

Consumer Managed Access to Financial Accounts and Sensitive Websites

A New Approach to an Increasingly Serious Challenge

By S. D. Skip Booren

Debit Card Dangers

"In November, thieves made more than \$100,000 in unauthorized cash withdrawals from ATMs at casinos in Las Vegas using stolen debit-card numbers and PINs. The U.S. Secret Service determined the cards had been compromised at two service stations in Costa Mesa, Calif. Police suspect that the skimming devices were planted in PIN pads at the pumps at night while the stations were closed.

In October, eight people were arrested in Los Angeles in connection with a scheme to skim more than \$1 million from **Wells Fargo & Co.** and **Washington Mutual Inc.** cardholders. Skimmers used at several restaurants ...were found to be the source of the breach."

Wall Street Journal, 3/08/07

Is Your Data Safe?

"Given all the unknowns, it's not surprising that even the experts are sometimes in the dark. A December 2006 survey of more than 200 North American security professionals by Enterprise Strategy Group Inc. showed that more than one-third had experienced a data breach at their company in the past 12 months, and another 10% didn't know if they had lost data."

"The old mind-set was that data breaches were the result of nefarious outside hackers, while the latest industry rhetoric blames insider attacks," according to Enterprise Strategy Group analyst Jon Oltsik in his June 2007 report, "The Case for Data Leakage Prevention Solutions."

"Your data's less safe today than two years ago"
ComputerWorld 08/20/07

Historical Overview

The coming of a connected digital age has meant benefits in terms of enjoyment, convenience, productivity and efficiencies that would have been unbelievable even just a few short years ago. More and more people are banking online, paying bills online, and making purchases online. At the same time increased broadband usage is leaving increasing numbers of home computers continuously connected to the Internet.

Simultaneously the security requirements to continue to enjoy those benefits are growing exponentially in order to continue to thwart an ever more sophisticated threat to sensitive personal information. ID theft in its many and varied forms is increasingly a problem that affects more and more people each day.

The following chart highlights just a few of the pertinent statistics coming from the most recent Symantec Internet Threat Report:

- **Home users** were the most highly targeted sector, accounting for **95%** of all targeted attacks
- **85%** of credit and debit cards advertised for sale on underground economy servers were issued by banks in the United States
- **Threats to confidential information** made up **65%** of the top 50 malicious code reported to Symantec
- **Keystroke logging threats** made up **88%** of confidential information threats by volume of reports
- Organizations in the **financial services sector** accounted for **72%** of the unique brands that were phished during this period.

September 2007 Symantec Internet Security Threat Report

Spoofing, phishing attacks, pharming, and Trojans that download keystroke-logging software are just a few of the ways the home computer user is under attack. Major data breaches at large merchants like the one reported by TJ MAXX, wherein millions of files containing debit card/PIN information further highlight the threat.

Then there are the petty and sometimes not so petty thieves who skim debit card information in restaurants and from gasoline pumps. Breaches of sensitive information like the recent one at Monster.com that exposed over 1.3 million accounts further add to the consumer's dilemma. Everyday, individual consumers find themselves targeted by increasingly sophisticated and seemingly personal email designed to solicit their confidential information.

Increasingly this kind of news makes the daily headlines. It is no longer just the grist of trade and banking journals. It now affects millions of people and costs consumers billions of dollars annually.

The Consumer's Dilemma

Do you sleep well?

A farmer hired a young man who said that his only qualification was that he could sleep well at night. Somewhat puzzled, the farmer took him on and gave him a list of chores and tasks to complete. The task included securing the barns, sheds, and corrals at the end of each day.

One night a terrible storm arose. Without luck the farmer tried to wake his new hand to check on the farm, it's out buildings, and corrals. Failing to arouse the young man, the farmer went out himself and found all well and secure.

Everything was as he had directed. Now he understood the young man's unusual qualification of being able to sleep well at night.



When a consumer's checking account is breached due to debit card fraud, more often than not they eventually have their funds returned to them, depending on how quickly they detect and report the theft. This can sometimes take several days or weeks, and entail lots of frustration and aggravation, to include bounced checks and many, many phone calls. In other words, it is not fun, no not a bit.

When major merchant accounts (like that of TJ MAXX) are breached, it can result in arbitrarily closed checking accounts, cancelled debit cards and additional aggravation, again all for the individual consumer.

Symantec's September 2007 Internet Threat Report suggests that the situation is only going to get worse as organized crime realizes the financial gain to be obtained through the theft of personal information.

