

Abstract

The combination of online banking's rising popularity and the increasing number of online services offered by financial organizations indicates a bright future for e-banking. However, to maximize such potential, financial institutions must overcome a major obstacle: identity theft. Identity (ID) theft, particularly phishing, is rapidly spreading worldwide, and straining the mutual trust between financial institutions and their customers that is a prerequisite for secure online banking. With identity theft leading to significant financial losses and decreased customer usage of online banking services, it is one issue that cannot be ignored.

Many financial organizations are looking to implement proactive security measures to combat identity theft. Strong authentication – a security method which employs the use of more than one factor to identify users accessing private networks and applications – is among today's leading choices. Enabling easy and secure implementation of certificate-based security applications, strong authentication provides banks with the foundation for implementing end-to-end security and a range of secure online services for its customers.

By improving security controls at every point in the banking infrastructure – from internal access by employees and partners to external access by customers – strong authentication not only combats identity theft and fraud, but also helps banks meet mandatory compliance regulations. Further, by enabling additional services such as secure money transfers, digital signing of loan applications, and stock trading, strong authentication solutions deliver quantifiable returns on investment (ROI) in the form of increased revenues, customer acquisition and retention as well as reduced operational costs.

The Identity Theft Phenomenon

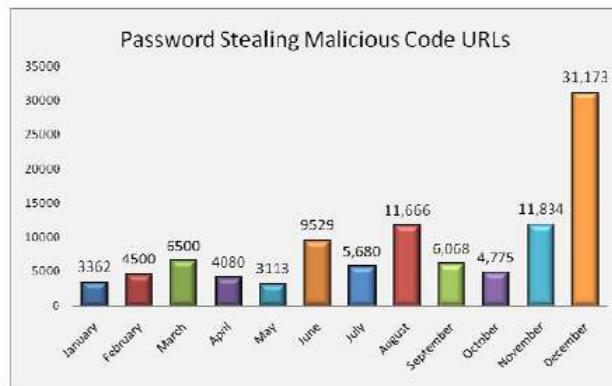
Identity theft is preventing financial institutions and their customers from achieving a secure world for online banking. About 7.5 percent of U.S. adults lost money to some sort of financial fraud in the year ending September 2008 and data losses cost companies an average of \$6.6 million per breach. Moreover, churn due to a data breach was almost double the regular rate 6.5% vs. 3.6%, and financial services faced a high turnover of 5.5%¹.

One of the major ID theft culprits is phishing, a type of online fraud. In phishing schemes, “e-thieves” steal confidential data such as passwords, credit card numbers and user IDs from individuals. Typically this is done by sending an email which redirects a user to a counterfeit web site designed to mirror a legitimate site such as an online credit card or banking site, in order to deceive an individual into submitting their personal credentials.

Called the “hottest, and most troublesome, new scam on the Internet” by the Federal Bureau of Investigation (FBI), the number of crimeware spreading sites infecting PCs with password stealing reached an all time high of 31,173 in December, an 827 percent increase from January of 2008².

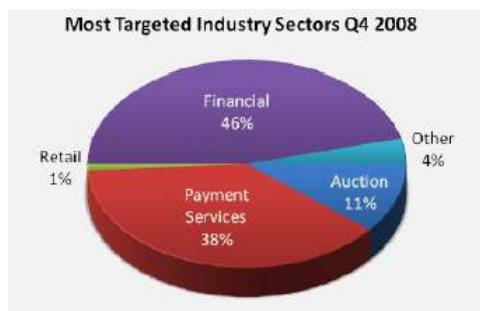
Approximately 7.5 percent of U.S. adults lost money to some sort of financial fraud in the year ending September 2008 and data losses cost companies an average of \$6.6 million per breach.

Gartner, 2009



Banks Hardest Hit

Financial institutions are the most vulnerable and hardest hit victims of phishing. According to the Anti-Phishing Working Group (APWG), the financial services sector is consistently the most targeted industry for phishing attacks, with financial institutions representing 46% of organizations attacked in 2008. To drive the point home, 93% of all electronic records breaches occurred in the financial services industry. And of these, 90% had ties to organized crime³.



¹ Gartner, Inc. February 2009, ID: 165825, “Data breach and financial crimes scare consumers away.”

² Anti-Phishing Working Group, March 2009

³ Verizon Data Breach Investigations Report, 2009.

