Technology

Percentage of Credit Unions Offering Websites	
United States	52.30%
California	71.95%
Nevada	75.86%

Credit Union Electronic Services

What online services are credit unions are offering? Credit unions in California and Nevada have increased their online banking services and generally offer a higher percentage of services than the rest of the credit unions in the United States. The percentage of U.S. credit unions offering websites was 52.3 percent while nearly 72 percent of California and 76 of Nevada credit unions offered websites according to Callahan and Associate Peer-to-Peer, data year end 2004. California credit unions increased their Web services since last year's WestScan that showed 64 percent of California credit unions had websites and 65 percent of Nevada unions offered websites.

How Credit Union Members Access/Perform Electronic Financial Services

	United States	California	Nevada
ATMs	52.92%	68.82%	82.76%
Audio Response	50.80%	70.56%	79.31%
Home Banking/PC Based*	15.41%	23.34%	31.03%
Internet Access Services	45.09%	60.45%	72.41%
Kiosk	3.16%	6.10%	3.45%
Wireless	2.43%	4.53%	10.34%
Other	2.47%	2.44%	3.45%

*Home banking/pc based: member access services via a home banking computer program. Generally, members use their computer to dial up the credit union directly and use the credit union

When we look at how credit union members accessed electronic financial services, California and Nevada credit union members accessed electronic financial services such as ATMs, audio response, Internet access, kiosk, and wireless at higher percentages than the rest of the country's credit union members did. The use of wireless services remained low and has not changed much since last year when U.S. wireless access was 2.4 percent, California access was 4.2 percent and Nevada access was 13.8 percent. U.S. wireless usage increased to 2.43 percent, California increased to 2.44 percent and Nevada decreased to 10.34 percent. Some credit unions who previously offered wireless access have stopped offering wireless services.

[Note: When I searched on Wireless access and credit union some that previously offered it, no longer did]

Financial Services Offered Electronically			
	United States	California	Nevada
Account Balance Inquiry	56.03%	71.95%	82.76%
Share Account Transfers	53.65%	70.91%	86.21%
Loan Payments	47.66%	64.11%	86.21%
View Account History	48.21%	64.81%	75.86%
Share Draft Orders	45.37%	59.76%	75.86%
Download Account History	38.60%	54.01%	65.52%
New Loan	32.98%	47.91%	48.28%
Bill Payment	28.61%	47.56%	41.38%
Member Application	22.09%	33.62%	10.34%
New Share Account	11.92%	19.86%	10.34%
Electronic Cash	4.80%	3.66%	3.45%
Merchandise Purchase	6.02%	7.84%	10.34%
Account Aggregation	4.26%	6.79%	3.45%
Electronic Signature Certified	0.69%	1.74%	0.00%

The types of financial services offered electronically by credit unions were much greater for Nevada and California credit unions than for U.S. credit unions. The percentage of credit unions in Nevada and California for; account balance inquiries; account transfers; loan payments; account history viewing; share draft orders; account history downloads; new loans and bill payment were higher than credit unions elsewhere in the U.S. Nevada was slightly lower in new share accounts (10.34 percent) than the United States (11.92 percent.)

Pew Research Online Bankers Educated, Affluent and Net-Savvy

The increase in website offerings by credit unions followed the trend in the U.S. towards online banking. In a February 2005 report, "The State of Online Banking," by Susannah Fox at the Pew Internet & American Life Project, found that 53 million people or 44 percent of Internet users and one-quarter of all adults said that they used online banking. The figures amount to an increase of 47 percent over the number of Americans who were performing online banking late in 2002.

Online banking has spread along with the increase of high-speed broadband connections. Fully 63 percent of those with broadband at home have tried online banking, compared to 32 percent of those with dial-up connections. Over half (51 percent) of those who have more than six years of Internet experience have tried banking online, while only 27 percent of those with three years or less of online experience tried online banking.

A large portion(60 percent) of Gen X (28-39) have tried online banking, 38 percent of Gen Y (18-27) and only 25 percent of those over 60 have tried online banking. Men are more likely to perform online banking than women, 49 percent of men have tried online banking compared to 39 percent of women online. Those with higher household incomes (55 percent with incomes of $75,000 or more) and the well educated (52 percent with a college or a post graduate degree) were major users of online banking.

The report suggests that the rise in online banking flows from two major trends. First as Internet users gain more experience online, they are more likely to perform more Internet activities that involve money. The second is that the banks themselves discovered the virtues of online banking and are aggressively offering it to customers. Financial institutions discovered studies showing that online banking customers are more profitable than offline customers because they make fewer service calls and are less likely to switch banks.

