



Retail Internet Banking

Regulatory Compliance & Future Security

In 2004, almost ten million Americans fell victim to various identity theft fraud schemes and nearly two million Internet users in the U.S. experienced some type of account hijacking. With global fraud losses estimated at \$50 billion dollars annually, identity theft is rapidly becoming one of the fastest growing types of consumer fraud impacting the financial industry.

The majority of consumers use their online financial account access to pay bills, transfer monies, and review banking, credit card, and investment account information. Increasingly, fraud perpetrators specifically target these consumer activities because they are the most susceptible and easiest consumer to fall victim to account-hijacking known as phishing. Phishing is the process of sending tens of thousands of bogus e-mails and/or WebPages to customers masquerading as a legitimate financial institution seeking confidential financial information.

In order to combat identity theft fraud and/or phishing, regulators and/or Congress have increased their efforts by introducing various new industry guidance and/or legislation. In the examination of these various recommended changes, the most common theme is the elimination of retail Internet banking reliance on existing customers' single-factor password authentication systems moving towards a two-factor customer authentication system for accessing online banking account information.

What are existing customers' single-factor password authentication systems? They are Internet banking products that solely rely on static username and/or password ID(s) to verify user identity and grant account access. In essence, single-factor authentication systems significantly limit financial institutions' security protection measures because it places account access security in the hands of their customers that firewalls and/or virus protection software simply cannot catch. Although financial institutions customers' bad password habits are the leading cause of identity theft crimes concerning online banking accounts, ultimately, financial institutions bear the burden for protecting their customers' confidential information and offsetting any customer losses occurred due to account-hijacking fraud.

What are online customers' two-factor password authentication systems? Two-factor online authentication systems rely on something known by the customer such as a username and/or password ID(s), in addition to the use of a physical device for identity validation. The most commonly known deployment of two-factor authentication within the financial industry is ATMs and their use of PINs and cards to obtain account access. Similar to that of an ATM card, if a two-factor online device is lost and/or stolen, it is rendered useless to thieves because most likely a thief will not have access to a customer's username and/or password ID information, and visa-versa. Regulators and/or Congress have declared that two-factor online authentication systems have the potential to eliminate, or significantly reduce online identity theft fraud occurring by the following:

Keystroke Monitoring Trojans: *The use of stealth software programs that monitor and/or store keystrokes that users enter into their keyboard and then forwards this information to the criminal.*

Social Engineering: *This form of attack is when an impostor persuades a financial institution's employee to reveal password and/or account information over the phone by claiming to be someone else. Shoulder surfing is another form of social engineering.*

Man-in-the-Middle Attack: With this type of attack, a computer is set up as an interface between a customer computer and a financial institution server that handles authentication. The computer in the middle accepts the client's password as if it were the server and logs in to the server using the customer identity. Server access is granted to the "man in the middle," which in turn passes information to the client's machine. The result is the client's unique login information has been taken without the user's knowledge.

Network Monitoring: Also known as sniffing, network monitoring occurs when a computer on a network looks for message streams that contain words such as password and/or login.

Password Cracking: Also known as a brute force attack, this type of security breach is a result of repeated login attempts with different key combinations and/or words. For example, on cnet.com there are free readily available applications designed to guess passwords by using dictionaries to look up common words, names of children and word combinations.

Key Under the Mat: One of the most common ways that passwords are compromised is when users access financial account information via a kiosk and/or unsecured wireless network.

Internal Employee Fraud: Security compromised due to a disgruntled and/or disenfranchised employee.

Phishing Breaches: The process of sending tens of thousands of bogus e-mails and/or WebPages to customers masquerading as a legitimate financial institution seeking confidential financial information.

As you can envision, two-factor authentication systems come in many unique solutions such as hand geometry, voice verification, iris scanning and facial recognition. Online consumer customers expect to have immediate and/or unobstructed access to their online accounts regardless of where they happen to be or what time it is. Qualities such as portability, reliability, multiple account access, regulatory compliance, reasonable cost, and ease of implementation will mostly likely determine what technologies become industry standard.

What appears to be on the vanguard is the widely used European solution of a Universal Standard Bus (USB) two-factor authentication keychain device. At a current cost of \$10.00-per device, this present solution enables online users to plug & play and obtain access into their financial online accounts with universal portability and ease of use.



Over the past few years, it has become increasingly apparent that regulators no longer believe that single-factor authentication methods are sufficient in properly securing online customer confidential information. Increasingly, they are commenting on the effectiveness of the European solution. Notwithstanding, one of the European solution deficiencies if deployed in the U.S. in its current form is the consideration of the U.S. consumer marketplace to have multiple financial accounts at numerous financial organizations. Consequently, we believe that new regulations will be enacted within the next several years requiring two-factor authentication systems for all online banking providers and/or financial institutions.