Authentication in Response

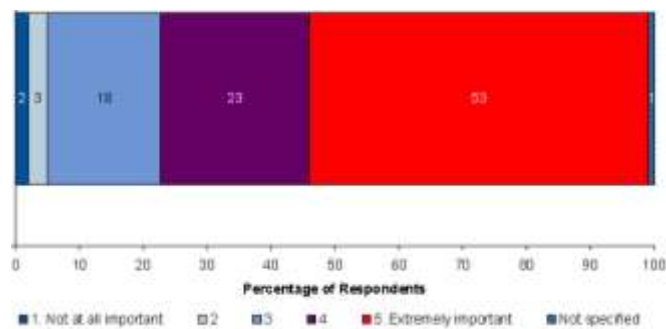
When it comes to network and Internet security, traditional password authentication, whereby a user has to provide a user name and password, remains the method of choice for most financial institutions worldwide.

Despite its popularity, password authentication is not ideal for either banks or their customers. Customers often maintain several user IDs and constantly changing passwords for a variety of online services and applications, making personal password management unwieldy. Banks, meanwhile, need to allocate significant resources, particularly help desk personnel and IT administrators, to manage password usage. More importantly, however, the sharp increase in ID theft and phishing is neutralizing the effectiveness of traditional password authentication: customers feel more vulnerable than ever, while banks are being exposed to unprecedented levels of fraud risk.

Password-based authentication poses security problems for banks not only at the customer level, but also at all network infrastructure points, starting from within the institution itself. Employees required to handle multiple passwords often either choose easy-to-remember words and numbers, or write them down, thereby increasing the risk that their access credentials will fall into the wrong hands. Without stronger controls on internal networks, applications and data, financial organizations are more vulnerable to internal ID theft attacks and losses.

There is a great need to restore the foundation upon which successful financial services rest – the mutual trust between banks and their customers. Indeed, customers themselves are now a driving force for better security at financial organizations. According to a 2008 Gartner report⁴, 53% of customers say security features will influence their decision to bank online.

According to a 2008 Gartner report, 53% of customers say security features will influence their decision to bank online.



Gartner Survey Results: Importance of Security Features in Influencing Consumers to Bank Online

⁴ Gartner, Inc. 28 May 2008, ID: G00158229, "Banks Need to Strengthen User Authentication While Appeasing Consumers."

Added Layer of Protection

Among the most popular and successful ID theft solutions is strong authentication. Also known as two-factor authentication, strong authentication involves the use of more than one factor to identify users accessing private networks and applications. Strong authentication combines “something you know” - such as a physical token - with “something you have” – a password for example - in order to verify a user’s identity.

Strong authentication which, according to the U.S. Federal Deposit Insurance Corp. (FDIC), “has the potential to eliminate, or significantly reduce, account hijacking” is recognized as a legitimate form for safeguarding consumer accounts. The number one recommendation from leading IAM analyst firm, Gartner is that custodians of customer accounts should employ “stronger user authentication, continuous fraud detection and out-of-band transaction verification” to prevent confidential information and data breaches⁵.

The authentication methodology that organizations choose to deploy is based on different factors, including: the level of security required, the range of security applications required, regulations that need to be met and ease-of-use for end users. Several of these options are discussed below.

Tokens as a Leading Option

Strong authentication methods can take many forms and continue to evolve with improved technology and innovation. Historically, the most common form factors were One-Time Password (OTP) devices and credit card-like Smartcards. More recently, the proliferation of USB tokens, software-based authenticators and hybrid devices which combine OTP and USB functionality in one device, has increased significantly. A brief description of each of these strong authentication methods follows.

- **Smartcards**

Smartcards are credit card-sized devices that contain highly secure microprocessor chips dedicated for cryptographic operations. To authenticate, users must insert their smart cards into a reader device on the PC and enter a password. Smart cards provide highly secure storage of user credentials and keys. They also secure PKI implementation by generating keys and performing cryptographic operations on-board, without ever exposing the user’s private key to the computer environment.

- **Smartcard-based USB Authenticators**

Smartcard-based USB authenticators, combine the convenience of a USB device which plugs into a computer’s USB port and the security of a smart card chip. In this way, USB authenticators leverage the advantages of both USB tokens and smart cards to provide the greatest level of security and versatility. USB authenticators enable a broad range of security solutions and provide all of the benefits of a traditional smartcard and reader — without requiring the separate reader.