Earlier research in 2004, from Forrester Research and the Online Publishers Association (OPA) both reached the conclusion that younger Internet users consume more financial services online than older demographics. Forrester determined that of consumers who applied for credit products in 2003, 48 percent of "Generation Y'ers" (age 18-28) and 42 percent of "Generation X'ers" (age 29-39), had conducted research online first, compared to only 30 percent of "Baby Boomers" (40-57) and 16 percent of Seniors (58+).

At first glance, both the Pew study and Callahan's Peer-to-Peer data indicate that California and Nevada credit unions are doing a better job electronically with members using most Web and electronic services, however, credit unions should always consider ways to improve services and keep ahead of the e-pack of financial offerings. A study by Forbes.com and ForeSee *Online Banking: Customer Satisfaction and Its Implications for Building Loyalty and Influences Buying Behavio*r confirms great customer satisfaction with credit union online services. It also offers some useful advice.

The ForeSee study rates services on customer satisfaction, the key metric to asses how effectively online banking furthers financial institution objectives of customer acquisition, retention and increase share of the wallet. The first survey was performed in summer 2003 and the overall satisfaction of online banking customers has increased 5.5 percent in fourth quarter of 2004. The survey also found that customers who pay their bills online were more satisfied than those who did not. Customers who paid their bills online were 11 percent more satisfied than online bankers who did not. Highly satisfied online bankers were nearly 40 percent more likely to purchase additional products and services from their financial institution than were very dissatisfied online banking customers.

Credit Unions Score High

The latest ForeSee study delved deeper into different types of financial institutions: large banks, community banks and credit unions. While scores for all three were strong, credit unions outperformed both types of banks in terms of satisfaction and usage of most online banking features. Satisfaction with most elements of the online banking experience were higher for credit unions except for "bill-payee set-up"

Usage of Online Bill Payment for Credit Unions Lower

In almost all cases credit union members in the survey were the most eager adopters of online banking features. Usage by credit union members exceeded that of all customers of both large and community banks. Even one of the lesser used features, loan applications was more popular among credit union members. Nearly one quarter of credit union respondents said they applied for loans online, compared to 9 percent for large banks and 5 percent for community bank customers. The only activity where credit unions fell short was in online bill payment. In this area credit union usage (65 percent) was less than larger bank customers (75 percent.) Credit union members who paid bills online were 9.2 percent more satisfied than members who did not. The report states credit unions could experience gains in satisfaction through conversion of more members to online bill payers.

Keep the Online Bill Pay Customers Satisfied

Online bill pay customers were 17 percent more likely to purchase more products/services and 34 percent were more likely to recommend their financial institutions website to others. Eighty-seven percent of online bill payers visit their financial website at least once a week and 41 percent visit the website daily. These frequent visits provide credit unions with opportunities to develop reinforced relationships and market new products and services.

[Note: It looks like the charts in the study are not that great. After I downloaded the study, they called me. Their guy said that if we want we can call and get a credit union quote from Larry Freed (734) 205-7570.]

Privacy Concerns

The Credit unions scored extremely well but the study warns of privacy concerns. Although online banking users privacy scores were higher for people who bank online and the group did not feel that they were required to provide too much personal information, respondents who did not bank online, cited privacy concerns. Among prospective respondents privacy concerns were cited by 34 percent as a barrier to signing up for online banking. For people who described themselves as "not at all interested in banking online" privacy was the key issue and it was cited by 68 percent of survey respondents as a reason for not banking online. The report concluded that the solution lies in better education of potential customers on privacy issues and safeguards.

A December 2004 poll by Cambridge, Mass.-based Forrester Research Inc., indicated 26 percent of online consumers surveyed said e-mail fraud concerns had stopped them from applying for a financial product over the Internet and 20 percent of online consumers don't open e-mails that appear to be from their financial provider because of fraud concerns, reported Jaikumar Vijayan in *Computerworld*.

Information Security

Security has become a major concern of members and credit unions. There is an increased climate of data privacy concerns in the news, such as customers' personal data being hacked by users of ChoicePoint in early 2005. Credit unions ought to consider better ways to protect information security and educate their members.

There are different aspects of information security a credit union needs to address. "The most important thing to keep in mind is that information security requires ongoing diligence" said Kelly Dowell, founder of the new Credit Union Information Security Professionals Association (*CUISPA*) in "What Are the Components of Information Security?" a *Credit Union Magazine* Online Exclusive in February 2005. The components of a good security program include:

- "Policies and procedures that outline proper use of information and information systems.
- Technology countermeasures to prevent intrusions, attacks, and system misuse.
- Education programs for the information technology (IT) staff management team, and all employees.
- Roles and responsibilities for managing information security.
- Periodic review and evaluation of the program's effectiveness."

In a corporate credit union guidance letter, the NCUA issued four guidelines for securing networks some of these overlap with Dowell's guidelines such as; **maintain an information systems security policy;** together with these additional recommendations:

- **Conduct regular vulnerability assessments** – The scope should include network infrastructure, user authentication procedures and organizational security practices. This work is usually accomplished by a combination staff resources, outside consultants and automated network analysis tools.

