



**Head:** Strength Meets Precision

**Subhead:** *The need for strong authentication ... when it makes sense*

**By:** Steve Neville, Entrust Director of Identity Products and Solutions

Across the globe, online criminals are focusing dedicated funds, time and resources to perpetrate fraud — and they are becoming more and more adept at this process. The result has been a dramatic increase in online fraud that specifically targets consumers, enterprises and citizens.

Every data breach, such as the Heartland Payment Systems, or costly identity-theft case reported in the media erodes the public's confidence in the security of online financial transactions. This loss of confidence could jeopardize the ability of organizations to conduct transactions online.

Today, a wide variety of organizations offering online services face increasing pressure to defend against phishing, man-in-the-middle attacks and other criminal activities that are ultimately focused on defrauding individuals and businesses.

### **More attacks, billions lost**

Identity-related online attacks such as account hijacking are amongst the world's fastest-growing crimes. Compromise of a user's online identity can allow an attacker to gain access to a victim's online accounts, including their bank account. Once access to the victim's bank account is gained, criminals typically will work towards the transfer of funds from the account, as well as take advantage of access to more personal information that may be useful in the future to perpetrate other crimes.

This type of identity fraud is alarming since the perpetrator need not reside in the same region as the victim, nor have access to any physical documentation. From virtually anywhere in the world, thieves need only trick a user into surrendering their password and the rest becomes a simple process of executing online fraud.

Even though stronger authentication policies are becoming more commonplace, reliance on simple passwords in the majority of online transactions allows identity fraud to continue to thrive.

Two major forms of online identity attacks clearly demonstrate the frailty of password-only authentication schemes. Phishing and man-in-the-middle attacks rely on the use of "spoofed" e-mail messages and other techniques to direct users to fraudulent Web sites where their online credentials (i.e., passwords) are stolen. By fooling victims into divulging their usernames and passwords, attackers can gain access to the victims' accounts. Man-in-the-browser and malware attacks use different, more

invasive techniques to steal the user's identity, but they are still typically initiated with phishing emails, and the end result are the same.

These attacks are made possible due to the inherent weaknesses in password-based, single-factor authentication. Once an online thief observes the user's name and password, he has all he needs to access the victim's online account.

Unlike traditional forms of identity theft (such as dumpster diving), an online attack can come from anywhere in the world and only needs to reach a small percentage of users to result in the compromise of a significant number of user identities.

Most online organizations provide some — or in the case of some retail banks, complete — reimbursement for losses from these types of attacks. This leads to significant cost to these organizations, and significant inconvenience for end users as the incident is investigated by the bank. This alone provides a valid business rationale for addressing the issue immediately. However, this is not the most significant impact or risk from online identity fraud.

### **The effect of declining consumer confidence**

Global organizations continue to seek methods to help stop persistent fraud attacks on invaluable information, customer identities and brand image. Unfortunately, because of cost, apathy or arrogance, they're still not taking the appropriate precautions.

According to the fourth annual "U.S. Cost of a Data Breach Study," research released in February 2009 by the Ponemon Institute, the average total per-incident cost for a data breach in 2008 was \$6.65 million. This represents an increase of more than \$300,000 per incident in 2007 and a 40 percent jump since the study's inception in 2005.

On Jan. 20., Heartland Payment Systems, a New Jersey-based credit card processing company, announced in a news release that as many as 100 million customer accounts may have been compromised after malicious software enabled a security breach in the organization's payment processing system. The breach, which Heartland says it first discovered in October 2008, is yet another example of organizations not implementing the proper security solutions that could help prevent fraud before it occurs.

Although three men were arrested in Florida in February 2009 after trying to imprint the stolen data onto fake Visa gift cards, the investigation still believes that a more organization criminal element in eastern Europe is the catalyst behind the data breach.

As online identity attacks have become more prevalent, a significant number of users have decreased or even discontinued online transactions, particularly in the financial sector. This decline impacts not

only revenue growth from these channels but also can increase costs where users revert to costly call centers or brick-and-mortar channels.

It is inevitable that users will continue to be less willing to take the risk of using online services without better protection of their online identity. This leaves organizations subject to two negative impacts: increasing direct costs of attacks that drive directly to the corporate bottom line; and limited online service use, impacting both costs and revenue generation.

At the same time, there is a significant reward for organizations that address this issue and provide their users with better protection of their online identity — based both on retaining existing customers, as well as having them transact more business in the cost-effective online world.

### **Mandates and regulations**

With these widespread attacks, losses and data exposures perpetrated through phishing, man-in-the-middle attacks and other criminal activities becoming the norm, it is natural that industry bodies and governments step in. How effective they have been is not clear, but global regulations are in place to help provide guidelines to properly secure financial transactions.

A sampling of those that have received the most interest include the U.S.-based Federal Financial Institutions Examination Council (FFIEC) guidance and the Red Flag guidelines (FACTA), UK-based Faster Payments Initiative, and broad-sweeping South American legislation mandating strong authentication. Regardless of region, all focus on providing specific guidelines and reasons for improving defenses against online fraud.

