Factors affecting the adoption of consumer oriented information technology biometrics solutions by the credit union industry

Kevin Scott
Midwestern State University

Charles R. Johnston
Midwestern State University

ABSTRACT

Biometrics systems have been in real world production for close to two decades. There is ample data to measure the success rate of these systems and to determine if the financial industry is widely adopting them and accepting the cost of these solutions. This research seeks to clarify whether or not it is likely that consumer oriented biometrics solutions will be widely funded and adopted by the Credit Union (CU) industry. The conclusion is that without catalysts such as firm regulatory requirements and industry standards, it may be fair to assume that consumer oriented biometrics lack sufficient business drivers to increase their use by CUs in the near future. However, CU managers must continue to monitor developments of biometrics solutions applications both within and outside the financial sector for opportunities to take advantage of the technology, rather than just deal with it, if required.

Keywords: biometrics, credit union, security, consumer, financial

INTRODUCTION

Biometrics

Merriam-Webster defines biometrics as, “The measure and analysis of unique physical or behavioral characteristics (as fingerprints or voice patterns) especially as a means of verifying personal identity” (2009). Biometrics technology has been touted as the preeminent solution to combat fraud and identity theft, enhance security and to solve password management issues. The capabilities of the existing and promised forms of biometrics are impressive.

The scope of biometrics can be divided into two primary categories for the purposes of this research investigation. They are: ‘organizational oriented biometrics’ for business security and access control, and ‘consumer oriented biometrics’ solutions for transactional security. Examples of organizational oriented biometrics are single sign-on systems and employee access controls. Examples of consumer oriented biometrics include finger print identification for transactional processing, voice interpretation for automated responses, keystroke rhythm awareness for at home banking and facial recognition systems with business analytics. The emphasis of consumer oriented biometrics in the financial services sector is to provide positive identification of individuals conducting financial transactions. These examples described are not an exhaustive list, rather a clarification of the terminology.

Biometrics systems have been in real world production for close to two decades now. There is ample data to measure the success rate of these systems and to determine if the financial industry is widely adopting them and accepting the cost of these solutions. More specifically, there is sufficient evidence to determine if consumer oriented biometrics are being used in the Credit Union (CU) industry. Some conclusions can be reached as to the drivers of their adoption and the effects of factors significantly challenging that adoption. This research will seek to clarify whether or not it is likely that consumer oriented biometrics solutions will be widely funded and adopted by the Credit Union industry.

Credit Unions

The Credit Union movement represents roughly seven percent of the United State’s financial services capabilities (Johnson, 2009). CUs are not held by stockholders. Rather, CUs are financial cooperatives governed by member owners democratically elected to serve as volunteer boards of directors. CUs also differ from banks in that they are not for profit entities. All profits are redistributed to the CUs’ membership in the form of dividends, advantageous interest rates, charitable donations and lower fees. CUs do not pay Federal income tax.

In 2006, there were 8,286 CUs in the United States. CUs have far less total assets than do banks; 85% of all CUs have less than one billion in total assets and 44% of all CUs have less than 10 million in total assets. With few exceptions, CUs do not have a unified national or global presence as do banks. The typical CU field of membership is relegated to a common employer or geographical location. Credit Unions do not offer as many products and services as the typical bank (Johnson, 2009). The size of management teams and total employees are both smaller than banks. The unique traits held by CUs are important to bear in mind when considering the adoption of a technology item such as biometrics.

CURRENT STATUS of BIOMETRICS in FINANCIAL INSTITUTIONS

In the early 2000s, there was an industry-wide rush to biometrics as a potential source of security to reduce the likelihood of fraud (Busch, 2006). Perhaps in the rush to move towards these technologies, technology business managers forgot to match the expenditures of biometrics solutions to the potential losses of fraud. In 2006, only five to seven percent of United States financial institutions utilized biometrics solutions. Of those, it was estimated that 50-100 CUs had solutions in place primarily in the form of organizational oriented systems (Heet, 2007). Aite Group, a financial sector research firm, estimates that in 2008 roughly 20% of all financial institutions used some type of biometrics solution. Their estimate is that 35% will implement by the end of 2009. However, most of the implementations are behind the scene with limited usage at the consumer level (Biometric Progress, 2008).