- **One-time Password (OTP) Authenticators**

OTP authenticators are small handheld devices that allow authentication using onetime passwords generated by the device, based on a secret key shared by the device and an authentication server. A user wishing to authenticate enters the one-time password appearing on the token, and this value is compared to the value generated by the authentication server. While OTP tokens are highly portable, they do not provide the same level of support for multiple security applications that USB tokens and smart cards offer.

According to the U.S. Federal Deposit Insurance Corp (FDIC), strong authentication “has the potential to eliminate, or significantly reduce, account hijacking” and is recognized as a legitimate form for safeguarding consumer accounts.

⁵ Gartner, Inc. April 2009, “The War on Phishing Is Far from Over,” Avivah Litan, ID 166605

- **Hybrid Authenticators**

Hybrid authenticators provide multiple types of functionality, which increases flexibility. Hybrid USB and OTP tokens allow full USB-based strong authentication and security solutions, as well as OTP-based strong authentication in detached mode when needed. Smartcard-based hybrid tokens that use the smart card chip for both USB and OTP functionalities provide maximum security.

New Trends in Authentication

Beyond the strong authentication methods mentioned above, over the past few years there have been innovations in authentication that open up the playing field to more flexible and diverse solutions.

Mobile Out of Band Authentication Solutions

Out of Band Authentication (OOB) is based on the two-factor authentication model but utilizes a combination of software authentication together with separate information channels for authentication and access. OOB methods leverage the one device users already have, such as a mobile phone, handheld device or PC, in order to generate passwords that facilitate authentication. Examples of OOB authentication include authentication via SMS in which an SMS is sent to a mobile phone for authentication, a voice callback to a phone for authentication or software-based authentication in which passwords are generated by software that resides on a mobile phone.

While very convenient and cost effective, OOB authentication methods are not as secure as traditional two-factor authentication methods. OOB methods are also dependent on mobile network coverage for the delivery of passwords to mobile devices. Lack of coverage can result in delayed delivery or delivery failure.

Reader-less USB Authenticators

Reader-less USB authenticators are an innovative form of USB certificate-based authenticators that, unlike regular USB certificate-based authenticators, do not require middleware on the end-user computer. Reader-less USB certificate-based authenticators offer the security of PKI technology with a much higher level of convenience and portability since they can be used on any compute that has a USB port and Internet connection.

Software Authenticators

Software authenticators enable strong authentication without a dedicated physical device. These tokens are software applications that can be stored on a user's computer, or on mobile devices such as a mobile phone or PDA. Software authenticators can utilize either PKI (certificate-based) or OTP technology. While software authenticators are convenient for users, they are less secure than physical tokens because the secret key can be stolen or misused more easily than with a physical authentication device.

Strong Authentication Benefits:

- Compliance with privacy regulations
- Protection of sensitive customer data and transactions at every point in the system
- Improved customer care through higher availability of online services and greater customer confidence
- Ability to move services online and reduce brick & mortar costs

SafeNet Solutions:

- eToken PRO Anywhere
- Software authentication
- SafeWord OTP Solutions

Strong Authentication Solution Checklist

With strong authentication, financial institutions don't have to dream about secure e-banking any longer. The following list reviews the most important features organizations should consider when adopting a strong authentication solution.

✓ **Secure**

A strong authentication solution must deliver the highest level of security, including on-board generation of keys and secure storage of personal credentials such as passwords and digital certificates. In addition, the strong authentication process should be robust, with customers required to use strong passwords and/or PINs.

✓ **Easy to Deploy**

The solution must enable easy token deployment via automated distribution, enrollment and personalization (i.e. individual or group characteristics) capabilities, and via user self-service token enrollment and maintenance capabilities, thereby minimizing an organization's helpdesk resources.

✓ **Easy to Use**

The solution should be user friendly; otherwise customers will not be inclined to take advantage of new online banking opportunities.

✓ **Easy to Manage**

Each financial institution needs to be able to manage an overall security solution without requiring extensive changes and heavy investments in IT infrastructure. The solution also should enable a range of token management functions including Web-based user self-service token enrollment and maintenance, automatic backup and restoration of user credentials, back-end token administration, and easy handling of lost and damaged tokens.

