

THE IMPACT OF STRONG AUTHENTICATION ON USABILITY

KEYS TO POSITIVE ONLINE USER EXPERIENCE FOR FINANCIAL INSTITUTIONS UTILIZING THE WEB

White Paper



THE WEB HAS THE POTENTIAL TO BE THE MOST PERVASIVE, COST-EFFECTIVE CONDUIT FOR BUSINESS EVER. THE HEALTH OF THE CHANNEL REMAINS STRONG IN SPITE OF INCREASING CONSUMER CONCERNS ABOUT IDENTITY THEFT AND ONLINE FRAUD. IN NO INDUSTRY IS THIS TRUER THAN FINANCIAL SERVICES.



The Security Division of EMC

The key to maintaining a healthy channel is to provide consumers with the assurance that their online interests are, in fact, being protected by effective security features. There are many important differences between the various security solutions available; however, one thing remains constant—no matter which solution you choose it will have a significant impact on your customers.

A person's interaction with, and perception of, a security solution is arguably as important as the technology itself. The more difficult it is to use a security product, the less secure that product actually becomes. A positive user experience can lead to increased consumer confidence and a higher number of online transactions. Whereas a negative experience would have the opposite effect. >



TABLE OF CONTENTS

I. WHAT IS "USABLE" AND WHAT DOES THAT MEAN FOR STRONG AUTHENTICATION?	3
Understand User Goals	3
Be Intuitive	3
Ensure Consistency	3
Communicate Effectively	4
II. BEST PRACTICES FOR FINANCIAL INSTITUTIONS DEPLOYING STRONG AUTHENTICATION	4
1. Understand What Type of Solution is Desirable to Whom	5
2. Introduce the Concept of Strong Authentication When it is Most Expected	5
3. Know What to Say	6
4. Say It on a Need-to-Know Basis	6
5. Add Value, Not Obstacles	7

Part 1: What is “Usable” and What Does that Mean for Strong Authentication?

The degree to which financial institutions will be successful at continuing to grow online channel usage will depend on their success in dealing with the core issues of security and usability. The deployment of consequential strong authentication will have consequences on the end user experience. When deploying strong authentication solutions, balancing security and usability is of paramount importance—and can only be accomplished if we first understand what is “usable.”

In the domain of security software, there is a classic conflict between security and usability. Usability professionals favor making it as easy as possible for the user to access any given resource; while the security professionals, tasked with protecting the secrets of individuals and corporations, favor making it difficult to access resources in an effort to keep out unauthorized users. This conflict can lead to a healthy symbiosis in which security offerings are designed and developed to be both secure and usable.

In this section, we will take a look at what makes an online experience more or less usable. We will also look at how that impacts the efficacy of the online channel, and what that means for strong authentication.

Understand User Goals: Do not interfere with the user’s ability to complete their desired task.

The key to usable online security is to provide the level of security desired by users without interfering with their ability to quickly accomplish their online goals. The user’s intention in using an online service is not to get slowed down by or overly involved in the process of verifying one’s identity. Authentication should reassure the user concerning the security of their transactions without becoming an insurmountable hurdle.

As identity attacks become more widespread, the level of security desired by consumers is increasing (see sidebar). As web savvy consumers become gradually more security savvy, they will begin to choose between online services based on the level and type of security provided. Providing consumers with an extra layer of protection will become necessary to compete in the online marketplace. Ensuring the convenience and usability of that extra layer of protection will be an essential competitive advantage.

Be Intuitive: Usability is the art and science of delivering a Web experience in alignment with the expectations of those who experience it.

Today’s most successful web enterprises appear intuitive as they display information to the end user. This intuitive quality stems from a company’s understanding of who is using their website and what their goals are. Online processes should unfold in simple, logical and linear sequences, and be measured against tasks successfully accomplished with minimum effort and maximum satisfaction. In the case of online banking and trading, it is essential for a website’s design and flow to work seamlessly as the end user works to accomplish their desired activity. Ensuring the usable nature of an online service decreases user frustration and increases satisfaction – leading to an overall decrease in the instance of failed transactions and opportunity loss for the financial institution.