Consumers are intrigued by biometrics. Despite this interest, only 10% admit that they are willing to embrace the technology for financial transactions according to Javelin Strategy & Research (Bits & Bytes, 2008). Consumers are worried about the intrusiveness of biometrics and loss of personal and private information. The low rate of acceptance lessens the likelihood that CUs would spend significant funds to push out consumer oriented biometrics systems.

This claim is supported by a recent survey of future CU technology spending conducted by the Credit Union National Association (CUNA). The survey shows that the top five planned technology expenditures are the following: online banking, bill pay applications, vendor online bill pay, e-statements and email alerts (Johnson, 2008). Technological security expenditures are not listed in the top five. Also, biometrics does not show up on the list of present technology features/capabilities offered by CUs. Nor, does biometrics show up on the list of what CUs plan to offer in terms of technology solutions within the next 3 years (Soltis et al, 2008). It seems the security features, efficiencies and risk mitigation currently offered by consumer oriented biometrics solutions have not been enough to garner support from CUs.

However, there is regulatory pressure driving the adoption of biometrics in the United States financial sector. Governing bodies such as the Federal Financial Institutions Examination Council mandated a multi layered authentication approach to online banking in 2005. A physical biometric tool is one of several options that would satisfy this regulation. Legislative bills such as the Sarbanes-Oxley Act of 1992 (Section 404) and The Basel Accord have added to the responsibilities of financial institutions to adopt authentication methods such as biometrics (Khan and Zhang, 2007). It is unclear at this point if non-consumer driven demand for biometrics, such as legislative guidelines, will be enough to persuade the CU industry to adopt consumer oriented biometrics on a large scale.

EMERGING TRENDS, APPLICATIONS and LIVE APPLICATIONS

One example of a live consumer oriented biometrics solution in CUs is at Forum Credit Union. Forum Credit Union is a $1 billion financial institution located in Indiana. They implemented a system of keystroke rhythm authentication to grant access to Internet banking. Keystroke rhythm authentication matches the keystroke speed and cadence for each user. The system uses a method of ‘dwell time,’ defined as the amount of time between key-down and key-up. The other metric is ‘flight time,’ defined as the amount of time between key-down and the next key-down. In this application, the Internet banking security system will decline access, even with correct user name and password, if the timing is not correct (Bartholomew, 2008).

Keystroke rhythm authentication has some flaws. Broken or damaged hands change the speed of keystroke entry. Other factors that can change the typing pace are alcohol consumption, drug use and fatigue (Bartholomew, 2008). Additionally, the speed and cadence are not believed to be unique to each individual, but are sufficient in providing a positive identity match to a user. This software system develops an identifier based upon these quantifiable measurements. The baseline data used for verification evolves as the user's behaviors change over time (Jain et al, 2008).

The CU reports that only two to three percent of its online banking members adopted the technology. The newness and confusion of the system caused many members to decline enrollment. A technology manager would have a difficult time gaining support for a security solution that reported this low voluntary adoption rate.

NCR Corporation developed, and is now testing, a form of voice recognition to be used at the ATM level. First, the consumer records a voice pattern within the NCR system by responding to a series of questions. Next, the consumer would type their phone number into the ATM. The software system would call the user to confirm identification. The system seeks to leverage the wide acceptance of cell phone usage in the marketplace (Wolfe, 2008). Debit cards can be easily lost or stolen. There is a value added benefit to a consumer to only keep up with a cell phone. The traditional problem with debit cards is that they are shared with family members and friends. Current laws allow a person to be reimbursed by the financial institution for fraudulent debit card transactions. The current structures of the laws put the financial responsibility of the transaction on the financial institutions.

Michael Barta of Smart Business Advisory and Consulting states that voice recognition is not a preferred method of biometrics due to the extremely high error rate as compared to other biometrics methods (Rodier, 2008). A major disadvantage of voice authentication is that background noise can interfere with authentication. A car radio, children playing, or engine noise could alter the accuracy. This system is also reliant on pre-recorded answers. The user must recall the correct answer to match the voice pattern. More sophisticated voice authentication systems use, 'text independent voice recognition.' This is defined as a system that recognizes the user not based upon specific phrases. However, text independent voice recognition systems are exponentially more difficult to successfully manage (Jain et al, 2008).