✓ **Portable**

The solution should be functional in a range of environments, including home, work and public locations, such as Internet cafes. In addition, it should be fully portable and easy to carry.

✓ **Value-Added Enabler**

The solution should allow financial institutions to provide a value-added offering that includes security services such as laptop security, credential management and file encryption – all with the same token. In this way, organizations can differentiate themselves from the competition, increase user acceptance of tokens, and enjoy the flexibility of providing additional security services in the future without increasing infrastructure investment.

Toward a More Secure Banking Environment

It may be difficult for financial institutions and their customers to envision a world where their information and transactions are secure from threats like phishing and identity theft. However, such solutions, in fact, exist today providing:

- secure, trusted connectivity between a financial organization and each and every customer;
- the same strong, easy-to-use security utilized in ATM transactions for online banking, giving banks the confidence that customers who appear to be conducting transactions are indeed those who are doing so;
- confidence to customers that their privacy, identity and financial assets are not being compromised;
- tight and enforceable security controls wherever valuable customer information resides, from internal databases to mobile devices such as laptops;
- the ability for banks to securely offer all of their services online – from foreign exchange through money transfers to mortgages;
- an equal level of customer confidence and sense of security in e-banking as with brick-and-mortar banking.

By securing their networks and data with strong authentication technology, financial institutions can turn this world into a reality.

SafeNet Authentication Solutions for Online Banking and Financial Services

SafeNet's strong authentication solutions offer business value for e-banking and related online services on a platform that is intuitive and easy to use. Offering a broad range of hardware and software-based solutions, SafeNet's authentication portfolio strikes the ideal balance between strong security and ease-of-use giving organizations the freedom to customize and grow their solutions to meet their needs not only today but also in the future. And with a focus on providing comprehensive, end-to-end security, SafeNet enables companies to protect sensitive customer data and transactions at every point in the system, from internal databases and employee laptops, to corporate transactions and online consumer banking.

Comprised of a wide range of devices, security applications and third-party integrated solutions with over 100 partners, the SafeNet authentication offering gives financial institutions the ability to rapidly implement a full suite of security solutions. Alternatively, for those seeking to address a singular need initially, organizations can implement a portion of the offering while future-proofing their investment, and gradually add other security features onto the same SafeNet platform later on.

But the mere availability of secure tokens is not enough – financial institutions also need enterprise-level deployment and lifecycle management capabilities to optimize token usage and efficiencies. To address this need, SafeNet offers eToken TMS which manages all aspects of assignment, deployment and personalization of tokens and related security solutions.

Below are details on some specific authentication solutions that are ideal for online banking and financial services.

eToken PRO Anywhere

eToken PRO Anywhere is the industry's first and only readerless smartcard USB token that enables certificate-based (PKI) applications such as secure web and email access, digital signature, encryption, decryption, from any computer. It does not require installation of any client software on the access computer, making this a highly secure and portable device.

Software Authenticators

SafeNet offers both certificate-based and OTP software authentication solutions that combine the security of proven two-factor authentication with the convenience of authentication via a personal mobile device or PC.

SafeWord OTP Solutions

SafeNet's simple to deploy and easy to use SafeWord OTP solutions enable businesses to quickly set up strong authentication for network access in a matter of minutes. SafeWord packages are ideal for Windows environments, offering seamless integration with Microsoft Active Directory.

eToken Token Management System (TMS)

TMS is a central fully configurable management platform that links security devices with users, organizational rules, and the associated security applications in a system. TMS enables centralized control of all authentication devices, for seamless deployment, administration and user management.

About SafeNet

In 2007, SafeNet was acquired by Vector Capital, a \$2 billion private equity firm specializing in the technology sector. Vector Capital acquired Aladdin in March of 2009, and placed it under common management with SafeNet. Together, these global leading companies are the third largest information security company in the world, which brings to market integrated solutions required to solve customers' increasing security challenges. SafeNet's encryption technology solutions protect communications, intellectual property and digital identities for enterprises and government organizations. Aladdin's software protection, licensing and authentication solutions protect companies' information, assets and employees from piracy and fraud. Together, SafeNet and Aladdin have a combined history of more than 50 years of security expertise in more than 100 countries around the globe. Aladdin is expected to be fully integrated into SafeNet in the future. For more information, visit www.safenet-inc.com or www.aladdin.com.