



# **Solving the Weakest Link in Financial Institutions Network Security: Passwords**

A Comprehensive Review

A Digital Persona, Inc. White Paper

By Vance Bjorn, Chief Technology Officer

September 2006

Digital Persona, Inc.  
1+ 650.474.4000  
[www.digitalpersona.com](http://www.digitalpersona.com)

## Table of Contents

Solving the Weakest Link in Financial Institutions: Password Security .....	1
Introduction.....	1
Passwords: The Weakest Link.....	1
The Cost to Institutions.....	2
Government Compliance.....	3
Alternative Authentication Solutions.....	3
Complete Fingerprint Authentication.....	5
A Look at ROI.....	6
Summary .....	7
About Digital Persona.....	7

## Introduction

Ensuring the security of access to computer systems and data is one of the key concerns facing financial institutions. The need to safeguard these assets from both internal and external threats has never been more urgent. Within a six month time frame, The Computer Emergency Response Team (CERT) reported over 70,000 security incidents.<sup>1</sup>

While IT spending on security continues to rise to meet these increasing threats, every new technology solution that is considered must deliver significant return-on-investment (ROI) and leverage existing technology to justify costs.

Passwords are still the most pervasive tool used to secure access to networks and databases. As the number of passwords per employee increases, the likelihood of them being forgotten rises. As a result, the costs of managing password-based security represent a growing burden for most organizations.

- 40% of all help desk calls are for forgotten passwords.
- Each year organizations spend up to \$150 per user trying to maintain secure passwords.
- Up to 15% of annual IT budget is spent on information security.

**Gartner Group**

Even more problematic, the dependence on password-based systems has increased vulnerabilities for institutions because many end-user password management practices cannot be policed resulting in loose practices and passwords being stolen, shared or intercepted.

This paper proposes a new approach to improving security by replacing the need for user-entered passwords with a simple touch of a finger, effectively eliminating the vulnerabilities and costs of the network's weakest link.

The remainder of this paper describes:

- The problems and costs of password practices in organizations.
- The strengths and weaknesses of most existing security solutions: passwords, tokens, single sign-on, etc.
- How organizations can implement fingerprint recognition technology to achieve secure authentication in their organizations.
- The ROI of fingerprint authentication solutions.

## Passwords: The Weakest Link

Security experts tell us to start by identifying the weakest links in our systems, and to work on improving the security of those elements to mitigate risk. For many, password authentication is the weakest link in the security infrastructure.

According to the Computer Emergency Response Team<sup>2</sup> (CERT), 80% of the security attacks they investigate are password related. The vulnerabilities of password-based solutions stem from a combination of the following:

Humans aren't perfect and cannot be relied upon to maintain a process that is highly rules-based.

Other, more "job-related" processes compete for attention.

Certain insiders or outsiders are intentionally looking for ways to compromise the solution.

### *Humans are fallible and predictable*

Passwords only work if individuals use them correctly, all the time. Despite countless hours in creating guidelines, procedures and purchased safeguards, one user can still override all IT's efforts by simply sharing a password. Despite established guidelines, the human element often results in a number of common password problems.

Too many passwords to remember: The NTA Monitor Password Survey found that the typical intensive IT user now has 21 passwords, and

---

<sup>1</sup> RED HERRING, "The Global Security Gap", 11/5/03. [www.redherring.com](http://www.redherring.com)

---

<sup>2</sup> CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

has two strategies to cope, neither of which is advisable from a security standpoint: they either use common words as passwords or keep written records of them. The survey found that some of these heavy users maintain up to 70 passwords. Forty-nine percent write their passwords down or store them in a file on their PC or Blackberry. The research shows that 84 percent of users consider memorability as the most important attribute of a password, with 81 percent selecting a common word as a result.

Easy passwords: Users tend to set passwords based on words that they can remember easily, making them easy for hackers to guess. Simple password cracking programs can find many whole word passwords quickly.

One FBI computer consultant, who said he was frustrated by bureaucratic delays in obtaining legitimate access to certain bureau files, was able to hack into the files surreptitiously via the FBI Director's secret password, which the consultant figured out using software found on the Internet.<sup>3</sup>

Single passwords for many systems: To avoid remembering many passwords, people often use the same password across many systems – including insecure sites where passwords may be sent in clear text. A single password, once cracked, may open many doors.