While criminals have been busy, so have security managers and experts in the financial industry. Solutions adapted have included increasingly complex log-on procedures which require the user to remember more and more information that they select or provide on initial log-on. At the same time, some banks and credit unions have acquired sophisticated heuristic software that analyzes the use patterns and purchases of consumers.

These expensive tools provide at best a false sense of security - many of the "most" sophisticated log-on protocols have already been hacked.

Worse is the consumer's experience as they try remembering answers to multiple personal questions, where the answers are "case sensitive." There is also the challenge of remembering a specific image in a field of many. Then there is the time they wait and wait to check in at their hotel and can't get through to their bank's customer service. They made the mistake of taking a whimsical trip without telling their financial institution. Now their debit card won't work because the heuristic software says they shouldn't be in that city.

As noted above, all of these solutions are instituted by the financial institution, whether it is new technology or closing accounts in the event of a major data breach. Little control is given to the individual consumer, other than to monitor his/her accounts for unusual activity. Even then, if they are defrauded, more than likely they will not know until well after the fact, even if they have e-mail alerts and check their accounts daily.

This has to be a frustrating situation for the security managers and executive teams in banks, credit unions, and other financial institutions like investment brokers that offer checking with money market accounts.

As described below, RBA International has developed a possible solution to this vexing problem. As of October 2007, this solution has been operational for close to 4 years, supporting debit card accounts for thousands of cards issued under license by VISA USA, Inc through a premier NW bank.

A Uniquely Convenient Solution

As a result of a unique intersection of experience, timing and emerging technology, RBA International has developed a combination of simple procedures and technology to answer many of the concerns outlined above.

This patented solution entails employing advanced telephony technology to lock and unlock authorization for purchases using debit/credit cards and to allow or deny access to website accounts. Elegantly simple in its approach, it is nonetheless robust in application because of the independent channel of the locking mechanism.

Development of this solution came as a result of

1. Blending extensive business-rules based object oriented software development in the on-line banking industry with
2. Many years of experience with pre-paid phone cards in the cellular phone industry, and
3. Experience building a deployed global IT security model for a major credit card consortium.

Benefits offered to the consumer are as follows:

1. **Convenient and dynamic control of access to debit/credit card accounts.** This allows the account holder to use their cell-phone with "speed dial" to "toggle" ON/OFF authorization for purchases. This is done through calls to a menu driven Interactive Voice Response (IVR) System.

Human interaction in the form of a customer service representative is not required, although available. Using the speed-dial on a cell phone, the "toggling" process normally takes less than 10 seconds.
2. **Protection against fraudulent purchases.** When an account is "toggled" OFF, the system will not authorize ANY purchases – Point-of-Sale, Internet (Card not present), ATM withdrawals, etc.
3. **Website Security.** Again, employing the same IVR system, consumers are given the option of "toggling" access to bank websites used to manage their debit/credit cards, thus providing protection against keystroke logging malware, phishing, and spoofing schemes.
4. **Real-Time Notification.** Many banks offer e-mail notification of payment due and even purchases made when using a credit card. This system provides similar alerts, but with a twist. This system also **offers real-time SMS text message alerts not only of transactions completed, but also transactions attempted when the account is disabled.** Additionally, these alerts include current available balance for debit card accounts.
5. **Real-Time Account-to-Account Funds Transfers.** One side feature of this system is that account holders can transfer funds instantly from one account holder to another, using the telephone number of the receiving party to identify the receiving account.

Debit Card Dangers?

"Users frequently assume that debit and credit cards are the same, but they are regulated by different laws. A credit-card transaction is similar to a loan. When a credit card is lost or stolen, holders are responsible for only \$50 of any fraudulent use, a charge that is often waived.

With a debit card, the liability varies. The loss could be limited to \$50 if a cardholder notifies the financial institution within two business days after learning of the loss or the theft of the card or PIN number. Beyond the 48 hours, the cardholder could lose as much as \$500. The loss could be even higher if the cardholder doesn't report it within 60 days after receiving a financial statement listing the fraudulent transactions."

"Growing Debit-Card Use Sparks Warnings"

Wall Street Journal 7/2/07

How this Solution Works

Secure Card Account

1. Upon Enrollment, the account-holder, either on-line or by using a hard-copy application, provides among other information their home and cell phone numbers.
2. Upon receipt of their card, they are advised to use one of those phones to activate the card, much like any other debit/credit card. At that time, they are connected to RBANet via the IVR.

RBANet is an Application Program Interface (API) used to integrate the IVR with issuing financial institutions' and third party card processing systems.

