



Market Primer

TWO-FACTOR AUTHENTICATION FOR INTERNET TRANSACTIONS

NEW SOLUTIONS FOR 21ST CENTURY
BUSINESS ENVIRONMENTS

© 2004 CardLogix Corporation. All rights reserved.

This document contains information that represents the present view of CardLogix Corporation and the issues discussed at the time of publication. Because CardLogix must respond to changing market conditions, it should not be interpreted as a commitment on the part of CardLogix, and CardLogix cannot guarantee the accuracy of any information presented after the date of publication. Document # 7 200 002

This White Paper is for informational purposes only. CARDLOGIX MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Winplex™ is a registered trademark of CardLogix Corporation in the United States and/or other countries.

Other product or company names mentioned herein may be the trademarks of their respective owners.

CardLogix Corp. 16 Hughes, Irvine, CA 92618, USA.

Table of Contents

SUMMARY.....	2
OVERVIEW.....	2
FORGET WHAT'S IN YOUR WALLET -- WHERE DOES YOUR FINANCIAL DATA TRAVEL?.....	3
THE PROBLEM WITH PASSWORDS.....	3
EXPOSURE OF PRIVATE DATA	4
WHAT'S BEEN DONE TO DATE?.....	5
WHAT'S REALLY NEEDED?.....	5
COMPARING THE OPTIONS.....	6
HOW A SOLUTION EVOLVED.....	6
CONCLUSION.....	7
RESOURCES.....	8

SUMMARY

This paper examines the approaches taken to date by the financial industry to authenticate account holders and build customer trust, especially in on-line transactions. We'll examine a new type of solution that builds upon existing technology for advanced authentication. This new approach bridges the gap between people's demand for independence and convenience in their finances, and the current, glaring lack of safety in filling that demand.

OVERVIEW

For most people, personal banking has always been the original, most fundamental financial activity. Regardless of their wealth or activity level, people count on keeping close tabs on their money. For decades, all banking was strictly face-to-face, with immediate teller confirmation of deposits, withdrawals, and payments. Both teller and customer were reassured that any transaction was secure and private. This one-on-one relationship changed as banking consumers demanded higher levels of convenience. Change started with drive-through tellers and led to ATM machines and plastic cards, which in turn evolved into on-line banking. These convenience-driven technologies have moved the customer from personal consultation to independent decision-making, aided greatly by the Internet. All this advancement comes at a price, however. As technology opens up consumer choice, it exposes greater risk as well.

The combination of regulatory changes in the financial services industry and Internet-aided independence for consumers has increased competition for selling products and services that used to be the sole dominion of a bank. These products include savings, credit cards, mortgage loans and investment accounts.

Today, many consumers park their money with a variety of companies that they trust and believe will give them the value they seek. These financial relationships include multiple passwords for every company that the customer needs web access to. With the growing number of financial service companies and other web merchants, a significant amount of fraud, deception and identity theft has developed. Much of this is the result of a lack of effective and secure authentication by these organizations. The increase is so noteworthy that many states are enacting regulations for institutions to publicly report these incidents.

These problems are contributing to a loss of consumer trust in financial institutions. Costs can multiply as banks and credit unions scramble to prevent and recover from attacks, then re-build customer trust. Lack of trust also results in customer reluctance to further engage with on-line services and products.

Authentication is the process of inspecting, and then confirming, the proper identity of parties involved in the transaction of data or money. In the old face-to-face days, this was easily done and verified by a customer pulling out a driver's license when making a withdrawal. This was the original form of Two-Factor Authentication: The customer presenting account data (something you know) along with an ID (something you have). In the digital age, authentication is much more complex

Forget What's In Your Wallet -- Where Does Your Financial Data Travel?

Most consumers don't realize that their financial data gets around more than they do. This has always been true when an ATM/Debit card is inserted into a machine for account access or transaction. However, threats in this world are primarily physical. Safety at the ATM has been problematic. In addition to a physical robbery, more sophisticated methods are used to facilitate card cloning and account attacks. Brute force has been replaced with sophisticated technical expertise. These methods combine card sniffing at the POS terminal or ATM with over-the-shoulder peeks or video recording of PINs as they are entered. All the data needed to recreate a card has been divulged and this new breed of criminal is spending the consumer's money in a matter of minutes.

On-line, the snooping threat begins within the customer's PC and is present throughout the many servers that the data must pass through on the way to the bank and back again. Most of these attacks are from malicious code that includes viruses, worms, spyware and Trojan Horses.




This dilemma is rapidly getting worse. Although a financial institution can secure itself and its networks, it cannot force customers to protect their PCs, networks, cards or personal practices.

THE PROBLEM WITH PASSWORDS

The primary method to access an online account is entry of a user name and password. This weak link has been exposing customers to potential problems and exposing banks to unneeded financial risk.