- **Follow a cross-functional network oversight program** – Vigilance and continual refinement of the security infrastructure are the primary lines of defense to safeguard corporate technology. An oversight process should involve the efforts of IS staff, internal external auditors, IS service providers and the corporate security officer and committee.
- **Penetration testing** - Penetration testing should be used to ascertain whether reasonable defense measures are employed to protect the corporate network.

Most credit unions have information security policies in place; however, it is still important to review the latest technologies, new threats, studies and trends in the financial industry regarding information security. There has been a surge of information this year with increased threats and stories of financial institutions data hacks and data loss one example being Bank America's loss of credit card data reported in February. The bank lost computer data tapes during a shipment to a backup data center. The tapes contained personal information on 1.2 million federal employees, including Social Security numbers and account information that could possibly make customers vulnerable to identity theft.

Penetration Testing

The April 2005 issue of *Credit Union tech-talk* explains the difference between penetration testing and vulnerability assessments. Assessments find vulnerabilities while penetration testing attempts to exploit a vulnerability. Penetration testing can be either external or internal.

External penetration testing can be conducted using one of two approaches: black-box (with no prior knowledge of the infrastructure to be tested) and white-box (with a complete knowledge of the network infrastructure). Both methods have value to help discover potential exploitations because often hackers are able to discover some information about the network.

A 2004 study by the FBI and Computer Security Institute reported that 50 percent of all organized network security breaches were caused by internal attacks. Internal penetration testing should be conducted from all access points including wireless points.

SOCIAL ENGINEERING – The Human Element of Information Security

Penetration testing also should include the human side of penetration. Social engineering exploits human vulnerabilities to obtain information about an organization and its network. It can take the form of eavesdropping during a conversation, getting data by "dumpster diving" or aggregating data from different sources.

Jim Stickley, Chief Technology Officer of TraceSecurity and his team of consultants successfully social engineer their way into banks and credit unions impersonating people of trust or authority, such as an air conditioning technicians, pest exterminators or a fire marshals. Financial institutions engage TraceSecurity to asses their vulnerabilities and deploy security measures.

The team's planning for their heists begins weeks in advance, often by mailing a letter to a bank branch on forged stationary, informing them of a planned "inspection." By the time they show up in their fake uniforms with fake badges and fake identification cards, the front receptionist often welcomes them with coffee. Within minutes, they have free range of the bank as they crawl under computers, steal backup tapes, and install spyware on the computers. In the evening, the TraceSecurity team returns to dumpster dive, an activity that often yields a surprising amount of sensitive customer account information.

Stickley in "Confessions of an Identity Thief" at the *TraceSecurity* website recommends financial institutions adhere to good practices to reduce security risks by: conveniently locating shred bins; making sure that computers or confidential information is not left unattended; encryption of data; e-mail verification; and employee training.

Conveniently Locate Shred Bins

Many banks use paper shredders, but unless shredders are conveniently located near all branch personnel, they don't get used properly. Stickley has found that unless the shred bins are within a few feet of employees, many documents will simply find their way into the trash bin, unshredded, and ready to be discovered by information thieves.

Unattended Computers

Most banks concentrate their security at the entry to the facility or branch. Beyond the initial greeting area, that security often becomes more lax. Employees, assuming that anything on their desk is safe because they are located away from the front area, often leave sensitive paperwork on their desks, or leave Post-It notes on computer monitors listing log-on IDs and passwords. This is a major mistake because visitors, maintenance, and other individuals often receive access to this area. In addition, computers should not remain logged in while employees are away at lunch or after they've gone home for the day. Unattended computers put a financial institution's information systems at risk.

Encrypt All Sensitive Data and Back-Up Tapes

Confidential data should be encrypted at all times when not being used. This includes information stored on workstations and laptops. There are a number of applications available that will encrypt sensitive documents on the hard drive, so if a laptop or workstation is accessed or stolen, the data that has been encrypted will be protected from identity thieves. Additionally, all backup tapes must be encrypted and stored securely off-site. There are a number of storage security appliances that encrypt the data as it is stored to the tapes. This will reduce the risks associated with tapes being lost or stolen. On numerous occasions Stickley has stolen unencrypted backup tapes that were sitting on shelves in plain view. These tapes, often as small as a pack of cigarettes, have contained account information for thousands of customers.

According to *Credit Union tech-talk*, in response to the Bank of America tape loss, Boeing Employees Credit Union (BECU) has partnered with Decru to encrypt all data written to their backup tapes. BECU uses Decru's appliance to protect against unauthorized access to tape information that is moved off-site to a long-term archival site from four main data centers.