Three dimensional facial recognition with analytic capability is gaining worldwide acceptance at the travel level and for border security. Facial recognition is less apparent to the user and requires less cooperation. Distant cameras can take a picture and verify identity while the subject is moving. The ability to capture a facial profile from a distance, in a crowded background and while the individual is moving differs from older technologies. In the past, facial recognition was limited to still shots with a monochrome or specially illuminated background much like a police mug shot (Jain et al, 2008). The false positive rate is lower than other forms of biometrics solutions. Identities can be confirmed in motion, thereby allowing a user to remain unhindered. These systems also use computer based analytics to measure a person's temperament. The system looks for signs of stress in various environments (Gluckman, Mar 2007).

The combination of biometrics and analytics is seen in another form of emerging biometrics applications, speech with analytics. Call centers in various industries are implementing this type of technology. Call centers are also used heavily in the CU industry. The biometrics system not only positively identifies the person on the call, but the system will also judge the emotion of the caller. Factors included in the emotion analysis are: pitch, rhythm, tonality and cadence. The application also looks for keyword usage in the many words spoken by a member and the software attempts to predict the meaning of a call. A practical example is that an identified angry member could be automatically routed to a manager or skilled problem resolution person. The angry member could be defused with a direct connection to a higher level decision maker. NICE, a provider of speech with analytics capabilities saw a $100 million jump in revenues in 2007. The company attributed the jump directly to the capability to analyze emotions (Chavis, 2008). CUs might be more willing to spend technology dollars if there is a sales enhancement capability coupled with the security measures of biometrics.

BIOMETRICS for CREDIT UNIONS

The Credit Union Economic Environment

It is important to understand the current economic environment faced by CUs. The available amount of funds from the bottom line relates directly to the available resources that can be applied to a biometrics solution. The economic environment from 2007 to 2009 generally had a negative tone. CUs found themselves struggling, as did most of the financial industry. There are several quantifiable factors that demonstrate the poor environment. The Misery Index, defined as the combination of unemployment rates and inflation rates, was at levels not seen since the recession of the 1980s and the monthly unemployment rate, at 9.5% in January 2009, was expected to rise (Bureau of Labor & Statistics Website, 2009). Foreclosure filings reached a level of one in every 54 households in 2008. New housing starts fell by more than 300% from 2006 to 2009 and new automobile sales fell by 19% in 2008 compared to 2007. This was followed by a 19% decrease, year to date, in 2009. The stock market lost over 50% of its value in less than two years, and nearly 40% of consumers had an interest in the stock market (Raddon Financial Group, 2009). The Gross Domestic Product was negative for four straight quarters as of the 2nd quarter 2009 (Commerce Department Website, 2009). Personal Net Worth declined by 18% in 2008, mainly attributable to the decline in real estate and investment portfolios (Bureau of Economic Analysis Website, 2009).

CUs were especially hard hit with loan losses (Raddon Financial Group, 2009). Loan losses from auto and mortgage loans represent one of the greatest risks to CUs. There was pressure to tighten lending practices which directly creates a loss of interest income to CUs. The result was shrinking bottom lines.

As a result of such an unfavorable economic climate, CUs, like other financial institutions, tightened budgets and discretionary purchases (Johnson, 2009). Non-essential items, plans for growth, and new hiring were generally scaled back. Innovative technologies, such as consumer oriented biometrics, without a proven track record of success and a measurable return on investment, stood little chance of funding.

Available Funding for Biometrics Initiatives

The amount of available funding for biometrics solutions appears to be minimal. Callahan and Associates put together a 2008 survey of technology spending specific to the CU industry. The survey was comprised of 205 CUs representing $124 billion in assets. This sample group represented 17% of the CU industry's assets in 2007. The average assets size of the sample was $606 million. The CU asset size ranged from $6 million to $15 billion. The average budgetary plans for technology averaged $300 thousand. The average technology budget represents 10% of total operating expenses (Johnson, 2009).

The good news is that 68% of these CUs reported an increased budget for technology in 2008 relative to 2007. But, the devastating reality for biometrics is that the solution does not appear anywhere near the top of the list for CU planning. The top seven channels where CUs plan to spend more money include the following: Mobile Banking – SMS/text messaging, Mobile Banking – Software Download, Live Chat, Customer Relationship Management Systems, Mobile Banking – WAP / Mobile Browsing, and Online Deposit Entry and Video Conferencing. The top seven channels where CUs intend to pull back funding include the following: Business Continuity – Backup Operations, Website Redesign, Layered Security Infrastructure Installations, Online Multi-Factor Authentication (which includes consumer oriented biometrics), Internet Home Banking, Outsourced Firewall Monitoring and Penetration Testing (Johnson, 2009). One should note that, if anything, biometrics appears to be in the category of reduced funding. Biometrics appears to have little traction or notice from CU decision makers.