Passwords and PINs are a type of Single Factor Authentication. Unlike the old-fashioned process, only one factor is used to authenticate a user and transaction. The consumer typically chooses a word or set of numbers that can be remembered easily and probably is used for multiple accesses i.e. the voice mail on their cell phone or home answering machine. This is contrary to a strong and secure password implementation. The average working person today manages at least five passwords across their business and personal life. These are often forgotten, lost or compromised. When used for multiple accounts, the password becomes vulnerable to detection and fraudulent use with the compromise of just one site that is accessed.

THE FOLLOWING CHART ILLUSTRATES THE MAJOR PROBLEM WITH PASSWORDS

Passphrase Guessing (Dictionary Attacks)			<i>Using easy-to-remember English words results in approximately 1.3 bits of entropy per character, (word space) vs. purley random characters (total space)</i>						
Strong	OK	Weak	example	# of characters	complexity	word space	total space	est.time to break total space	
			"dogie"	5	25 (lowercase)	12 bits	23.5 bits	40 minutes	
			"br1a9Ax"	7	62 (alphanumeric)	24 bits	41.7 bits	2 days	
			",".THX1LB.	10	95 (full Keyboard)	40 bits	65.7 bits	Infeasible (3.8 x 108 yrs)	

EXPOSURE OF PRIVATE DATA

In addition to the ease of obtaining a customer's password, a very nasty type of attack has emerged called *phishing*. This phonetically-named type of attack comes as a Spam email masquerading as an official bank's email message. The message asks the user to reset or confirm their password on a form that looks identical to the bank's website. This malicious website will be up for a day or so to collect thousands of passwords and then the attacks begin on the harvested accounts.

With the typical level of ATM/Debit card and web security, there are three main problems with password -based account logon. The first is that it exposes the user's identity and password together. This data can be intercepted and read anywhere along the path from the user's keyboard to the institution's secure server. The second is the authentication method used with passwords is static and never changes, thereby enabling replays of these passwords for unauthorized access. Thirdly, a user name and password does not securely authenticate that the real account holder and their card are present and valid.

On-line fraud and theft have reached epidemic levels worldwide. Last year alone, the Federal Trade Commission received over 516,000 reports of identity theft, The FTC estimates that over 27 million people in the U.S. have been victims over the past five years. According to Gartner, Inc. 1 in every 50 consumers has suffered identity theft.

In early 2004 financial institutions including Wells Fargo, Bank of China, and UBS all experienced public (phishing) attacks that exploited weakness in password-protected access.

Around 40 million people now use the internet to update checking and savings accounts and transfer funds. Market researcher Gartner Inc. says that number will rise at 14% per year. At the same time online fraud is picking up. Financial Insights a unit of market tracker International Data Corporation... Says electronic identity theft cost banks and mutual fund companies \$4 billion last year. By the end of 2006 that's likely to double.¹

According to RSA Security: *Security is the Key to Internet Confidence*. A Forester Research survey showed that 80% of their respondents used the Internet to send E-mail 56% Use the Internet to research products. Yet only 21% use it to conduct some kind of financial transaction.²

These transactions include all web shopping and brokerage houses such as E-trade and Charles Schwab. Most likely, e-banking constitutes a much smaller percentage. These numbers indicate that a lack of consumer trust in on-line systems is what's holding back mass adoption.

WHAT'S BEEN DONE TO DATE?

Banks have been experimenting with different solutions for many years including biometric identifiers at the ATM and fingerprinting at the bank. Most customers found these methods intrusive and the programs were dropped. To secure the burgeoning volume of Internet transactions, Secure Socket Layer (SSL) evolved into the standard protocol for web security and encompasses multiple cryptographic layers designed to encrypt and protect user and account information activated at log-in. Despite this and other safeguards, at any junction along its path, including the user's PC, the data, complete with passwords can be spied on and replayed fraudulently.

In the late 90's a consortium of banks formed the Indentrus organization to create a sophisticated smart card solution for business and consumer banking built on PKI architecture. This group acknowledged that the best technology for Two-Factor Authentication was smart cards. However, this methodology required a very expensive type of smart card because much of the encryption processing is done on the card. On top of the high card costs, the additional IT management components have proven too costly to be used in a widely deployed consumer solution.

Many financial institution's mission statement, bylaws or charter demand that the management take all possible steps to maintain trust with their customer. Public outcry over privacy rages on with individual states enacting legislation that exposes these breaches of security publicly, i.e. California's bill SB1386.

The critical intersection of increased web traffic, ever more sophisticated hacks and industry reluctance to reveal and remedy security weaknesses has set the stage for a potential disaster for banks, credit unions and their customers.