Any new task can eventually be learned — finding a new doctor’s office, filing taxes for the first time, registering a vehicle after a move. However, the degree to which financial institutions can reduce this learning curve in the online environment can translate into benefits such as reduced rates of transaction abandonment, lower call center volumes, and higher customer satisfaction. When deploying strong authentication, financial institutions should consider the major points of exposure for the end user, including both the initial and ongoing contact with the given solution. In

IN AN ONLINE SURVEY
CONDUCTED IN MAY 2005
BY LIGHTSPEED RESEARCH,
4,062 ONLINE BANKERS AND
TRADERS WERE ASKED:

“If your online account provider were to offer you a service such as this [service described was a one-time-password token], how would it affect your trust in transacting online?”

- 85.4% would have more or much more trust in transacting online

“How would it affect your likelihood to transact online [versus offline]?”

- 63.2% would be more or much more likely to conduct more transactions online



part two of this paper we will explore how and when to introduce different forms of strong authentication as supported by extensive consumer research.

Ensure Consistency: Usability is the absence of unnecessary confusion, conflict, or uncertainty.

The cardinal rule to making the online channel “usable” for customers is to ensure consistency. This means end users should interact with an interface that is predictable, aesthetically pleasing, and reinforces the brand’s promise. Usability has as much to do with the succinctness of a task as it does with the consistency of the steps within the task.

Let’s take, for example, the account login process. Today, a typical online banker or trader goes to the financial institution’s main page, is prompted to enter a user name and password, and in some cases to select the account he wishes to access. The first time a user does this, perhaps he spends some time locating the login fields or recalling his user name or password. Perhaps the user forgets to select his account type and is reminded to select that information. However, after some practice the process is learned, and the associated behavior pattern becomes automatic. It grows to be so routine that the user can click on the user name field, tab to the password field, and hit “enter” in seconds flat. What happens when you introduce a new step into the process, for instance, introducing strong authentication? The users must re-train themselves and learn the new behavior pattern. Ensuring a consistent interaction with proper assistance and communication can greatly affect a user’s willingness to adopt the new process.

Different forms of strong authentication have a different impact on user experience. Risk-based authentication is a predominantly behind-the-scenes technology which only prompts the user for an additional credential when a given activity or transaction appears anomalous. The anomalous activity model runs the risk of confusing the user with an inconsistent authentication experience. However, when the solution is deployed with effective language to explain why additional authentication is required, the user experience is preserved. If one risk-based solution has a 30:1 genuine to fraudulent user ratio and another has a 1:1 ratio, then the solution with the 1:1 ratio will impede fewer users and deliver fewer inconsistent experiences. It will also drive fewer customer care calls by a factor of 30, which is an enormous cost component when considering the total cost of deploying a solution.

There are also usability challenges faced by utilizing one-time-passwords with either hardware tokens or software that resides on a mobile phone or handheld device. However, a benefit of this technology is the consistent user experience. The user must enter the six-digit code at each login, thus the behavior quickly becomes routine. Two important factors in reducing the impact of one-time-passwords on the user experience center on user education: (1) the effectiveness of the communication describing what the technology is, and; (2) the availability of easy-to-use online self help. For instance, automating the generation of temporary access codes for customers temporarily without their token can minimize potential support costs. In part two of this white paper, we provide further exploration of the usability of the different forms of strong authentication.

Communicate Effectively: Usability is by definition comprehensible.

One of the strongest benefits of the online channel is that dynamic content can deliver a tailored experience depending upon a user’s unique set of needs or interests at a given time. This can outweigh the need for consistency. Above and beyond consistency, it must be comprehensible.