3. When activating their card account, the account holder is also asked to create a 4-digit PIN for use in IVR transactions.
4. The account holder then has the option of enabling/disabling the account instantly with their cell-phone.
5. Assuming the account is disabled and the account holder desires to authorize a purchase, they can do so in seconds using the speed-dial feature of their cell-phone to dial the toll-free IVR and then digitally entering their PIN, and the code for enabling the account.
6. When the card is swiped or used for an on-line purchase, the ON/OFF status is checked by RBANet and the transaction is authorized or denied.
7. With authorization of the purchase, RBANet will (optionally) send an SMS text message to the account holder's cell-phone indicating the amount of the purchase and remaining balance. This information is also indicated in real-time on the account web site. The account holder may also receive e-mail notification of the purchase.
8. The system is designed for convenience in that consumers can choose to activate a card for a one time use, wherein the card is automatically deactivated as soon as it is swiped. Alternatively, if the consumer knows that they will be out of cell-phone coverage at the time of anticipated use or that they will be making multiple purchases in a short period of time, the card can be activated to remain on until deactivated.
9. Designed for flexibility, security, and real-time transactions; this system currently supports **VISA**[®] debit, ATM, payroll, gift, and instant issue. The configurable nature of the system ideally lends itself to customized solutions.

Subordinate Accounts

1. Account holders have the ability to create “subordinate accounts” for minors, employees or other individuals wherein it is important for the account holder to
 - a. Maintain overriding control over the funds in the subordinate account by establishing system rules for purchases in terms of limits, spending locations, etc.
 - b. Monitor spending and/or purchases for that sub-account on a real-time basis
 - c. Transfer funds instantly into and out of that sub-account
 - d. Independently lock access to the sub-account via Primary account holder’s website.
2. Subordinate Accounts are established after the Primary Account is activated and offer the subordinate account card holder the same security features (account toggling, alerts, etc) offered the primary account holder.
3. A customizable menu of available controls allows for simplified management of card limits and usage.

Reports Generation

1. With a full set of reporting capabilities in PDF, text and comma delimited format, this system provides a full accounting of system balance on a daily basis, to include revenue sharing and cardholder transactional activity.
2. The system supports accounting and reporting for multi-layers of payout schedules including visibility to agent, retail, and program performance.
3. Accounting of international payments for merchants and payees through web based transactions is also feasible.

Secure Website

1. The "Secure Website" offered by RBA International can be made available to consumers as either a stand-alone service or in conjunction with the Secure Card Account.
2. In either situation, enrollment in the Secure Website is similar to enrollment for the Secure Card Account.
3. The addition of a PIN, specific system status codes, and voice response messages, further add to the security of the system and provide greater flexibility in managing the security of the website.
4. Maximum protection from spoofing occurs when the User:
 - a. First attempts log-in using User ID and Password, prior to unlocking the site using the telephonic interface.
 - b. Confirmation that the correct site has been accessed comes with the message: "Your online banking website is locked. Please unlock your site and try again."
 - c. The user then dials the IVR, provides PIN and code to unlock access to the Secure Website.
5. Acknowledgement of the change in status is provided by either an audio message via the IVR or optionally via e-mail/or SMS text message to the caller's cell-phone.
6. When "toggled" the Secure Website relocks after each session is completed.
7. The Secure Website Authorization System in conjunction with the supporting IVR and RBANet can also be set up to authorize or deny specific transactions within a Secure Website in accordance with previously established business rules. Examples of specific transactions include: setting up payees for automatic bill-payment, transfers of funds from one account to another, changes in credit limits, access to specific accounts within the Secure Website, etc.
8. Specific transaction management can be setup with the Secure Website or in lieu of control over access to a particular website.

When it comes to Website Security, which do you prefer?

This?



This?



Or this?



Who is RBA International?

RBA International provides financial and banking products, processing services, and secured hosting on a global basis. RBA provides a debit card processing platform for license to member banks. All cardholder support, order fulfillment, regulatory compliance review, settlement reporting, and security are included. In the course of developing these products and services, RBA has developed proprietary tools and methodologies for assessing, analyzing, and evaluating existing processes and procedures in use at client banks and financial institutions.

Founded in 1994, RBA has serviced over 80 clients, including Fortune 500 companies. RBA's staff has won awards for technology innovations and successfully managed multi-million dollar projects. RBA uses advanced technologies designed for scalability, security, performance, and integration with legacy systems. RBA has applied for and received patents on banking technologies and methods, as well as for phone based Mobile Banking and security applications. RBA was runner-up for the "Oscards 2006" Technology award for its Mobile Banking security innovations.