Accessible passwords: Longer passwords containing different kinds of characters are harder to crack. They are also harder to remember, prompting many users to write them down often in accessible locations. Strong passwords also result in more Help Desk calls for forgotten or expired passwords, in addition to increased employee downtime. The less convenient security is, the more likely it is to be bypassed.

Accommodating or gullible people: Passwords are subject to social engineering attacks. Two-thirds of workers polled in downtown San Francisco turned over their passwords without flinching when asked. Their reward? \$3 coffee coupon. 70% of those who said “no way” to the request still gave up hints, like anniversary date, wife's name and pet name. 79% said they use the same password for multiple Web sites and applications.<sup>4</sup> In another study, four out of 5 workers would disclose their passwords to someone in the company if asked.<sup>5</sup>

<sup>3</sup> San Jose Mercury News, 8/28/06

<sup>4</sup> San Jose Mercury News, 5/6/05

<sup>5</sup> CNET News, 5/22/02

It's a frightening thought, but your information systems are only as secure as your least responsible user.

Figure 2. Using fingerprints solves a number of problems

Password issues	Solved?
Written down and easily accessible e.g. Post-it notes	✓
Easy to remember, easily guessed	✓
Single passwords for multiple systems and applications	✓
Stronger passwords increase password resets and support requirements	✓
Subject to social engineering attacks	✓

## The Cost to Organizations

### User Productivity and Support Costs

Arguably, most users try to securely manage their identity data (credentials) by creating secure passwords and hiding their passwords and/or tokens from others. Unfortunately these conscientious users will inevitably forget their password or token and generate a support call. As users are given access to more accounts, the number of passwords they must manage correspondingly rises.

Between 25-50% of calls into help desks are for password resets and each of those calls cost from \$20-38 per reset. In many cases, the actual cost of a password reset goes beyond the support call costs.

- Loss of employee productivity and effectiveness: When an employee is unable to log-in and contacts support, the employee experiences downtime and decreased productivity.
- Impacts mission critical operations: In financial institutions, records must be quickly accessible.

In California Commerce (Citicorp) Bank's call center, employees needed to quickly access multiple databases and accounts, all of which used different passwords which changed frequently. Switching between databases required signing out of one program to access the next. One forgotten password seriously impacted the banking workflow. Accessing and authenticating using fingerprint

systems, employees quickly and safely access information and improved service levels. By eliminating password dependencies, they also eliminated calls to the support desk for forgotten passwords.

## Government Compliance

Government regulations are creating additional pressure to provide better security for private information. Password management is fundamental to compliance:

- In October 2005, the FFIEC issued a guidance encouraging banks and other financial institutions to pursue two-factor authentication, including biometrics, for online transactions. <http://www.fdic.gov/news.financial/2005/fil10305.pdf>
- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to establish security standards that will protect the security and confidentiality of customer information from internal and external threats and unauthorized access via networks and online systems.
- The Sarbanes-Oxley (SOX) Act of 2002 requires higher security standards for financial or confidential data. According to this Act, any public company may be liable if it has not taken adequate steps to protect this type of data. Many existing password and security policies would not be considered sufficient under SOX.
- State Breach Notification Laws enacted in a number of states applies to companies that conduct business in the U.S. and maintain electronic data about state residents. If customer or employee data is breached whether by a lost notebook computer or by a hacker attack, breach notification laws of these states require the company to notify the user of the security breach whether that company resides in their state or not.

Laws such as these, coupled with stiff penalties for non-compliance, have forced organizations to take a closer look at their information security protocols.

## Alternative Authentication Solutions

Since standard password practices are not providing sufficient security for organizations, alternatives have surfaced. Organizations have explored everything from making password policies stricter to adopting tokens to using biometrics.

### Stricter Password Policies

Traditionally, user authentication means providing user IDs and passwords – a technique that has been in practice for decades. Although incremental improvements have been made to this process, such as not sending clear text passwords over networks and requiring "stronger" passwords, the fundamental approach has not changed. Its weaknesses are well known and are the primary methods by which network security is compromised.

The approach of requiring frequent changes and applying complexity requirements to passwords tends to backfire, since people can't remember the new passwords and are even more apt to write them down. Password security policies rely on end-user cooperation, and strict policies motivate users to compromise security. Those who comply will generate higher support costs due to forgotten passwords. It's a catch-22, with stricter policies actually lowering overall security.

