WHITE PAPER

Security Solutions

Online Identity Management Needs a Universal Answer

In what the U.S. Justice Department is calling the largest identity theft case ever prosecuted, three suspects were indicted in August 2009 for stealing more than 130 million credit and debit card numbers from a payment processing company. The alleged criminals are believed to have targeted known computer system security weaknesses to steal the card numbers and then used them to make unauthorized purchases and bank withdrawals. The payment processing company puts the cost of the data breach at US$32 million, but the final bill may be far higher.

Many Identities, Many Risks

In the U.S., identity theft strikes nearly 10 million consumers every year.[i] That number is growing rapidly around the globe, with a 36 percent increase in the past two years in the U.K. alone.[ii] As people become more connected online—and pieces of their identities are more readily accessible—the potential to become a victim of identity theft grows exponentially.

According to Verizon Business Data Breach Investigations Reports, 900+ million records were compromised over the last six years in investigations analyzed by Verizon.[iii]

According to Internet World Statistics, as of 2009 an estimated 1.7 billion consumers conduct transactions online. That number will continue to grow as more people discover the value of online self-service. The Internet allows them to interact with, get access to, and share personal information with dozens of organizations in a wide variety of industries. Consumers can review insurance claims, pay utility bills, access tax-related accounts, manage personal finances, participate in social networking and gaming, and purchase a variety of goods, with just a few keystrokes.

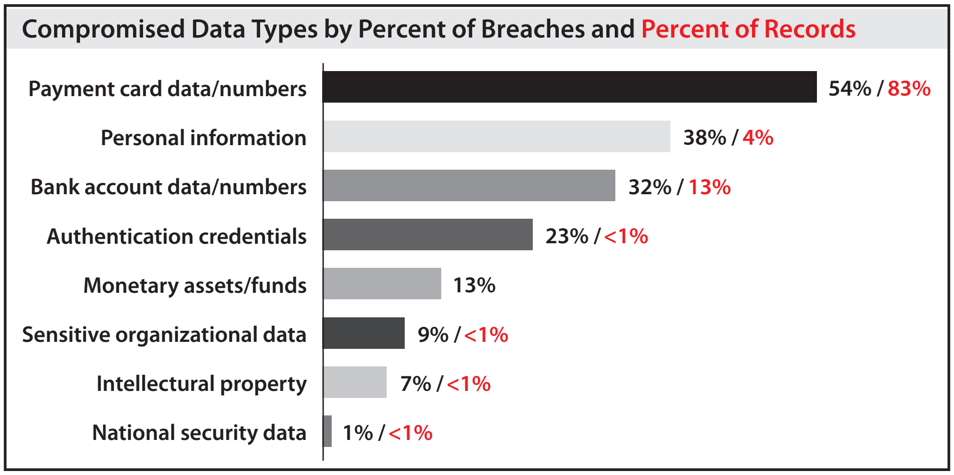
While online technology brings convenience, it also creates a dilemma. Because there is no single identity management platform for the Internet today, having numerous online relationships means managing multiple identities. And, when consumers head off to work, their list of identities grows further. Every online provider, and often every system, has its own authentication and access model depending on the level of identity assurance needed. This means users have to remember a variety of username and password combinations, possibly carry a hardware token device, or even use a smart card reader or biometric scanner. Having multiple, different usernames, passwords, and devices helps create more avenues for unauthorized access.

Identity Fraud Is Big Business

The lack of a single, user-friendly online identity access platform increases the risk of identity theft and identity fraud, and makes it difficult for people to find out they've been hit until it's too late. Evidence of this risk frequently appears in the news and has a widespread impact, affecting not only the person victimized, but also the organizations they do business with. Victims of identity theft can spend countless hours and, on average, lose hundreds or even thousands of dollars to resolve the impacts of the crime. Much of the costs related to identity theft are absorbed by online organizations around the world; losses to businesses and consumers around the world are estimated in the tens of billions of dollars annually.

The impact of identity theft and fraud as a result of vulnerabilities in online security is staggering. The financial costs include potential legal expenses and fines, additional costs to upgrade technology and the cost businesses fear the most: the cost of a damaged reputation.

