication space must be capable of solving identification and authentication issues within multiple channels and must conform to standards developed by the financial and commerce industries. We must be proactive regarding solutions to identification and authentication threats; else we again run the risk of having a solution handed to us by the government regulatory agencies – a position that rarely provides a good outcome for any party involved.

## Where Do We Go From Here?

As players in the financial and commerce sectors of the US economy, we must all work to develop standards for cross-channel authentication techniques and transaction processing procedures that are easy for a consumer adopt. This will require a partnership between the stakeholders and interested parties such as consumer groups, software development companies and the finance and commerce institutions themselves. Without this partnership, we will continue to loose ground in the fight with the criminals that perpetrate fraud against our customer base.

We must all work together in order to mitigate the risks in our current consumer and institution identification and authentication processes, solutions should focus on:

- The development of cross-channel authentication techniques, enabling the use of strong authentication online as well as within traditional offline channels such as telephone and in-person transactions.
- The development of standard processes and procedures for performing transactions, such as:
  - Processing credit card transactions.
  - Performing account-to-account and institution-to-institution monetary transfers.
  - Performing consumer identification and authentication.
- The development of standard ways to transport identification information between the consumer and the institution, such as:
  - Providing identity information to consumers regarding the legitimacy of online applications and websites presented, detecting and alerting to the presence of potentially fraudulent interactions before they have an impact on the consumer.
  - Developing methods for securely requesting and transmitting consumer identity credentials, immune to crimeware and other types of attacks.
- The development of standards that outline consistent consumer education efforts to promote online safety and educate consumers on standardized transaction processes.

In conclusion, the major stakeholders in strong consumer identification and authentication must form a long-term partnership to ensure that the critical online channel is not lost to fraud and other criminal operations.

Innovation and standardization will present mitigating alternatives to the risks that manifest online and off. We cannot afford to focus on securing only one business channel at the expense of all others.