Mountain America Credit Union required employees to lock down their workstation when they step away. Multiple passwords are required to unlock their computer and gain access. These passwords led to staff documenting passwords on Post-it® notes or sharing them among co-workers. With fingerprint sensors, the notes disappeared, password reset calls to the help desk disappeared and staff responded positively to the "cool" factor in using fingerprints for authentication.

### Single Sign-On

Single Sign-On (SSO) products simplify the management of password credentials by allowing a single password to provide access to all applications. Ideally, this would eliminate the management of all password credentials, except for one, and give the user free access to all applications with only one logon.

In reality, there are several drawbacks that limit the viability of SSO for many companies. Most SSO solutions require an administrator / programmer to

perform complex scripting for each application to be supported. This work is often multiplied over time as applications are updated and their logon screens change.

Furthermore, many security experts consider SSO less secure than using separate passwords. This is because SSO still relies on the users to create and maintain a secure password and only one password is required to access all of the users' accounts (sometimes called "Single Break-In"). In the end, the combination of high cost of ownership and continued reliance on an end-user to securely manage a password limit the viability to all but a few organizations.

### Password Self-Reset

Password self-reset solutions have recently gained a lot of attention in light of the growing password problem. These solutions reduce help desk calls for forgotten passwords by allowing users to reset their own passwords without calling for support.

Password self-reset products do not address the source of the security problem; end-users still must create and maintain (manage) a number of secure passwords.

Additional downsides of these solutions are:

- (1) they are not turnkey and often require immense professional services projects to support the integration effort required for each application, and
- (2) while they do significantly reduce help desk costs associated with forgotten passwords, end-user productivity is still impacted as they must perform the password reset.

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall... The weakest link in the chain is the people"

**Kevin Mitnick, Oct. 2002, BBC Interview  
Former Famous Hacker**

### Tokens & Smart Cards

Strong authentication solutions typically use a token/smart card in addition to a password to authenticate users. This is known as "two-factor" authentication. Increasing the number of required credentials (factors) is a broadly accepted method of improving security.

Token and smart card authentication solutions have been commonly used but limited to where the added security can justify the cost and burden. There is a large upfront and ongoing cost to deploying and managing tokens or smart cards: these solutions typically require setting up and maintaining a private key infrastructure. Users often forget them or leave them at their desk. Traditional strong authentication solutions also do not support all applications and do not tightly integrate into the native network directory and management infrastructure. These issues have limited the deployment of token and smart card authentication products only to users who require secure remote access.

### Fingerprint Authentication

Fingerprint authentication solves many of the security issues addressed in this paper. In particular, fingerprints are less susceptible to human error.

Fingerprints cannot be "guessed" or shared.

A user doesn't have to think up a "strong" fingerprint, so the security of the metric doesn't depend on user effort.

People can't "forget" their fingerprints – eliminating a common source of Help Desk calls.

Because biometric technologies use a physical characteristic instead of something to be remembered or carried around, they are convenient for users and less susceptible to misuse than other authentication measures.

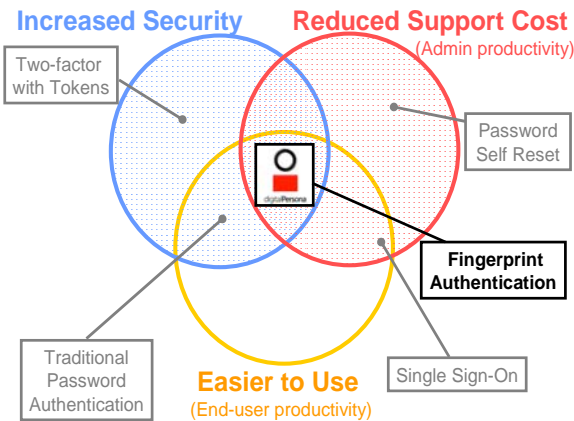
Banco Azteca of Mexico serves many with limited incomes in poor and rural communities. With many folks not having a secure form of identification, Banco Azteca found it difficult to ensure the security of the accounts. Additionally, many of their customers were farmers and construction workers whose fingers were damaged and worn. Their finger-scanning system needed to be sophisticated enough to image and authenticate these difficult fingerprints. Today, over 8 million of their customers are using fingerprints as a form of identification in over 1,140 branch offices. Banco Azteca averages over 200,000 users accessing the DigitalPersona system daily and maintains a high success match on the first try.