Email Verification

Financial institution customers are not the only people vulnerable to phishing attacks. Phishing tactics can extract critical information from employees. Employees need to understand that any e-mail that appears to come from another employee or legitimate source could be forged. If a manager requests confidential information from an employee via email, the employee should always contact the manager via the phone for verification. Banks should also consider adding cryptographic signatures to enable authentication.

Policy Enforcement and Employee Training

Employee awareness training and strict policy enforcement are the most important methods to protect an organization from identity thieves. Monthly meetings should be scheduled to review security policies. For example, employees must understand that bank visitors must be accompanied at all times, and that unoccupied desks should be free of confidential information, and filing cabinets should locked when unattended. Additionally, policy management software should be an essential component of any security program to ensure that employees are contacted when policy and procedure changes occur.

The March 28, 2005 *Credit Union tech-talk* newsletter offers the following spin on employees and security:

> "The Ernst & Young Global Information Security Survey last year revealed that end-user security training was the No. 1 problem inside large organizations. Many security experts are arguing that before employees are given computers and passwords, they should be given at least a half-day, if not a full-day, tutorial about the ins and outs of secure computing practices as defined by an IT department. They believe that dedicating precious time and resources to such a learning experience tells new workers (and existing ones) that management is very serious about IT security procedures. Some even go so far as to say that you should use the carrot and stick approach to security: employees should lose one day of vacation for every security violation after the first breach, and your staff should be rewarded for keeping you secure. For example, if a credit union goes a full year without getting infected by a virus/worm, everyone gets an extra vacation day in the next calendar year."

Firewalls

A firewall is a device at the point of entry of the network designed to prevent unauthorized access to or from a private network. Sometimes there is confusion if a firewall has enough security. In "The Top Ten Security Questions" a *Credit Union Magazine* Web Exclusive provided by Cavion Plus states that a firewall does provide some security but often times, even a properly configured firewall does not block allowed services such as e-mail and Web traffic. In these environments, a firewall does not filter, block, or even examine this traffic once it is allowed. There are three ways of looking at your firewall.

Maintained Firewall

With a maintained firewall, no one is managing or monitoring it. This can be summed up that somebody can fix it when it breaks. An example of this is one day a company can not get e-mail and they realize their firewall is down. Then they call someone to come and fix it.

"This unfortunately is the most common occurrence in credit unions," said Kevin Prince, President, Red Cliff Solutions, an Internet security company that provides services for credit unions. For instance, a credit union orders high speed Internet access and the ISP tells them that a firewall is included. Typically, an ISP performs only maintenance, which means if the device fails, they will replace it and it often doesn't have the robust security features needed to protect a financial institution. Usually, the ISP configures the firewall for the base level connectivity requirement and leaves it as is. Most never update the software.

Managed Firewall

A managed firewall includes maintenance of the firewall and a trained Internet security expert:

- Ensures the configuration is correct.
- Keeps the software and security patches up to date.
- Makes appropriate changes when needed or requested.
- Acts as a consultant to assist in ensuring the financial institution makes proper Internet security decisions.

Monitored Firewall

A monitored firewall includes all the features of maintained and managed firewalls plus the addition of review logs for suspicious activity and monitoring of uptime to make sure the firewall is always online.

Most firewalls typically do not have the capabilities to warn or stop an intrusion except for high level attacks like port scans, denial-of-service, spoofing etc. This is due to a lack of deep packet inspection capabilities (the ability to look inside the packet payload for malicious activity), which is a sophisticated method to identify an attack. It is not that monitoring is not important, it is just that monitoring a firewall alone has little value and only provides login information, basic alerts, traffic, and other high level information. Therefore, there is far more value in installing and monitoring an intrusion detection and prevention system in addition to a firewall, rather than a firewall by itself.

Intrusion Detection and Prevention System (IDS and IPS)

Intrusion detection systems monitor system and network resources for malicious attacks or intrusions. Intrusion prevention systems use the same technology but have the added benefit of stopping attacks. Most financial institutions do not realize that the intrusion prevention technology exists to accurately prevent attacks in real-time without blocking legitimate traffic. Therefore intrusion prevention systems are a better investment.

If a credit union hosts services (which means the server is in the credit union network) such as e-mail, a website, online banking, and so on, then an intrusion prevention system is critically needed says Prince. If the credit union does host any services but has many other potential attack sources, such as inbound modems, partner connection, or virtual private network, then using an intrusion prevention system is moderately to highly encouraged. If the credit union has broadband Internet access and employees have unrestricted access to the Internet, an intrusion prevention system is moderately encouraged.

Vulnerability Assessments

A vulnerability assessment is intended to be a test against any Internet accessible device for vulnerability and weakness. If the credit union hosts services, monthly assessments are highly encouraged due to the increased risk according to Red Cliff Solutions. If the Internet access is for outbound use only (i.e., web surfing), a quarterly assessment usually is sufficient. Test all publicly accessible systems. This includes the firewall's public address or any public system, such as a website, e-mail server, or file transfer protocols server that is hosted at the credit union. Depending upon the credit union environment, the Internet router may need to be tested as well.