In 2008, Credit Unions were divided into asset categories in the United States as follows: 72% of all CUs have less than 50 million in assets, 17% are between 50 million and 200 million, while the balance of only 11% are above 200 million in assets. 60% of all CUs report that they have no more than a single main office branch. Another 12% of all CUs have only one additional branch office (Johnson, 2009). The overwhelming majority of CUs are small, under $50 million in assets, have only one branch and therefore possess limited technology budgets.

Typically, one-half of CU technology budgets are spent on hardware and software. The balance includes salary and special projects such as biometrics. Another reputable survey was conducted by the Credit Union National Association and reported as the Technology and Spending Report. The purpose of this survey was to determine likely 2008 technology budgets specific to various types of technology. IT Security spending is estimated to be 6% of overall CU technology budgets for 2008. Biometrics is a small subset of IT Security spending. There is some indication that security dollars may increase over the next three years. When asked, CUs said that IT Security was the number one likely expenditure in the three year range. However, only one percent of the reporting CUs list biometrics as an increased item (Soltis et al, 2008). It is likely that biometrics expenditures are being pushed out due to the extreme competitive environment within which CUs exist. The emerging demands in mobile banking, compliance and a need to data-mine for cross-sale opportunities could be lessening the available resources for biometrics. Without a catalyst such as a firm regulatory requirement, it may be fair to assume that consumer oriented biometrics have no business drivers to increase demand by CUs.

CU Benefits of Consumer Oriented Biometrics

The benefits of consumer oriented biometrics are significant. The first is the positive and accurate identifications of individuals conducting financial transactions. Too often, CUs are not aware of the true identity of the person at the teller counter, ATM, or drive-thru lane (Jervings, 2006). The costs to the CU in conducting fraudulent transactions due to false identification include the loss of the transaction amount, reduced confidence by the membership and potential fines from the NCUA. Biometric identification can add a significant layer of protection to the overall process of identifying a customer.

Biometric security can be used in CUs' marketing campaigns to assure the membership of its strong commitment to financial security. Biometric security is an obscure concept to CUs' memberships (Jervings, 2006). With proper member education, the membership's perception could be altered to one of CUs being technologically advanced and secure. This might be a source of competitive advantage for CUs employing biometrics solutions.

Furthermore, biometrics can reduce the human bias involved in financial transactions. Humans have the tendency to make decisions based upon the physical appearance of the person conducting a financial transaction (Heet, 2007). Biometrics can assure the CU employee of the true financial position of the member, thereby lessening the bias. Where there is true automation of services, such as an automatic teller machine (ATM), the bias is totally removed.

There is a significant portion of the U.S. population that is classified as 'unbanked.' In late 2006, according to an EaringPoint and Visa study, there were 84 million people defined as 'underbanked' or 'unbanked.' The dollar value of the 'unbanked' represents $510 billion annually. These individuals have difficulty cashing checks, finding loans, or opening basic share draft accounts. Some of these individuals may have mental deficiencies, personal issues, or documentation problems that preclude them from joining a financial institution under the guidelines of the Patriot Act (Heet, 2007). A confirmed biometric identification measure on a national level may reduce the difficulties these people face in keeping up with and presenting identification documents. Once enrolled in such a system, the consumer does not have to bother with the process of showing identification documents.

An example of this type of system is found at AllTrust Networks formerly Phoenix Check Cashing, Inc. in Herndon, Va. Over 5 million individuals signed up for the company's BioPay system. The system requires the user to consent to a photograph and two finger print scans. Once part of the system, the users are allowed to engage in routine financial transactions like check cashing and cashier's check ordering. This consumer oriented biometrics system clearly has helped to reach the 'unbanked' (PRLeap.com, 2009).

Consumer facing biometrics systems also are attractive because the user carries the authentication method on their person. Unlike debit cards and pin numbers that are lost, stolen or shared with unscrupulous family members, physical characteristics remain attached to the customer. This lessens the likelihood of financial loss to the CU (Rodier, 2007).