RBA's co-founders' experience goes back many years before that seminal date in 1994. They cut their engineering teeth in the world of the "old" Hewlett Packard, when Bill and Dave still roamed the labs and passageways of HP. This was a time when solid engineering was deemed of greater value than marketing, and when technology was built to last.

Even at HP they were visionary. They automated and turned the lights out in the data center at a printer manufacturing facility in Vancouver WA. In doing so, they thereby increased its uptime by eliminating as much as possible human interactions. This allowed the plant to engage in a new manufacturing philosophy then known as "Just in Time Manufacturing." Their efforts received a great deal of notoriety and acclaim throughout HP.

Early on in its existence, RBA's technicians were involved with cellular phone technology supporting development work for the billing system for McCaw Cellular, which later became AT&T Wireless. RBA developed the technology behind one of the first US pre-paid phone cards for Bottomline Telecommunications which was bought by MCI Worldcom. RBA developed technology for the billing system for NTT DoCoMo Japan's pre-paid cell phones.

As on-line banking came to the fore RBA's professionals developed the On-line Express Banking for US Bank and on-line payment systems supporting Washington's King County licensing services.

In 2003, RBA conducted a Global IT Security Operations analysis for **VISA International**. Out of that analysis came an operational model for Global IT security that was adapted by the **VISA** Executive Management team.

RBA is a certified processor for **Star**, **VISA**, and its member banks, as well a bank merchant. RBA uses First Data's EFS Net, VeriSign's Secure Commerce Technology, Global Server Certificates, and Verified by **VISA**. RBA's technology complies with **VISA**'s CISP and **MasterCard**'s SDP requirements, and uses Fair Isaac's neural network to prevent card fraud.

RBA International – Vancouver WA – www.rbaintl.com

OSCARDS 2006

**Sponsors –
French Media
MasterCard**

**Competition –
700+ bank card
products worldwide in
Technology Division**

**Results –
Winner: French Bank
with MasterCard
product**

**Runner-up: RBA with
VISA Debit Card and
an American Bank**

Priceless

RBA International - Key Personnel

René Babi - Founder and President



Mr. Babi has over 35 years of extensive international experience in business processes, banking systems, information systems technologies and methodologies, and organizational development. He is described as a visionary, inventor, product evangelist, and dynamic leader.

Prior to founding RBA International, Mr. Babi served as Worldwide Service Systems Manager, Group Marketing Systems Manager, and IT Director for Hewlett Packard, IT Director for Mentor Graphics, and VP and CIO for Sequent Computer.

He has been the keynote speaker at numerous technology conferences by Apple, Hewlett Packard, Council of Logistics Management, Airfreight Forwarders, and recently the 2006 MVNO Conference in Las Vegas. He was asked to provide a white paper to the US Senate Banking Committee.

Since founding RBA International, Mr. Babi has founded and helped form numerous companies here and abroad. He is a technology and business consultant for emerging and established companies, including VISA, Nike, and Hewlett Packard. Mr. Babi and the RBA team have won prestigious awards and international recognition for their innovations and strategic contributions. Foremost is the "MCI Entrepreneur of the Year Award."

Mark Silbernagel - VP of Engineering



Mr. Silbernagel has been a partner with Mr. Babi since 1985, and has over 25 years experience as a software engineer and systems architect. He specializes in object oriented technologies for eCommerce and banking systems and worldwide network and server security.

Mr. Silbernagel served as a Technology Development Manager for Hewlett Packard, Mentor Graphics, and Sequent Computer. He was an architect for HP's global systems and Internet security policies. He was the Systems Network Architect and Project Support Manager for one of the world's largest object-oriented development projects (over 2,000 engineers, 10+ million lines of code). He has been a key speaker at Interop.

Sam Rollins - SVP of Bank & Security Products



Mr. Rollins has over 30 years in management of information technology and security systems. Most recently, as Senior Vice President of Global Information Security for VISA, he established the Information Security function at VISA, developed VISA's global security operations, risk assessment, and global network security monitoring processes, including the VISANet Security Compliance Management Framework. He was responsible for the implementation of VISA's Information Security Program at VISA member banks globally.

Prior to VISA, Mr. Rollins was Senior Manager of Information Technology for Nike, he was responsible for developing and deploying Nike's global product design and production networks linking Asia, Europe, South America and the USA. He designed and implemented Nike's financial management network and Information Security Program.

RBA International, Inc.
703 Broadway, Suite 600
Vancouver, WA 98660
800-348-8962
www.rbaintl.com