Today the opportunity is ripe for institutions to alleviate the customer's lack of trust and aggravations that come from multiple financial service relationships. This can be accomplished by offering the customer tangible evidence of increased security with the ease of a single logon process, minus the hassles of passwords.

WHAT'S REALLY NEEDED?

Three objectives must be met before on-line log-on is really secure. These are:

1). **Protection of Log-on Data:** Instead of entering and sending the data along with SSL bodyguards, it's better not to send it all

2). **Reliable Authentication:** That links all critical identity elements together for real security

3). **Card- Present Transactions:** Fortifying an absolute link between the authorized card and authorized cardholder

COMPARING THE OPTIONS

Technologies	Drawbacks	Advantages	Relative Cost per user	Relative Security
Passwords	Weak Single factor, static clone-able	Low entry Cost	\$ 14*	Very low Security
Bio-metric Server Centric	High false positives or rejection rates Liability for biometric storage	No lost passwords or cards	\$ 55	High Security
Smart Card Symmetric Key Style (ATMobility)	Data storage is limited	2 factor Authentication Read-Write Capability, Durability	\$ 14	High Security
Smart Card Asymmetric Public Key Style	High yearly cost due to cert authority, Requires client side software installation and extensive server side modifications	Read-Write & Computing Capability, Durability, Security, Storage	\$ 45	Ultra-High Security
Key-Chain Fob	Only works with USB enabled customers, Not extensible to mobile banking, Requires client side software installation	Durability	\$ 18	High Security
R.F.I.D. - ISO1443	High Cost of cards, readers and terminals, Requires client side software installation. Difficult to emboss cards	Read-Write Capability, Durability	\$ 45	Low Security

* Based upon the average yearly cost of resetting passwords through a third party

HOW A SOLUTION EVOLVED

In Europe, Latin America, and Asia financial fraud has accelerated well beyond U.S. levels. Factors contributing to this include insecure telecommunications systems, plus many and disparate countries and currencies.

ABN AMRO Bank of the Netherlands devised a solution that has been in place for a few years and has produced good results. This Bank, now the fourth largest in Europe, found that combining smart cards with SSL for online access met their needs for increased security. The bank witnessed an astonishing revenue growth in their other services after the deployment of a two factor smart-card implementation.

Since smart cards are commonplace in most of the world, they are becoming a pivotal element for enhancing ATM card security in physical and on-line applications. Smart cards achieve Two-Factor Authentication by presenting something you know (your PIN) and something you have (your smart chip enabled ATM Card). Additionally, smart card security prevents everyone other than the card issuer from discovering and using the secret key.

Based upon this model, but with improved encryption, and lowered costs ATMobility™ was developed by CardLogix, a leading smart card manufacturer and platform provider.

The ATMobility platform has a full-featured smart ATM card, plus a low-cost unconnected smart card terminal. These items combine with server-side software and provide a superior authentication method over passwords. This platform increases trust, lowers costs and can stimulate sales of additional services. It also guarantees that the transaction is 'card-present', further solidifying the transaction's security.

With ATMobility, only the numbers representing private data travel the web. Every log-on generates its own one-time session password. If it is intercepted, it cannot be replayed to access accounts or fraudulently transact data or dollars.

Unlike passwords customers rarely lose or forget their PIN. There is a measurably lower cost of maintaining customer relationships when the institution can remove the password help desk / call center.

CONCLUSION

Trust has always been the cornerstone of financial transactions. Despite legislative and technology-based advancements to ensure trust, a practical, cost-effective solution has been beyond the reach of banks and credit unions. Today, true Two-Factor Authentication restores the level of trust in a transaction that customers have known for centuries. Smart cards, a proven transaction technology used worldwide, fill an immediate and growing need to deliver the next level of security.

RESOURCES

1. Banking On a Secure Transaction

- Yahoo News by Murray Coleman 01/12/04

2. Security is the Key to Internet Confidence

- Vantage Magazine, Spring 2004 by Arthur Coviello Jr.

ID Theft: How to Prevent It and How to Get Over It

- CUNA, [CUNA: The Credit Union National Association](#) 09/03

The Retailers Home Run

- Card Management Magazine, by Robert Bennet 07//03

Major Debit Card Scam Uncovered in Canada

- SC Infosecurity News, 02/04 [www.infosecnews.com](#)

[www.Epaynews.com](#)

- Statistics , ongoing updates

E-Banking What Next

- Retail Banking, By Bill Orr 12/03

Smart Cards and the Retain Payment Infrastructure: Status, Drivers, and Directions

- The Smart Card Alliance, 10/02 [Smart Card Alliance](#)

Smart Card Basics

- CardLogix, [www.smartcardbasics.org](#)

[www.smart-ecard.com](#)

Document # 7 200 002