The language used to explain what the user is seeing and why is essential to successful completion of the activity or transaction at hand. Text on the Web must be clear and concise. Financial institutions should know the terminology their customers understand and to what degree. In the communication of online security, this becomes indispensable information. User understanding of different terminology can easily be discovered through qualitative and quantitative research. An online survey would uncover what percentage of consumers claimed to know a particular term, whereas focus groups or one-on-one interviews provide the appropriate forum to discover if users truly understand a term or concept and to what degree. For instance, we strongly recommend against using the words “strong” and “authentication” when explaining a new strong authentication solution. This is basic, yet fundamental, learning gleaned from our extensive focus group research.

A second critical factor is when and how to communicate new concepts to end users. Here we consider the importance of a well thought out marketing campaign. This includes announcing the new security service and educating the customer base through the use of email, banner advertisements, contextual integration, packaging, direct mail as well as other online and offline campaigns. It is important to introduce a new concept when you have a consumer’s interest. For instance, a banner ad on the safety and

security page might receive a higher percentage of clicks than a banner ad on the account setup page. How you deliver the message also plays a key role. Encouraging customers to enroll in a program while educating them about online security in general or responding to an inquiry about account protection, would be viewed as delivering value. Conversely, forcing them to view information when they are not naturally receptive to it will be seen as a nuisance and could damage your brand.

Additional considerations for effective communication include limiting the number of new concepts introduced in a particular time frame, and repeating key messages to ensure comprehension and reinforce value. Each of these is explored further in part two of this paper.

Part 2: Best Practices for Financial Institutions Deploying Strong Authentication

A positive user experience starts well before any architect, designer, copywriter or developer creates a single user flow or interface. Delivering an intuitive, consistent, well communicated online interaction begins by understanding the end user. With the introduction of strong authentication, it is important for financial institutions to not only understand how their customers utilize their existing web applications, they must understand what their customers know about online threats and how they will react to the introduction of new security features.

Now that we have explored what makes a given experience usable, let's explore some best practices for financial institutions implementing a strong authentication solution. These recommendations are a result of RSA's extensive consumer research and the expertise of our on-staff Consumer

Marketing and User Experience Design teams. Both qualitative and quantitative in nature, the proprietary studies—from which we've drawn for this paper—include the following:

QUANTITATIVE STUDIES

- **Concept Testing:** Two online surveys conducted in May and August 2005 with 8,189 and 3,068 active online users, respectively; by LightSpeed Research. The surveys tested for interest in, willingness to adopt, and purchase intent of strong authentication solutions and their impact on consumers' attitudes and behaviors.
- **Attitudinal Study:** Published as the Annual Financial Institution Consumer Online Fraud Survey, this survey was administered by Infosurv to 402 online users in November 2005 to gather attitudes and opinions on strong authentication and e-mail fraud, such as phishing
- **Segmentation:** An online survey conducted in June 2005 among 2,644 online consumers by Forrester Research to develop a segmentation model to define the addressable market and identify optimal messaging and outreach strategies.

QUALITATIVE STUDIES

- **Focus Groups:** A series of nine focus groups conducted by Cymbal Research in three markets (Boston, MA, Chicago, IL, and Orange County, CA) to understand consumer perceptions, understanding and behavior regarding the Internet, associated threats and potential security solutions.
- **Usability Tests:** Three rounds of one-on-one usability test sessions (each with six to eight end users) conducted in the RSA usability lab facility between December 2005 and March 2006. Products tested include risk-based authentication, networked one-time-password tokens, and one-time-password web toolbar.

1. Understand What Type of Solution is Desirable to Whom

Different consumers have different preferences. What is acceptable or desirable to one consumer may not be to another. This basic credo of Consumer Marketing is the very reason there is competition in the market. It is the reason we can have our pick of sedans, SUVs, trucks, minivans, coupes, and convertibles. RSA's August 2005 quantitative study supported this notion in the strong authentication space as well. Testing multiple forms of strong authentication—including five types of one-time passwords, risk-based authentication and mutual/reverse authentication—there surfaced clear segments of users that were willing to adopt certain technologies and not others. The segmentation study went on to show that these groupings actually break along psychographic rather than demographic attributes. That is, the research showed that differing attitudes and behaviors drive what consumers choose to adopt, rather than indicators such as age, gender, income or education.