The impact of identity theft and fraud as a result of vulnerabilities in online security is staggering. The financial costs include potential legal expenses and fines, additional costs to upgrade technology and the cost businesses fear the most: the cost of a damaged reputation. Replacing the loss of shareholders, share value, and especially the loss of customer trust after an incident can be very difficult. Consumers will be quick to avoid merchants that have suffered a breach, significantly impacting revenue.



Source: Verizon Data Breach Investigations Report[iv]

How Authentication Has Evolved

When the Internet first came of age, the commonly accepted form of online authentication was a username and password. This is still the case almost two decades later. However, as security threats evolve and more sensitive data becomes available online, authentication methods improved to not only include something a user knows, such as a username and password, but something a user has, like a hardware token device or smart card. The two methods combined can significantly reduce computer crimes. Biometrics further increase security strength, providing a third form of authentication such as something a user "is" (e.g., voice, fingerprint, face, iris, or retina).

Every country's government and even every industry has different requirements for online authentication. In the U.S., the National Institute of Standards and Technology (NIST) uses different authentication form factors to classify identity authentication security into four levels of assurance that range from low to very high. In Europe, the European Union (EU) has launched the E-Privacy Directive, which provides its own guidelines for addressing the protection of an individual's data—often interpreted differently in every country.

NIST Security Levels 1-4		
Level 1 – Low		You are who you say you are without any verification from a third party
Level 2 – Medium		You are who you say you are with some validation of government ID
Level 3 – High		You must prove who you are with two forms of government-issued picture ID, plus address verification, and have it reviewed by two people
Level 4 – Strictest		Same as Level 3 with the addition of a background check

HEALTHCARE-SPECIFIC CHALLENGES IN THE UNITED STATES

The healthcare industry is certainly not "immune" to the challenges of fraud, which is estimated to amount to as much as $226 billion dollars per year in the U.S.[v] Stolen identities are used to create fake medical records, allowing thieves to bill thousands of dollars in fraudulent claims to Medicare, the health insurance program managed by the U.S. government, and private insurance companies. Its impact goes far beyond dollars and can affect the future medical treatment of the victim.

Medicare fraud, in particular, is a big business for criminal organizations. On October 13, 2010, the U.S. Federal Bureau of Investigation (FBI) announced the arrest of 52 people across the U.S. in the largest Medicare fraud scheme ever executed by a single criminal organization. The organization billed Medicare over $100 million dollars for treatments never performed by using the stolen identities of approximately 2,900 patients from the Orange Regional Medical Center in New York.[vi]

These challenges have driven the U.S.-based healthcare sector to implement a stronger identity assurance model. The Health Information Technology for Economic and Clinical Health (HITECH) Act, signed into law in 2009, addresses the privacy and security of electronic health information and strengthens the enforcement of the Health Insurance Portability and Accountability Act (HIPAA) rules. Healthcare providers are aggressively working to meet these new standards and get all medical records online by 2016, when fines begin for those out of compliance. The new requirements also raise the bar on electronic prescriptions of controlled medications, requiring doctors, medical personnel, and anyone touching an electronic medical record to use advanced authentication methods.

Good, but Not Good Enough

As effective as these security methods can be, significant challenges still remain, leaving organizations stuck between a rock and a hard place. Stronger security increases the cost exponentially and is not always worth the tradeoff. Other forms of security are difficult to use and expensive to support, preventing their mass adoption. And, while current security measures may conform to standards like NIST, government documents can be easily bought on the black market. All of these issues ultimately create the weaknesses that identity thieves exploit.

High Costs

Probably the single biggest challenge to organizations, both public and private, is the high cost to implement and manage authentication. These costs can vary widely, depending on how authentication is addressed. Simple username and password methods are the least expensive but also offer the least amount of protection. When combined with security devices and other forms of authentication, the risk can be greatly reduced but the cost can be difficult to justify.

Probably the single biggest challenge to organizations, both public and private, is the high cost to implement and manage authentication.