### **Who can help and what can be done?**

A myriad of security vendors have stepped forward with proposed solutions to this important problem. While some are trusted sources of online security expertise, there are many newer players that lack the experience and know-how that larger organizations require.

Logically, the intent of online security is clear: to better protect individuals and businesses from online crime. However, the implementation details often are seemingly complex and difficult to comprehend. Around the globe today, organizations struggle with the question, "Where should we begin?"

Protecting the corporate brand, safeguarding customers and meeting the appropriate regulations are now primary security concerns. To properly address these requirements, organizations should partner with proven security vendors that offer the right balance of affordability, service and expertise.

The first step of this process is a thorough review of online activities and risk assessments to better understand what is really required for both authentication and fraud detection.

A strong first step should be the consideration of implementing a strong authentication solution that can be leveraged based on risk across multiple applications and user communities. Institutions must also strategically acquire and deploy additional online safeguards, including coupling online fraud detection with a range of multifactor authentication capabilities, as identified by the assessment.

Security threats will continue to evolve and organizations must develop solutions that can adapt to future challenges and protect consumers for the long term. Developing a strategic vision for securing online transactions means making security choices that will address today's requirements and can adapt to help meet tomorrow's challenges.

With this risk-based approach, organizations have the flexibility to implement varying levels of security for a given application (as opposed to a one-size-fits-all approach) dependent on the type of risk (e.g., high-volume transaction, sensitive account information) involved.

### **Benefits of coupling strong authentication with fraud detection**

One of the most effective ways of stimulating e-commerce and meeting industry regulations, the combination of a strong authentication platform with an online fraud detection solution can help organizations meet the challenges of online fraud.

Modern strong authentication solutions can now leverage risk assessment to determine the appropriate level of authentication. For example, a user checking their account balance from home has a different risk profile than someone attempting an interbank transfer from a foreign country.

Online organizations should deploy a solution that embodies flexibility and security, as defined by Gartner as a Versatile Authentication Server. Leveraging a solution like this enables organizations to choose from a variety of strong authentication methods that best align with the risk of a given transaction. This also allows authentication to be only as invasive as required by the risk to improve user acceptance.

A strong authentication solution simplifies the risk remediation process by allowing organizations to establish a clear risk-driven authentication policy. First, organizations can quickly establish policy around which transactions are considered higher risk, independent of user context. For example, a bank may decide that all inter-institution transfers of more than \$10,000 require additional authentication above and beyond username and password.

Organizations also can use authentication as an input to and output from their application's fraud detection capability. For example, a user

authenticating from a known device or computer when requesting to register a bill may be used as a valuable input in assessing the risk of that transaction. However, if the application determines that the bill being registered does not fit the transaction history and profile of the user, additional authentication can be requested from the solution.

A capable strong authentication platform should support a variety of authentication methods such as IP-geolocation, device identity, questions and answers, out-of-band one-time passcode (delivered via voice, SMS or e-mail), grid cards, digital certificates (PKI), and a range of one-time-password tokens. As an open platform, it should have the capability to be expanded and adapted to help security needs today and in the future.

Complementing the strong authentication platform, the fraud detection solution should defend against fraud attacks without impacting the user experience and should have no impact on existing applications. Ideally, it should be a cost-effective solution that can be rapidly deployed to all users and is interoperable with the given versatile authentication platform.

An additional component of this equation is the ability to leverage an open fraud intelligence network, which is an information-sharing service designed to help combat online fraud by consolidating and sharing key fraud behavior patterns and data among network participants. It is focused on providing participating members the latest fraud behaviors and tactics, as well as key data for helping to detect and combat fraud as it evolves.

### **Asking the right questions**

Not for the faint of heart, securing access to information and digital identities is a deep and arduous undertaking. Knowing where to start can be even more so. There are, however, specific questions an organization can consider when beginning the process of finding the right online security strategy.

Does the organization have to send its data to a third party to be analyzed? Can the organization afford to have a large staff of analysts investigate a high number of suspicious activities? Does the system require back-end integration with applications? Does the fraud platform allow organizations to actually stop the fraudulent transactions before the money leaves the financial institution? Does the fraud platform integrate with the vendor's authentication platform?

These are just a sampling of inquiries that should be considered when deploying a sound risk-based authentication solution to combat online fraud. The answers will vary from vendor to vendor, but understanding the needs of the organization will help decide which factors are simply important and which are absolutely vital.

### **Protecting customers, business**

As the criminal element continues to evolve and adapt, the security measures that organizations implement need to include sophisticated, forward-thinking solutions to secure the online channel and protect consumers, enterprises and end-users.

When addressing vital security requirements and regulatory compliance, organizations conducting online transactions need to strongly consider a solution that consists of a strong authentication platform, real-time fraud detection and an open fraud intelligence network.

Following this approach can help provide a successful long-term strategy for protecting consumers, enterprise users and citizens. Deploying this tactic with the help of a single, experienced vendor will instill a synergy that embraces interoperability, efficiency and cost-effectiveness.

[www.entrust.com](http://www.entrust.com)