An internal vulnerability assessment can also be performed against all systems on the inside of the network. This often is performed in conjunction with a patch management system to keep internal systems up-to-date.

Outsourcing Vendors – Managed Security Service Providers

Often it is more cost effective to outsource security components with a MSSP (managed security service provider), such as remote vulnerability assessments, firewall management, and intrusion detection and prevention. "Most MSSPs offer a range of services… are more cost-effectively than doing the job in-house. But not all MSSPs are alike," says Megan Goldin in an article "Who's Minding the Store?, Questions to Ask Managed Security Service Providers" posted at the *SecureWorks* website. Many have experience working with credit unions and compliance issues. Ask for recommendations from other credit unions and case studies. Make sure that the service understands your credit union's security and compliance issues. It is helpful to find out:

What the MSSP does when it detects an attack – IT managers should ask if they actually stop attacks (intrusion prevention) or if they sound the alarm (intrusion detection). Stopping attacks in real-time is the definition of an intrusion prevention system.

The lag time between detection and blocking - The time between detection and protection is crucial. Automated attacks, like Code Red and Klez, call for automated responses. Make sure that the MSSP detects and protects instantaneously, using automated attack blocking and proactive signature updating.

How often the MSSP updates the signature set - An IDS/IPS must be updated regularly to be effective. The MSSP should be able to describe its process for writing and distributing new signatures and how often they do it.

If the MSSP monitors the network live, 24x7x365. When Internet security is outsourced to an MSSP, services should include around-the-clock protection. Find out about the MSSPs security operations center and review their security analysts' backgrounds and experience.

Reporting Features – Make sure that the credit union has access to reports and logs that are easy-to-read and understand. The reports should be saved for compliance. Some MSSP offer the ability to co-manage security measures and set privileges such as e-DMZ which allows the credit union to retain as much or as little administrative privileges as deemed necessary.

Here is a list of some Managed Security Service Providers.

CavionPlus – http://www.cavionplus.com.
CuProtect - http://www.cuprotect.com/
e-DMZ Security - http://www.e-dmzsecurity.com/
Message Secure Corporation - http://www.messagesecure.com/
Red Cliff Solutions - http://www.redcliffsolutions.com/
SecurePipe Managed Network Security - http://www.securepipe.com/
SecureWorks - http://www.secureworks.com/

(Note: you can move these to an appendix at the end if you prefer.)

Two Factor Authentication

Authentication is the process of identifying an individual, usually based on a username and password.

Two factor authentication includes a password and a second factor via software or hardware. It was reported in the March 7, 2005 issue of eWeek, that E*Trade customers will be the first financial institution customers to be offered two-factor authentication system for transactions. The company will offer RSA Security's SecurID tokens to high-end customers in the second quarter of 2005. E*Trade's program is called Digital Security ID and will be voluntary. SecurID tokens will be free for customers who have more than $50,000.00 in assets managed by E*Trade.

The E*Trade authentication scheme is based on RSA Security Inc.'s SecurID token technology and will allow E*Trade customers to use a random and constantly changing number in conjunction with their regular user IDs and passwords to access their E*Trade accounts. The tokens give customers an additional layer of protection and make it impossible for unintended or unauthorized users to gain access to E*Trade accounts by stealing, reported Jaikumar Vijaya in *Computerworld*. Unlike static passwords, which can be stolen and misused, RSA's tokens generate a unique six-digit code that changes every 60 seconds.

Thomas Wright, Editor and Publisher at *Credit Union tech-talk* forecasts that two-factor authentication is the wave of the future, he recently wrote:

> “Some security experts believe that the day when two-factor authentication is mandatory for online banking access is drawing near. They point to the fact that the Federal Deposit Insurance Corporation (FDIC) is currently formulating guidance that will encourage US banks to abandon single password-based ID systems in favor of two-factor authentication following a sharp rise in account hijacking ID theft.”

At the RSA Conference in February 2005, both RSA and VeriSign announced new tokens according to *Credit Union tech-talk*. VeriSign announced that it will offer a one-time password token with a total cost of operation per user of less than $10 a year They also will be releasing a dual-purpose USB authenticator with either 128-Mytes or 265-Mbytes of secure storage. The USB authenticators can be used to store one-time passwords, PKI (Public Key Infrastructure) credentials, and provide functionality similar to that of smartcards.

Bio Two-Factor Authentication

The San Antonio City Employee FCU has added a second layer of protection in authentication for laptop use, according to *Banker’s Hotline*. SACE FCU uses software based on biometric technology that recognizes keystroke speed and the rhythm of the user’s typing. Once BioNet software is installed, the employees create their biometric keystroke pattern themselves by entering a company provided password. Employees can only access the information on the notebook computer by knowing the password and having the right touch in entering the password. The system is invisible to employees once it is set up.