There are five primary cost components to authentication:

- Identity Proofing. The process of identity confirmation requires in-person verification with presentation of multiple forms of ID. The cost varies depending on who is obtaining what information but is estimated, on average, to be $50 or more per user in the healthcare industry alone.
- Credential Lifecycle Management. Issuance, revocation, and renewal of the credentials for each credential type and for each different type of user in the enterprise is done independently. To date, one service for all does not exist.
- Security Devices. Devices like hardware tokens, smart cards and readers, and biometric scanners can run between US$20 and $100 for each device, not including back-end authentication systems to support these components, such as ACE and OATH servers.
- Application Integration. Integrating security across applications so that each system can use the same credentials for authentication can be expensive, for even the largest enterprises. Based on the number of users and applications they must access, up-front hardware, software, tokens, single sign-on and web access management software can increase these costs exponentially.
- Support. User support costs can exceed all of the other costs combined. Password resets are among the highest number of technical support requests and security devices further add to support costs when they break or are lost.

These various costs must all be justified against potential risk. For example, for a large U.S. bank, NIST Level 3 authentication would most effectively reduce losses from identity theft and fraud. But the financial risk is almost certainly less than the cost of robust authentication. To date, organizations have not been able to cost-effectively scale Level 3 authentication for large deployments, leaving most to accept the "Medium" identity assurance provided by Level 2.

User Complexity

User complexity is probably the single biggest weakness with existing authentication methods. Today, the most common form of online access for both consumers and business users is the username and password combination. However, with access to dozens of sites, users find it hard to remember their credentials for each site. For one site, the username may be an e-mail address and for another, a chosen alias. Password requirements vary from free form to restricted formats, and may be set to expire on a regular basis. This means today's users have a lot to remember when accessing different online sites, leaving many to reuse the same password or maintain a username and password list on their computer, which defeats the purpose of the security measure.

User complexity is probably the single biggest weakness with existing authentication methods.

While hardware tokens, biometrics, and smart cards can provide stronger protection, many users have no experience with these methods and might find them hard to use. Software and devices, like smart card and biometric readers, must be installed, which can be complicated and may require ongoing technical support. These devices may also be easily lost, forgotten, stolen, or broken. And, the devices are not always portable. Readers and token devices may not work on technology the user doesn't own, like that of friends, other companies, or public computers. So, users can't easily access restricted accounts when they're not using their own computer.

Liability

The decision of who should bear the cost of charges or damages incurred by fraudulent identity use can be an expensive one. Today, most companies doing business online have chosen to cover the liability expense themselves. For them, the cost of increasing protection is greater than the cost of losses resulting from fraudulent access. While most have agreed to accept their own liability, should these same online providers still be expected to pay for losses that occur as a result of identities stolen from another online provider?

Online providers that do use advanced methods, particularly PKI, often rely on third-party identity service providers. These providers have lengthy documents that define liability consequences should their methods ever fail. The zero-error rate specified in these types of contracts is not practical or sustainable. Because of the potential risk, third-party providers often operate under corporate shells with little or no assets. Liability models of unknown and unlimited liability simply cannot scale for the hundreds of thousands of online merchants and businesses that deal with hundreds of millions of users.

Enterprise Complexity

For the enterprise, managing online security means having to bear both its cost and complexity. For many, strict information security compliance requirements must be addressed, increasing the difficulty. Online providers handling credit cards are expected to comply with financial standards such as PCI DSS, which requires credit card information to be adequately encrypted, transmitted, and stored. These difficulties show up quickly in data breaches. Of the organizations that experienced a data breach analyzed by Verizon in 2009, 79 percent of those subject to PCI DSS compliance had not yet achieved it.[vii]

Providing access beyond an organization’s own employees puts additional pressure on existing identity services to manage users that companies have less control over and exposes systems to additional risks.

Compliance issues aside, most organizations have to manage security applications in multiple systems for both business users and customers. Disparate systems often use different security applications and standards, leaving organizations to deal with the challenges of managing multiple applications or the difficulty integrating them. Some have worked toward implementing single sign-on capabilities with web-access management software, but this option is costly and time consuming, especially when incorporating more advanced security methods.