### Alternatives Reviewed

Figure 3 reviews various options pursued by organizations to reduce the vulnerabilities of their

systems. Many of the tools discussed in this whitepaper such as single sign-on, tokens and password resets fall short of achieving their desired goal: increasing security without radically increasing inconvenience and costs.

Figure 3: Using fingerprints has all three advantages



Regardless of how secure a new technology promises to be, if it's hard to use or inconvenient for end-users, it won't be accepted. Financial institutions face a tough challenge, trying to address increasing security threats without hampering productivity and while keeping IT costs down.

In an attempt to improve network security, one government entity initiated a more complex password program. When users began to push back, they resolved the issue by installing fingerprint readers for user convenience and simultaneously tightening security.

Fingerprint authentication sits squarely in the middle of the three circles in Figure 3. As discussed in this paper, fingerprint authentication eliminates the reliance on users to manage their authentication credentials (passwords, tokens, etc). The touch of a uniquely identifiable finger is applied to make each system more secure. Because it's hard to forget a finger, fingerprint authentication solutions are much easier to use than most security options on the market today.

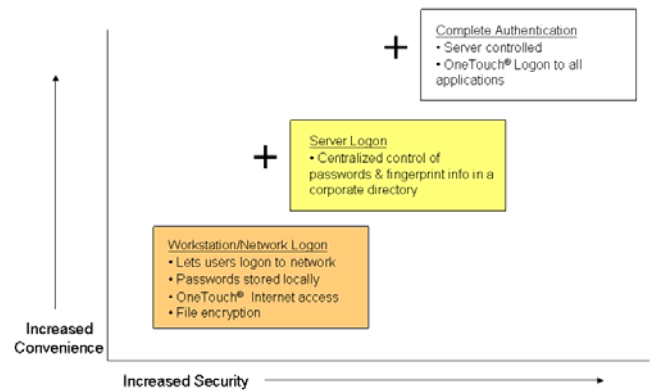
## Complete Fingerprint Authentication

Figure 4 conveys how different fingerprint authentication configurations can produce varying levels of convenience and security benefits:

**Workstation/Network Logon:** Fingerprint authentication solutions installed locally on desktops improve security and convenience. With Microsoft® Active Directory® integration, users

simply touch their finger to the reader and they can be quickly authenticated and logged onto the network. There's no need to remember or type in user account and password information. Digital Persona's solutions do not store fingerprint images, data collected from the user's finger are encrypted and stored locally.

Figure 4: Fingerprint Configurations



Within the DigitalPersona® Pro authentication solution, users can take further advantage of fingerprint technology by using OneTouch® SignOn to teach the fingerprint reader to know the logon information of any of their Internet applications. Users can apply their finger and logon quickly and easily anywhere on the Web.

**Server Logon:** Consider the next step of storing and matching fingerprint templates on a centralized server. This step enables organizations to have even greater control over network logon by moving the authentication process to a secure administrator-controlled environment. It's also possible to take advantage of administrative tools that come along with corporate directories.

**Complete Authentication:** The recommended approach is all of the above plus providing OneTouch SignOn access to any application. This is accomplished without any custom integration, as it uses the existing password infrastructure. A user submits their finger to the reader and they are logged into all applications, thereby taking all password management out of the hands of end-users.

Organizations are more secure with a complete fingerprint authentication solution for these reasons:

- Fingerprints (biometrics) are unique to the user; therefore audit trails can be traced back to the user, not to the system or application. This

makes for a more secure system when fraud or losses are critical.

- End-users no longer need to be involved in password management. Passwords are automatically applied when they touch their finger to a reader.
- Security risks due to compromising end-user password practices (e.g. writing them down, sharing them, etc.) are eliminated.
- Audit trails and other tracking tools provide further information on access to applications.

### **Top 5 Advantages of Fingerprint Authentication**

- **Secure Authentication**  
Identity is based on who you are (fingerprint) versus what you know (password)
- **Ease of Use**  
Quick access to data
- **FFEIC & Data Breach Compliance**  
Restricts access, protects data and provides audit trail minimizing misuse
- **Speed**  
Users get fast secure access to data
- **Quick Return On Investment**  
Reduces help desk costs and increases productivity

The United Banker's Bank (UBB) was concerned that passwords were too weak an authentication method for protecting confidential online data and in particular, allowing their community banks to initiate transactions including the wiring of money through their correspondent accounts. They were also experiencing a high volume of support calls when passwords were expired or forgotten. After researching smart cards and tokens, UBB chose fingerprint authentication because of its superior reliability. They found it provided a maximum level of protection, was easy to use, and was cost efficient.