Identity Theft Services for Credit Union Members

Two services have been recently launched to help credit union members deal with identity theft; Identity Theft 911 and Identity Guard® ProtectX3^{SM} from CUNA MUTUAL GROUP.

Identity Theft 911 offers credit members who fall victim to identity theft a free program that includes a personal advocate to help restore identity after it has been stolen, preparation of all needed documents, and fast, effective notification of all credit bureaus, agencies, and businesses. The program also includes access to an educational website filled with up-to-date news and information about the latest identity theft scams and defenses. Identity Theft 911 has been adopted by several Credit Unions.

Identity Guard® Credit Protect® X3(SM) is a plan paid for by the members and sold via the credit unions that includes a 3-in-1 credit report, 3-credit-bureau monitoring every business day with prompt alerts , quarterly credit updates, $20,000 identity theft Insurance, access to credit education specialists, and access to identity theft recovery unit

Technology Round Up

Technology changes quickly and it is always advisable to check-in on industries and examine at the latest developments and trends before making any technology decisions. Following is an overview of some technology trends, some are new and others that have been around for some time.

NEW ATM TRENDS

The top trends in ATM technology are the move to Windows-based ATMs; Web enabled ATMs, cross-channel integration and the first phases of checking imaging adoption.

Windows Software a Window of Opportunities

With the implementation of Triple DES compliance many ATMs have been upgraded to the Windows operating system but there could be more reasons for upgrading for Windows. The Windows-based machines are requiring fewer service calls than OS/2 models and when techs visit the Windows ATMs they are spending less time there due mainly to available menu-driven diagnostic tools that make it easier to pinpoint problems according to *ATMmarketplace*. The capability to run some diagnostics remotely and distribute software remotely cuts down on service calls. A high percentage of service calls are resolved by rebooting the machine.

According to research by TowerGroup 30 percent of the world's ATM machines will run on Windows by 2006.

Web Enabled ATMs

The Windows operating system has made it easier for financial institutions to Web enable their ATMs. According to *Computerworld*, Wells Fargo completed a five year project to Web-enable 6,200 of its ATMs in 23 states. It also installed 3,000 online Internet stations in branch locations.

Wells Fargo’s webATM machines feature customizable fast-cash amounts and receipt preferences, six language options and access to 22 financial accounts such as brokerage and mortgage services. Customers can check on their account balances and transfer funds among accounts just like they do with their online banking.

In addition, all Wells Fargo ATM locations have at least one machine offering voice instructions for the visually impaired in both English and Spanish. The Windows-based infrastructure allows Wells Fargo to update and add new services to its network remotely, making it easier to add new features such as the ability to accept envelope-free deposits. Wells Fargo claims it is the first bank to have completely Web-enabled its ATM infrastructure. Bank of America has also Web-enabled 3,500 of its 16,500 ATMs.

Wells Fargo webATM machines and online stations are part of its strategy to integrate all channels: stores; phone; ATM; and Internet to enable customers to access financial services through all of them.

Cross Channel Personalization and Integration

“While 50 percent of financial institutions share customer profile data across channels, only 13 percent offer actual cross-channel interaction,” said Brian Adrian at Gartner Inc. in an interview with *ATMmarketplace*. In an ideally integrated world, a consumer who placed a query about a missing check via a telephone banking system could received a message that it had been located while using the ATM. As ATMs become more compatible with other systems, financial institutions ought to consider ways of aligning their ATM vision with their Internet vision advised Adrian.

Cross-channel personalization can save time in the ATM line and online. If a member does the same transaction at the same ATM every week and or always does the same function during an online session, and their preferences are remembered, customer satisfaction will be enhanced.

National City, one of the nation's largest financial holding companies which operates through an extensive banking network primarily in Ohio, Illinois, Indiana, Kentucky, Michigan, Missouri and Pennsylvania, in August 2004 introduced the ability for its customers to pre-select a preferred language, a receipt feature and a usual withdrawal amount. Customers appreciate the feature because it saves them time at the ATM reports *ATMmarketplace*. The ATM system from First Data Corporation, automatically recognizes pre-selected preferences when customers enter their PINs. The fast cash button is positioned at the top left where it easy to see. Wells Fargo has a similar service called

MyATM which also shows advertising for products targeted to the specific ATM customer.

Check Imaging ATMs

Wells Fargo is testing ATMs that use the check imaging technology and have achieved a 96 percent rate approval according a March 7, *New York Times* article. Customers place checks directly into the machine which records the check amount and displays the image of the check on the screen and on the customer's receipt. Because the deposit is entered into the bank's central accounting system, via the Web, those funds can be used immediately.