Lastly, traditional corporate security boundaries are blurring as companies allow system access to partners, suppliers, and even customers. Providing access beyond an organization’s own employees puts additional pressure on existing identity services to manage users that companies have less control over and exposes systems to additional risks.

Lack of Mass Adoption

Mass adoption of any authentication method requires acceptance by both a large majority of users and organizations providing online access. Stronger methods, like smart cards, hardware tokens, and biometrics, have not been able to replace username and password authentication. Doing so would require the provisioning and credentialing of hundreds of millions of users across all industries, private and public. Going forward, each authenticator would have to trust in the diligence and accuracy of the original identity issuer and then configure their own systems to accept a singular authentication method. Without every online party “buying in” to the solution, mass adoption will not happen.

Instead of continuing to try to solve authentication problems with the same methods that have been used in the past, it’s time to think differently and create a new identity assurance and authentication model—a universal identity solution.

Today’s users have their own concerns about a single authentication solution, such as smart cards and biometrics. These methods must be registered and maintained in a single authentication management system, and users fear that a breach to that system could put their entire livelihood at risk. It would also be difficult to find an authentication management service willing to assume this level of liability.

Time for a Revolution

Instead of continuing to try to solve authentication problems with the same methods that have been used in the past, it’s time to think differently and create a new identity assurance and authentication model—a universal identity solution. With more users transacting business online every day, authentication services must remain one step ahead of criminals, while at the same time reducing the risk and complexity and controlling the cost associated with authenticating online access.

Reduce Risk

Current authentication methods needn't be discarded. Instead, add techniques that appropriately raise the level of assurance. A new universal identity solution would not just rely on what a person knows (their username and password) or what they have (security device), but also on who they are. Doing so would greatly reduce the risk of identity fraud. Accomplishing this greater protection need not be complicated or expensive, but does need to leverage additional user information already available and work with devices users already have.

Integrating contextual information about the user with existing authentication methods greatly reduces the ability of identity thieves to access personal account information. New, dynamic authentication techniques should combine a broad range of user attributes, such as matching the geo-location of the user's mobile phone to their IP address, comparing a computer's IP address against a list of compromised IP addresses, asking pre-established security questions, matching real-time biometrics like a voiceprint or keyboard patterns, and asking dynamically-generated authentication questions based on a variety of data sources. Even if a person's identity is stolen, these methods help make it difficult for the criminal to use that person's identity to commit fraud at the expense of the consumer and the online party.

Easy to Use

It's important that a universal identity solution be as easy as possible for consumers and businesses to use. Much like there are now several ways to unlock a car, such as physical keys, remote controls, and keypads, users should have access authentication options that fit their personal preferences. These might include the use of different devices and the use of personal information and should be flexible enough to accommodate additional options in the future. For example, the presence of a mobile phone near a laptop could unlock the laptop. As the user walks away with the mobile phone, the laptop would lock again.

Preserve User Privacy

Personal privacy and the protection of personally identifiable information become even more critical as nearly everything about a user becomes accessible online. Because of this, a universal identity solution should be able to authenticate users with online sites based on their persona for that site, without having to give up personal data, such as his name. For example, the solution could identify and authenticate a doctor by comparing enough contextual information about him, such as his employer and his affiliation with his medical association, to verify with a high degree of certainty that the user is indeed the licensed doctor associated with the identity credentials. The organization requesting identity confirmation only need submit the request, not the user's data, through the universal identity solution, and receive a "yes" or "no" response in return.

Personal privacy and the protection of personally identifiable information become even more critical as nearly everything about a user becomes accessible online.

Control Cost and Reduce Complexity

A universal identity solution should be delivered as a cloud-based service, eliminating the in-house resources required for setup, configuration, testing, and ongoing support. In most organizations, identity and access management is not a core competency and a universal identity service offered by experts would relieve IT from having to learn and maintain these evolving, specialized skills. Additionally, a cloud-based identity and authentication service could quickly scale as needed, be available to users almost wherever they are, and ease integration challenges.

To further support integration, it's imperative that a universal identity solution support every open standard and proprietary protocol—including SAML, OpenID, Microsoft® Active Directory®, Kerberos, X.509, and others. This will allow the enterprise to integrate this new security access model with existing applications and systems easily while managing costs. In addition, there must be a means to integrate legacy systems that don't support standards.