CU Challenges for Consumer Oriented Biometrics

Credit Unions face many challenges in the implementation and successful adoption of customer oriented biometrics. The first challenge is the lack of technical expertise found within many CUs. There are typically small and limited information technology departments at CUs. In fact, a majority of CU technology departments are comprised of a single employee. The complexities of implementing a sophisticated biometrics solution may be beyond the technological abilities of the staff. The typical CU technology staff is overwhelmed by the level of systems and support needs found in their existing environment (Neil, 2009). CU management may decline to add technology professionals to manage a new biometrics system.

Some types of biometrics require a member to use a home fingerprint scanner (Anil, 2006). Once the fingerprint scan is authenticated, the member can conduct transactions. CUs lack the staffing to support the natural volume of calls that are generated from defective equipment and operator error. CUs cannot practically travel to individual homes for repair. Additionally, the cost of supplying individual scanning stations cannot be justified at an account level basis.

As previously noted, Credit Unions typically have a limited field of membership. Membership to a CU can be restricted to a place of business, type of occupation, or small geographical region. CUs currently are not able to take advantage of economies of scale derived from a large membership base. A small membership base means that the average technology dollar spent would be higher per member, as compared to a large bank.

Member foot traffic has declined within CU lobbies. Generation X and Generation Y both indicate a lessening of visits to financial institutions (Raddon Financial Group, 2009). There are inherent problems with distributing biometric devices outside of the traditional brick and mortar. The cost of distribution and maintenance make this concept impractical for CUs. The problem for biometrics providers becomes how to effectively market a product designed to mitigate a risk in a declining usage environment.

There is currently no centralized shared database available to CUs for positive identification. A CU may match forms of identification such as government issued documents, driver's licenses, or paystubs to a person's fingerprints. But, there is no secondary system for cross referencing the biometric data. There are similar national databases such as the following: credit scoring, Check Systems, and criminal records that offer background data on a national level. There is no comparable system in place for biometric data. Estimates are that it would take at least one decade to effectively change the nation's infrastructure to realize large improvement from shared biometric databases (Gluckman, Feb 2007).

CUs typically have an older average age of members than do banks (Raddon Financial Group, 2009). The average age of a CU member is 49, whereas the average age of a bank member is 45. Whether this is a significant difference or not, the fact remains that an older consumer may be less likely to be accepting of a biometrics solution. CUs potentially face a harsh backlash from their membership if biometrics are implemented as a requirement to normal transactions. A system that causes a loss of membership is less likely to be implemented by a board of directors unless there is a regulatory requirement.

Biometrics has limited effectiveness on the major potential sources of loss to CUs. CUs face a tremendous amount of risk, according to CUNA Mutual Insurance Group, caused by the following factors: loan loss, rogue employees and by remote criminals. For example, a rogue employee can quickly transmit hundreds of thousands of dollars to a foreign account electronically. A misguided employee could sell hundreds of confidential account listings to a European trafficker of information. The cost to repair the data loss and damaged reputation is exceedingly high. A hacker may penetrate the CUs financial database. However, the dominate risk factor faced by CUs is their allowance for loan loss due to bad lending practices. Allowance for loan loss represents one of the largest losses for CUs. The relative loss at the teller line or ATM is small. Biometrics provides no real defense against the most damaging and costly forms of loss to a CU. Consequently, there is less support to implement a solution that does not address these sources of risk.

Biometrics systems currently do not integrate well with core financial software systems or customer relationship management systems. In fact, CUNA's listing of core software providers for CUs shows that none currently support biometrics integration. Biometrics are normally supported by a third party's system outside of the CU's basic transactional database. An additional software system increases the resources required by technology support and lessens the efficiency of transactional staff.

Credit Unions are not ready for, or equipped to deal with, privacy concerns that their membership will have from consumer facing biometrics (Rodier, 2008). The frontline staff does not have the technical and legal knowledge to deal with the questioned aspects of biometric files. They do not know how to respond to questions relating to the mechanics of storage and security of these files. The potential confusion is a deterrent to CUs. There is a pronounced psychological resistance to a potential loss of highly sensitive data.

CONCLUSIONS and A MODEL for EVALUATING the UTILITY of CONSUMER ORIENTED BIOMETRICS for CREDIT UNIONS

Based upon the current environmental operating conditions unique to CUs, coupled with the challenges and benefits of consumer oriented biometrics, it is possible to construct a model of the factors driving the adoption of biometrics solutions in the CU industry and the counteracting factors presenting significant challenges to that adoption. From that model, a listing of questions that should be asked by technology managers of CUs prior to investing in the technology can be derived. The model is presented in the appendix.