Most of the top 20 banks in U.S. and Canada are piloting check imaging programs, reported *U. S. Banker*. In the fall of 2004 Bank of American ran a high profile television ad touting ATMs that let consumers feed cash and checks directly into a Diebold machine. TowerGroup data estimated the cost of an ATM deposit on par with a teller transaction at $1.70 per transaction, and new check-imaging ATMs cost 40 cents each.

Starting in May 2002, America First Federal Credit Union in Riverdale, UT, participated in a pilot check imaging program with Diebold and deployed ATMs with check-imaging. The FFCU ATMs have greater numbers of check transactions than machines without imaging. The ATMs cost $2,000 to $3,000 more than conventional ATMs but the operating expenses were reduced.

Check Imaging Financial Services

After the Check Clearing for the 21 Century Act (Check 21) took effect last October, financial institutions began adopting Check 21 service. The law enables financial institutions to generate substitute checks, or image replacement documents (IRDs), with the same legal status as an original check.

Navy Federal Credit Union selected NCR Corporation to provide end-to-end, image-based technology across Navy Federal's entire enterprise for check-image capture, processing, storage and access for image delivery and exchange applications, states an NCR news release. Transactions will be electronically transmitted to Navy Federal's processing center in Vienna, Va., where NCR's ImageMark Transaction Manager system will validate, balance and consolidate check images.

The credit union needed to replace their check archiving and microfilm system with a single enterprise-wide image archive. They also wanted to utilize distributed check-image capture to further automate deposit processing.

Desktop Scanned Deposits

Wells Fargo is bringing the ability to deposit checks right from a customer's desktop with The Desktop Deposit (SM) service available through Wells Fargo's Commercial Electronic Office ® portal. Customers scan checks at their desk using equipment provided by Wells Fargo. Then they review the images and electronically send the deposit to the bank over the Internet, stated a Wells Fargo News Release.

Check imaging is also being implemented by U.S. Bank commercial customers through On-Site Electronic Deposit, according to *The Colorado Springs Business Journal*. Commercial customers purchase scanning machines and software from U.S. Bank that enables them to electronically deposit checks. The checks are scanned and then electronically transmitted to U.S. Bank for deposit into the commercial customers account. The process eliminates the need for the customer to take the checks to bank.

CRM for Websites

Personalization of websites can be achieved via specialized software. WebMRM, a Web customer-relationship software, developed by aaBeck Technology Group, was implemented at Monterey Park, CA-based F&A Federal Credit Union in 2004, reported *The Credit Union Times*. In April, May and June cross-sales were substantially higher than expected at F&A FCU because of the software. WebMRM is designed to use a credit union's MCIF and member transaction data to analyze and automatically select the offers to which a member is likely to respond. It then rotates the chosen offers to that member when he or she visits the credit union's website.

Payroll Cards

One of the fastest growing additions to the stored-value-card market is the payroll card, an alternative way for an employer to pay employees, especially needed for employees who are unbanked. Payroll cards have been marketed as a method for employers to eliminate the high costs of issuing and processing paper checks. The Fed's Consumer Advisory Council estimates that payroll cards will be dispensed to 25 percent of the country's unbanked workers by 2006, according to *American Banker*.

In the past, payroll cards allowed employees to access funds through an ATM or some PIN-based point of sale locations. Currently, the trend is for payroll cards to carry a Visa or MasterCard brand so that they can be used anywhere those cards are accepted according to *Community Banker*.

The National Restaurant Association added to its member benefits a program that provides restaurant employees payroll cards that work like a PIN-based ATM through Money Network which offers a 24-hour, 7 day a week, bilingual customer service center and electronic pay-stub delivery. Employees receive the cards instead of traditional paper checks and money is added to each employee's account each pay period. The program was announced via a news release last year.

Santa Barbara-based Business First Nation Bank launched "eZmonE payroll Card" to eliminate paper paychecks and for the convenience of the unbanked reported the *Knight Rider Tribune News Service*. For the employer the cost of processing the payroll card is much lower when compared to a traditional payroll check. The bank charges a one-time $5.00 fee for each card. In comparison the American Payroll Association reports that the cost of processing a traditional payroll check is about $1.35 per check issued. For 100 employees paid bi-weekly, the traditional cost would be $3,510 a year as compared to $500.00 total for 100 payroll cards.

RFID Radio Frequency I.D.

RFID stands for radio frequency identification. Its technology lets anyone send, store and retrieve data remotely, using RFID tags equipped with antennas. RFIDs first became prominent in the news as part of inventory systems. Wal-Mart required suppliers to implement RFID systems. RFID tags are used to track beer kegs, identify Las Vegas poker chips and lost pets. They can be found in car key fobs, books in libraries, clothing tags, airline baggage tags, ID badges, On-Star auto systems, toll booths and can be attached to prison inmates. Mexico City Police are implanted with tags that are designed to help track them if they are kidnapped, reports Molly Wood on *CNET.com*. The tickets to 2006 World Cup Soccer Tournament will be embedded with RFID tags which should speed up entry the games. Some medical centers are tracking patients with RFID badges.