Provide Adjustable Levels of Assurance

Unfortunately, there is no way to provide a 100 percent guarantee against identity fraud, although today's identity service providers are generally held liable to a zero-breach standard. A universal identity solution should incorporate a risk-based pricing model that varies based on levels of assurance. Using a service level agreement (SLA) approach, the universal identity solution provider would support an agreed-upon error rate depending on the level of assurance needed. Banks, for example, would subscribe to an

SLA providing higher levels of assurance, but would pay more per user. A risk-based approach is both sustainable and scalable, and encourages many more identity service providers to offer stronger and more advanced authentication services.

Take Part in Shaping the Future

Governments, commercial entities, and consumer-focused organizations all desire an online authentication solution that simplifies the process for both themselves and those that access their online systems, and provides strong protection against identity fraud. This paper outlined several ideas that could transform the way online authentication is done today and may provide the secure online digital identity that both business and consumers need.

Creating a universal identity solution that meets the needs of every industry cannot be done in isolation. It requires the collaboration of professionals from all industries to understand and accommodate the issues each industry faces. It also requires creative thinking to move beyond the traditional methods and create a new solution that will be readily adopted by the marketplace.

Verizon has created a group called the Verizon Universal Identity Alliance to provide a forum for leaders to come together and work collaboratively toward a universal identity solution. And, to support the specific needs of the healthcare industry, Verizon is also heading the Verizon Medical Identity Consortium. These groups, which will be made up of stakeholders across all industries, will define and shape a new solution, including exploring risk-based service level agreements, identity confidence scoring, user attribute sharing, and technology interoperability.

Verizon, a recognized leader in security solutions and known for its groundbreaking Data Breach Investigation Reports, invites you to join its efforts to develop a universal identity solution by learning more about either the Universal Identity Alliance or Medical Identity Consortium. With insight gained from managing over 25 identity programs for countries around the globe, our expansive IP network, and from working with nearly all of the Fortune 500 companies, Verizon has a clear understanding of the security issues facing today's enterprises. Together, the Universal Identity Alliance and Medical Identity Consortium groups will work together with Verizon to shape the future of identity access management. To be a part of this ground-breaking effort, you can:

- Contact a Verizon Business account manager to learn more.
- Visit verizonbusiness.com.

While today's online authentication methods should be sufficient to help prevent identity fraud, news headlines say otherwise. There is no shortage of stories that describe the identity breaches that occur on a regular basis. Identity thieves continue to evolve their methods to thwart existing barriers. The solution to staying one step ahead of these thieves lies in the brilliant minds of those who deal with security every day. With those thieves gaining ground, it's time to take online identity management to the next level.

About Verizon Business

Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.

[i] ftc.gov/bcp/edu/microsites/idtheft/downloads/FTC_DDD_One-pager.pdf

[ii] Cost of UK Data Breaches up 7% in 2009, Warwick Ashford, ComputerWeekly.com, January 28, 2010, computerweekly.com/Articles/2010/01/28/240101/Cost-of-UK-data-breaches-up-7-in-2009.htm

[iii] 2010 Data Breach Investigations Report, Verizon Business, verizonbusiness.com/resources/reports/rp_2010-DBIR-combined-reports_en_xg.pdf

[iv] 2010 Data Breach Investigations Report, Verizon Business, verizonbusiness.com/resources/reports/rp_2010-DBIR-combined-reports_en_xg.pdf

[v] The Problem of Health Care Fraud, nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud

[vi] Manhattan U.S. Attorney Charges 44 Members and Associates of an Armenian-American Organized Crime Enterprise with $100 Million Medicare Fraud, Federal Bureau of Investigation, October, 13, 2010, newyork.fbi.gov/dojpressrel/pressrel10/nyfo101310.htm

[vii] Data Breach Investigations Report, Verizon Business, verizonbusiness.com/resources/reports/rp_2010-DBIR-combined-reports_en_xg.pdf

verizonbusiness.com

verizonbusiness.com/socialmedia verizonbusiness.com/thinkforward