Questions to be Considered by CUs

First, is there a potential for a positive return on investment? It is vital to estimate the risk in terms of dollars that the biometrics solution will offset. Business managers would not spend $100,000 to protect against $10,000 in potential losses unless there are other measurable benefits to be realized. The same fundamental business logic must apply to technological spending.

Technology managers must look for consumer oriented biometrics that offer integration with their core sales systems. Biometrics must not only be a means of security, but also a means to develop sales opportunities. The added value of potential sales leads will help offset the cost of biometrics and enhance the likelihood of acceptance by upper management. This potential sales capability is found predominantly in facial recognition and voice analytics. Customer level biometrics must have analytical capabilities as previously discussed. The ability to accurately assess a customer's mood, tone of voice, or patterns of speech can positively affect sales opportunities. Sales will lead to funding and justification for biometrics initiates.

The level of involvement required by the consumer must be minimal for biometrics to be embraced. Users are emotionally resistant to intrusive forms of biometrics such as retinal scans and fingerprinting. The biometrics solution must be transparent to the consumer. The most effective form of this presently appears to be facial recognition.

Technology managers must factor in the speed of the biometrics solution aimed at consumers. Modern consumers move at a high rate of speed and demand their vendors to move in like manner. Systems that are slow to respond, or that cause a delay in the transactional process, will not be accepted.

The accuracy level of the biometrics solution must be near 100% for this to work in a financial environment. Consumers are typically more emotional when dealing with their personal finances. The results of denying or delaying access to funds that are rightfully theirs would be disastrous to the CU's image. There must be a backup plan for positive authentication in the event that the biometrics solution fails.

The system hardware reliability must be high. Modern consumers will not tolerate delayed access to money due to technological issues. Consumers can easily move to alternative sources of financial service providers. Technology managers must fully vet references of biometrics providers to determine the level of uptime.

Due to the small numbers of available technology staff found in CUs, the biometrics solution must be easy to support. CUs typically have less staffing resources. The result is that the technology workers have less time to fully master a system. If the biometrics solution is not intuitive and easy to support, there will be failure at the consumer contact point. Any technology implemented in a CU that has a small IT staff must have easy to learn training programs. In other words, the seller of consumer oriented biometrics must make it simple to learn (Jervings, 2006). Examples of easy to learn training methods include: short pod casts, webinars, short and concisely written technical documents, live chat channels, and remote control capabilities.

Summary of questions technology managers should ask when considering implementing a consumer oriented biometrics system:

1. Is the cost of the proposed system exceeded by the combination of tangible and intangible benefits to be gained by the CU?
2. Does the system offer a sales channel that shifts the nature of the software system from a cost center to a revenue center?
3. Does the system interfere with the smooth transactional process that might negatively impede the consumer's experience?
4. Is the speed of the biometrics system fast enough to keep up with the demands of a fast paced society?
5. What is the false rejection rate of the proposed system?
6. What is the stated up-time of the biometrics system? Can normal operations continue without the availability of that system?
7. What is the sophistication level of the biometrics system? Can both the staff and the membership easily embrace the nuances of the system?
8. What channels of training and support does the software provider offer to the technology team of the CU?

Final Thoughts and Future Directions

There are many failed consumer oriented biometrics initiatives to cite. The intriguing aspect that is commonly evident is the apparent disconnect between what consumers say they want and what they will actually embrace. One example will illustrate the significance of the problem. Marc Kilgore, Vice President of City & County Credit Union in Minnesota, states that their members, in surveys, overwhelmingly asked for a biometrics solution at the ATM level. The CU implemented a finger print solution. There was a severe backlash from their membership. Kilgore states that the members did not trust that their fingerprints were secure no matter what assurances the CU offered. The CU ended the biometrics solution. The cost to the CU was a $150,000 lost capital expenditure. The expenditure represented close to 10% of their 2007 net income (Fleming, 2007). Perhaps the lesson to be learned from this experience is that consumer acceptance of biometrics solutions may be more of a marketing and perception issue than a technological issue.

As for the administration of financial institutions themselves, most have adopted some form of biometrics for back office support (Khan and Zhang, 2007). However, Credit Unions do not follow the trends of most financial institutions. Credit Unions typically have far less total assets, available capital for business initiates and technical expertise than do the traditional large banks.