Contactless Payments

One of the most widely known uses of RFID is the ExxonMobil's SpeedPass. At the gas pump, the customer waves the pass and then does not have go through the process of sliding a credit card or entering a PIN.

In 2004 MasterCard International's PayPass system was rolled out to some 715 McDonald's restaurants in New York, Dallas, and Orlando reports *Credit Union tech-talk*. The McDonald's deployment was the first commercial rollout of MasterCard's RFID technology. With PayPass, cardholders tap or wave their cards on or near a receiver linked to a point-of-sale terminal. McDonald's is using the Omni 7000, a terminal from VeriFone,.

In February, 2005 Visa USA launched an RFID card system, designed for small ticket items. The card works at a distance of 4 inches or less and Visa in guaranteeing purchases for items up to $25.00 according to *Information Week*.

RFID Passports to Information

The use of RFID as a form of identification, appears to be growing steadily. The State Department's Office of Passport Policy, Planning and Advisory Services announced that is ready to issue RFID enabled passports, reported *Medill News Service* in March 2005. The agency plans to issue the first passports carrying the chip by mid-2005. The chip will include all the personal data found on the information page of today's passport and a digital face image, the biometric component. The new passports comply with requirements set forth by the International Civil Aviations Organization for machine-readable passports with biometric information. The fee for passports is expected to increase to cover the cost of the new technology.

It will be interesting to see where RFID goes and whether or not, in the future credit unions will have to adapt RFID technology for ATM/credit cards or to read employee badges or some new form of identification. Credit Unions have been known to be on the cutting of edge of technology and will swiftly scan the environment for best services for their members.

BIBLIOGRPAHY

"Biometric Passports Set to Take Flight," by Erin Biba, Medill News Service, appearing at PC World, March 21, 2005.

"Confessions of an Identity Thief: Jim Stickley Robs Banks for a Living," TraceSecurity website.

"E*Trade Touts Two-factor Authentication Service," by Jaikumar Vijayan, Computerworld, March 02, 2005.

"F & A FCU Finds Promise in Single-Channel MRM Solution," by Marc Rapport, Credit Union Times, September 28, 2004.

"Full Speed Ahead for World's Largest Credit Union Thanks to NCR's Check 21 Technology," NCR News Release, March 8, 2005.

"Hawking the ATM of the Future", by Matthew de Paula, U.S. Banker, November 2004.

"Information Security Part II, Penetration Testing," Credit Union tech-talk Newsletter, April 2005.

"Information Systems - Network Security Guidelines," Corporate Credit Union Guidance Letter 2001-02, NCUA 2001.

"Is Channel Integration Finally Ready for Its Close-Up?" by Ann All, ATMmarketplace, April 19, 2004.

"Microsoft ATMs Are Easier to Keep Up and Running," by Ann All, ATMmarketplace, March 7, 2005.

"National Restaurant Association Launches New Member Benefit," US Newswire, August 4, 2004.

"New Study Highlights Impact of Online Media on Financial Services Sector," The Smart Marketing Report, Double Click, September 2004.

Online Banking: Customer Satisfaction and Its Implications for Building Loyalty and Influences Buying Behavior, ForeSee Results, 2005.

"Paperless deposit program saves time and money," by Marylou Doehrman, The Colorado Springs Business Journal February 11, 2005.

"Payroll Cards," by Nancy Feig, Community Banker, January 2005.

"RFID: Bring it On," by Molly Wood, CNET.com February 11, 2005.

"Santa Barbara, California Bank Hopes Payroll Cards Appeal to Unbanked Workers," Maria Zate, Knight Ridder Tribune, News, July 11, 2004.

"Second Layer of Password Protection," Banker's Hotline Volume XIV, Number 8.

"Security" Credit Union tech-talk Newsletter, March 28, 2005.

"The New Wells Fargo Electronic Deposit Services Break Through Banking Boundaries in the Age of Check 21", Wells Fargo News Release, March 28, 2005.

"The State of Online Banking," by Susannah Fox, Pew Internet and American Life Project, February 2005.

“To Attract More Internet Customers, Some Banks are Adding Services Available on their Websites to Their ATMs.” by Bob Tedeschi, New York Times March 7, 2005.

“Warming Up a Cold Channel” by Ann All, ATMmarketplace, January 13, 2005.

“Wireless World,” Credit Union tech-talk newsletter, August, 23, 2004.

”Wells Fargo Web-enables ATMs,” by Lucas Mearian, Computerworld, Mar 7, 2005.

“Who's Minding the Store? Questions to Ask Managed Security Service Providers,” by Megan Golding, SecureWorks website 2004.