For example, some consumers' online behavior is not at all influenced by perceived threats. They trust that their financial institutions are providing them with the protection that they need. For this group, risk-based authentication is ample. There exists another segment of consumers that prefers more tangible security—security that they can see and hold onto. They aspire to feel in control of their online experience, and they find comfort and empowerment in security that they can interact with. In fact, they're willing to conduct more transactions online when they feel this control. The type of authentication appropriate for this audience is something they can physically hold in their hand—like a one-time-password for their handhelds or mobile phones.



The key, with regard to user experience, is knowing what type of solution to offer which user. Well-developed strong authentication solutions will have mechanisms built in to help segment the user base and will be accompanied by relevant market research such as a segmentation scheme for targeting the right solution to the right individual online users. With this type of insight, financial institutions are able to introduce the right solution for a given user the first time, increasing that user's satisfaction and furthering the trust and loyalty he/she has for the institution.

2. Introduce the Concept of Strong Authentication When it is Most Expected

Despite a feeling of helplessness displayed by consumers during focus group research, there exists a strong underlying interest in improving the Internet security, demonstrated by strong favorable responses to the strong authentication offering described in the sessions and quantitatively tested for interest, willingness to adopt and even purchase intent. Consumers also displayed a high level of trust in their financial institutions to provide the protection necessary for them to bank and trade online safely and securely. As a trusted source, financial institutions "have permission" to introduce new security measures to customers. It is an expected or intuitive offering—the first key to guaranteeing a positive user experience. To extend the feeling of trust online bankers and traders exhibit, financial institutions should introduce a new strong authentication solution—be it risk-based, one-time-passwords or some other form—when the user is in a comfortable and routine state. For instance, once the user has logged into their account, they feel more protected and therefore, more receptive to new offerings. New security should not be introduced prior to or during the login process.

If a given solution is elective and requires the financial institution to build awareness and interest in the product or service, an appropriate time to do this is just after a user has logged out of their account. They have completed the task at hand and as a result are in a satisfied state. Delivering new value at that point is very well received. Once a customer has become sufficiently interested in the solution and elects to enroll, the process much be streamlined. Guide the user through the flow with clear headlines, prominently placed action buttons, and repetition of key messages. Simplify the burden on the customer by pre-populating any required information that the bank has on record, but do this without making the user feel exposed. Always provide clear direction on what to expect next.

Similarly, if a solution runs entirely in the background and the user will never have any interaction with it, a simple announcement in a billing statement, an account alert/update or at logoff are enough to relay the value of the protection but with minimal impact on the user's mind share. Solutions that fall somewhere in the middle—that is, they don't impact user experience, nor are they entirely transparent—must evaluate each touch point closely, anticipating the user's state of mind. Carefully considering what the customer is trying to accomplish and associated attitude during each flow will help identify the most opportune places to introduce the new security measure. This is where usability testing becomes indispensable.

3. Know What to Say

Being able to talk in terms online users can understand is the most significant step a financial institution can take to ensure a positive user experience when deploying strong authentication. RSA has conducted focus groups and one-one-one interviews to level set on consumers' familiarity with different online threats and Internet security,

and their common lexicon for describing these two core communication components. This information has been captured in the Marketing Implementation and User Flow Reference Guides that accompany RSA's authentication solutions. For risk-based authentication, the guides cover solution introduction, initial data collection, challenge intervention, and frequently-asked questions. For one-time-password authentication, the guides include solution introduction, enrollment, activation, authentication, self help, and frequently-asked questions. A reassuring tone—one that communicates the customer's best interest is at heart, but without using such clichéd overtures—is most effective. Second, when introducing how the security solution works, use straightforward, active sentences that tell customers what to expect and when to expect it. Empty words do not add to the value delivered—only length—and can be interpreted as disingenuous. For example: "At OurBank, your security is our top priority. Our mission is to ensure your online banking experience is safe and secure." The consumer's response? "Well, I should hope! I do business with you, and you have all my money." Value is delivered by what you do, more than what you say. The financial institution's deployment of the solution alone can communicate that sentiment. Third, if collecting personal information, tell the user how it will be used. At this point, advice being given by consumer protection groups and the media is beginning to sink in: To guard against identity theft and online fraud, don't give away personal information. An upfront explanation can assuage the uneasy reaction a subset of consumers may have. These are just three examples of the many language lessons learned through RSA's primary research.