The existing adoption level of consumer oriented biometrics by CUs remains low. Many reasons for this have been explored in this research. The high cost of biometrics is a deterrent to CUs with low available funding. Small CU technology staffs make the implementation of new, sophisticated systems hard to accomplish. The loss risk that is dealt with by current consumer oriented biometrics applications is not significant enough for managers to spend technology dollars addressing it. Also, the lack of standards and a nationalized database for identity matches limits the effectiveness of current biometrics solutions. Finally, there are no present regulatory mandates that force CUs to adopt biometrics solutions for positive identification at the transactional level.

However, in the future, some of these situations may change. The International Organization for Standardization (ISO) is developing standards for the use of biometrics authentication and devices for the financial sector (International Standards Organization's Website, 2009). The standardization of devices and databases could help CUs leverage the potential advantages of biometrics. CUs could see more fully integrated systems with more richness of database in the future, thereby offsetting one of the challenges to biometrics implementations. Additionally, regulatory compliance could emerge as a primary factor to drive the adoption of biometrics solutions and move them from the back office to the consumer side of financial institutions.

Without catalysts such as firm regulatory requirements and industry standards, it may be fair to assume that consumer oriented biometrics lack sufficient business drivers to increase their use by CUs in the near future. On the other hand, if they so choose, or are required to do so, CUs possess the ability to implement technology quickly due to their relative small size and flattened managerial hierarchy structure. Business implementations such as biometrics solutions can be introduced at a high rate of speed. CU managers must continue to monitor developments of biometrics solutions applications both within and outside the financial sector for opportunities to take advantage of the technology, rather than just deal with it, if required.

REFERENCES

Anil, Jain K., Arun Ross, and Sharath Pankanti (2006). "Biometrics: A Tool for Information Security." *IEEE Transactions on Information Forensics and Security* 2nd ser. 1, 125-43.

Bartholomew, Doug (2008). "The Rhythm of Identity Management." *The Baseline* Feb., 38-40.

Biometric Progress (2008). *Point for Credit Union Research & Advice* 1 Jan., 3-3.

Bits & Bytes (2008). *Community Banker* 17.5, 54-54.

Bureau of Economic Analysis: Net Worth Summary (2009). http://www.bea.gov/histdata/NIyearAPFFiles.asp?docDir=Releases/GDP_and_PI/2002/Q2/Final_September-27-2002&year=2002&quarter=Q2 (Manual Calculation required).

Bureau of Labor Statistics: Monthly Unemployment Rate (2009). http://www.bls.gov/web/cpseea1.pdf

Busch, Christoph (2006). "Facing the Futures of Biometrics." *Science & Society* 7.Special, S23-25.

Chavis, Selena (2008). "The Fastest Growing Application in the Market and Why." *Credit Union Business* Jan., 38-42.

Commerce Department GDP (2009). Raw data. http://www.bea.gov/national/xls/gdpchg.xls

Fleming, Cathy (2007). "Biometrics Offers Security, Efficiency." *Credit Union Magazine* Mar., 100-01.

Gluckman, Geoffrey M. (2007). "Interview with an Expert." *Credit Union business* Feb., 42-46.

Gluckman, Geoffrey M. (2007). "When it comes to Security the Swiss Have a Secret." *Credit Union Business* Mar., 49-55.

Heet, LaRita M. (2007). "Reaching Out to the Unbanked Through Biometric Technology." *Credit Union Business* Mar., 54-57.

International Standards Organization Website (2009). http://www.iso.org/iso/catalogue_detail.htm?csnumber=50145#

Jain, Anil K., Karthik Nandakumar, and Abhishek Nagar (2008). "Biometric Template Security." *EURASIP Journal on Advances in Signal Processing* 579416th ser. 2008, 1-17.

Jervings, Jim (2006). *Biometric Trends and Practices*. Tech. CUNA Technology Council.

Johnson, Jay (2009). "Credit Union Technology budgeting and Spending Priorities in 2008." *The 2008 Technology Guide for Credit Unions* 2, 13-24.

Khan, Muhammad and Jiashu Zhang (2007). “An Intelligent Fingerprint – Biometric Image Scrambling Scheme.” *Research Group for Biometrics & Security Engineering* 4682, 1141-1151.

Neil, Bartlett (2009). *Drinking from a Firehose: running a Successful One-Person IT Department*. Tech. CUNA Technology Council.

PRLeap.com (2009). "Enhanced Velocity & Check Verification Tools from AllTrust Networks Improve Check Cashing Risk Management." http://www.prleap.com/pr/142207/

Raddon Financial Group / CEO Strategies Group (2009). *A Review of Critical Drivers of Credit Union Performance*. Rep. 2009 ed. Vol. Spring. Presentation attached to email.

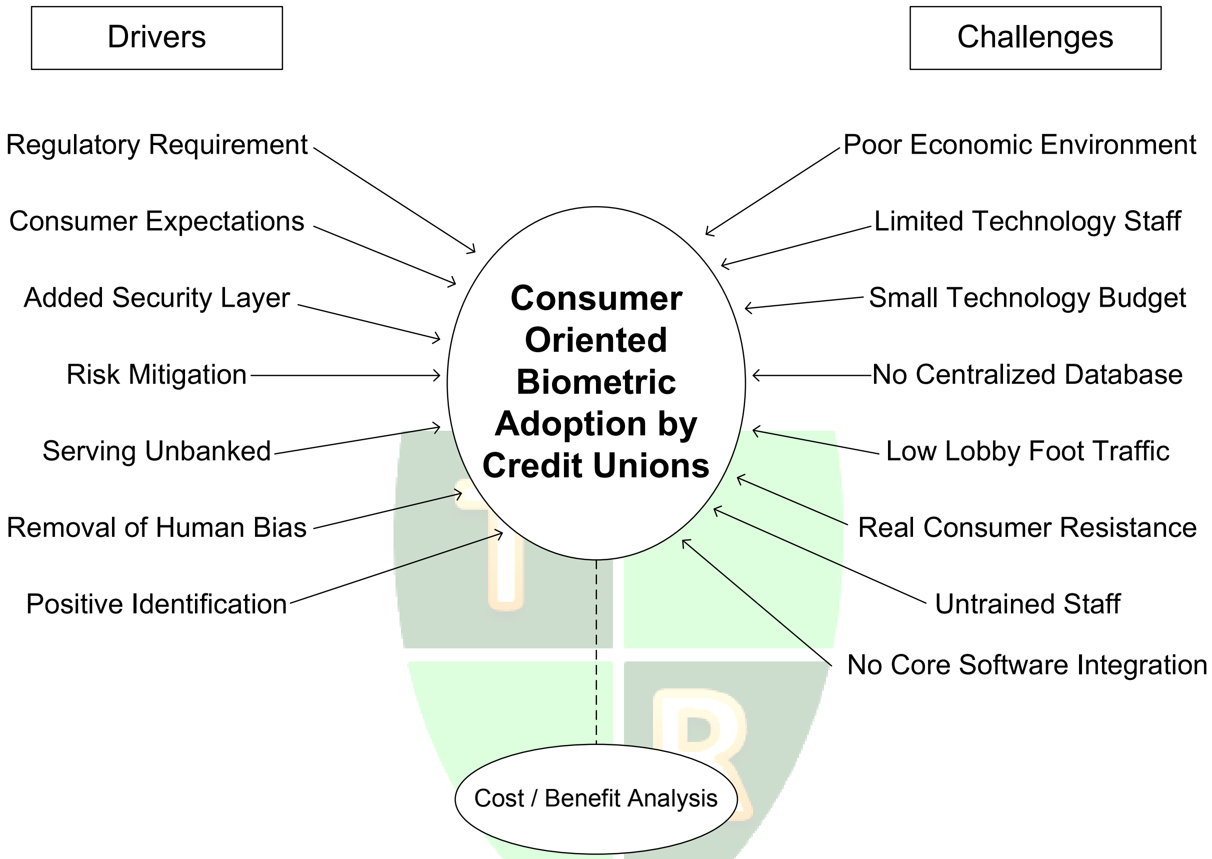
Rodier, Melanie (2008). "Financial Institutions Evaluate Biometrics." *Credit Union Journal* 18 Apr. 50-54.

Soltis, Beth, Kristina Grebener, and Tom Dunn (2008). *Technology and Spending Report*. Rep. CUNA's Center for Research & Advise.

Wolfe, Daniel (2008). "NCR to Test Voice System for ATM User Authentication." *American Banker* 173.125, 13-13.

APPENDIX

Model



Drivers and Challenges Model