Fingerprint Authentication and Microsoft Active Directory

Fingerprint authentication can be integrated with Microsoft Active Directory (AD), as in the case of Digital Persona's solution, to take advantage of AD

administrative and security tools to fully integrate with an organization's identity management program.

### **Enhance system security with multiple factors**

Additionally, it's worth considering other measures to reduce risk for high security environments and users. The easiest is to enhance fingerprint authentication with additional security layers (a practice called "multi-factor").

1. Add multiple fingerprints to an authentication scheme. This is essentially a no-cost solution, although it requires users to use the reader twice for each authentication.
2. Add a password or PIN to the fingerprint solution for high security applications. Again, this makes it significantly more difficult for an intruder to gain access.

These additional factors can be used to protect specific applications or data, or even classes of users. For example, accounts with administrative privileges could require both a fingerprint and a password. These individuals are likely to be better about password usage than the general population and the combination of a password and fingerprint raises the bar.

### **A Look at ROI**

Over the last five years, the costs and viability of fingerprint technology have developed to a state where entities can, and are, taking a serious look at the technology for password replacement and enhanced security.

Fingerprint authentication solutions can literally pay for themselves in help desk savings alone. The typical enterprise spends an average of \$150 per user per year to support password resets, according to Andreas Faruke, head of Deloitte & Touche's Identity Management Services in Canada.

**"The strongest return on our DigitalPersona Pro investment came through a reduction in demand on our help desk, where password-related help desk calls have dropped by 90 percent,"**

***Patrick Honny,***

Department Information Services Manager  
County of San Bernardino

There are added cost savings in user productivity which are less easy to measure. However, if a user on the road can't access the network because they've forgotten a password, then they've lost productivity for that entire period. Embezzlement, fraud or other losses due to unauthorized access can be even further costly to a business.

Considering that fingerprint authentication is more convenient, easier to use and more secure, the decision to go with fingerprint recognition technology is an easy one for many organizations.

## Summary

Passwords are even less secure today, despite more stringent requirements such as 90 day expirations and strings that must be a certain length. Passwords should be managed automatically, where users aren't required to remember or keep track of them.

Fingerprint authentication creates a more secure environment by requiring users to prove who they are in the most natural way. An individual's fingerprint is mapped to their credentials on a server where identities can be tracked and mapped to their provisioned applications. The whole fingerprint authentication process is more convenient, more reliable, and thus less costly overall. Best of all, fingerprint authentication solutions are much more secure.

## About DigitalPersona

DigitalPersona is the leading provider of biometric authentication solutions for enterprise networks and commercial applications. Founded in 1996, DigitalPersona, Inc. designs, manufactures and sells solutions that improve security and regulatory compliance while resolving password management problems. The company's fingerprint readers utilize superior optical fingerprint scanning technology, providing an unmatched ability to authenticate users more accurately and rapidly regardless of finger placement. DigitalPersona's award-winning technology is used worldwide by over 25 million people in the most diverse and challenging environments.

DigitalPersona has strategic relationships with market-leading manufacturers and resellers including Dell Inc., Microsoft, GTSI Corp. and Hewlett-Packard. DigitalPersona® Pro, the company's flagship turnkey security solution for enterprise authentication, is used by leading financial institutions such as NASDAQ, Lending

Tools, United Banker's Bank (UBB), Royal Bank of Scotland, Mountain America Credit Union, San Antonio Credit Union, Mortgage Information Services (AdvizeX), Allegiance Credit Union, South Carolina Bank and Trust, Honda Federal Credit Union, Telesis Credit Union, La Caixa De Pensions De Barcelona, Banco Azteca, and California Commerce Bank.

Additional information is available by contacting Digital Persona, Inc. at +1 650.474.4000 or at [www.digitalpersona.com](http://www.digitalpersona.com).

© 2006 Digital Persona Inc. All rights reserved. DigitalPersona and One Touch are the trademarks of Digital Persona, Inc., registered in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.