4. Say It on a Need-to-Know Basis

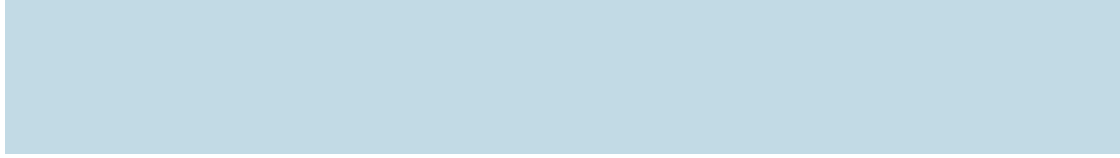
RSA's quantitative study undertaken in May 2005 showed that over 80 percent of all online consumers feel threatened by online fraud; twenty percent feel extremely threatened. But what do percentages like this tell us? The June focus groups qualified it: "Most consumers feel powerless to control or protect themselves online. They are daunted by the options available, if they are even aware of them, or feel overwhelmed by whatever actions they perceive to be helpful in limiting or containing the threat." This sentiment that was reinforced repeatedly throughout the research, supporting the old adage, "Less is more." Consumers want to be protected but shouldn't have to be security experts to do so. They do not need to understand the intricacies of how something is working—rather simply that it is working. Any solution that requires deeper understanding will not be viable in the consumer market.

Take, for example, one-time-password tokens. Millions of workers—who are, after all, simply consumers with day jobs—use these devices to access their corporate VPN and other applications remotely. If you asked them how the device works, the vast majority wouldn't be able to articulate the technology that provides the security. What they would be able to articulate is that it allows them to safely access their corporate resources from wherever they are. The good news is that this is a sufficient level of understanding for the user to still benefit from the technology.

This same level of simplicity is mandatory when introducing strong authentication in the online banking and trading environment. The implementation of any security solution shouldn't take more than a few bullets to explain the benefits, how it works, how it will impact the user, and to get set up. If any type of enrollment is necessary, it should not be more than a three-step flow. And, while minimizing the number of steps is critical, it can't be at the expense of dense content on a given screen. Don't leave this to chance. Spend the time upfront to determine the optimal exploratory language necessary to effectively communicate the value of the solution and ensure the customer's comfort level with it. This is as much an exercise in knowing what to say, as knowing when and where to say it. The order and hierarchy of information impacts the user's understanding and comfort. Guiding the user through a simple, calculated flow—while allowing to learn more by clicking out of the flow and to easily return to it—is the recommended approach for security.

5. Add Value, Not Obstacles

Offering additional account access and transaction-level protection to online bankers and traders provides a myriad of benefits to financial institutions. Beyond the most obvious of reducing fraudulent account activity, it can increase customer satisfaction, loyalty and willingness to conduct transactions online. However, these benefits will only accrue to institutions that implement strong authentication based on rigorous consumer research and usability testing. A cumbersome user experience has the ability to negatively impact a customer's satisfaction, drive customer care calls and tarnish the brand's image. Partner with vendors that understand the importance of user experience—demonstrated through dedicated user experience design and consumer research teams—and deliver this learning as an integrated, not an ancillary, component of the overall solution.



RSA CONSUMER SOLUTIONS

©2006 RSA Security Inc. All rights reserved. RSA and RSA Security are trademarks or registered trademarks of RSA Security in the U.S. and/or other countries. All other products and/or services are trademarks of their respective companies.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC