Marketing Strategy

BioBanking Financial Transaction Security System

Watson MegaTech Inc.

*Chad Watson President and CEO*

# Target Market

BioBanking is a revolutionary approach to minimize fraud and identity theft that affects consumers and companies alike. Financial crimes are at epidemic proportions and many organizations must come together to put an end to this heinous invasion of the financial markets.

There are many points of invasion of the financial system. Many of these invasion points involve activity by individuals. It is this human vulnerability that BioBanking seeks to influence and stop. Many things like identity theft, money laundering, and terrorism funding can be significantly reduced with implementation of the BioBanking technology and long-term implementation strategy.

## Identity Theft and Fraud Epidemic

Identity theft has been the number one reported consumer crime over the last five years according to the Center for Identity Management and Information Protection (CIMIP). The CIMIP uses data from the Federal Trade Commission (FTC) Consumer Sentinel Network (CSN) to track cases of identity theft among the many consumer complaints. Figure 1 shows the total identity theft and consumer fraud complaints reported over the last five years.

|  |  |  |
| --- | --- | --- |
| **Federal Trade Commission** | | |
| **Consumer Sentinel Network Data Book Report** | | |
| **Year** | **Fraud and Identity theft Complaints** | **Identity Theft Complaints** |
| 2006 | 670,000 | 241,200 |
| 2007 | 800,000 | 256,000 |
| 2008 | 1,200,000 | 312,000 |
| 2009 | 1,300,000 | 273,000 |
| 2010 | 1,300,000 | 247,000 |

**Figure 1: FTC CSN Reported Identity Theft**

Out of this total number of complaints a large percentage relate directly to bank cards, consumer loans, and government document/benefits fraud. All of these are financial crimes and cost consumers or company’s money.

Another key area of fraud involving individuals is money laundering. This includes both the organized crime element and for terrorist activities. In money laundering cases there is usually an individual or group of individuals completing legitimate transactions of ill-gotten money. To combat this transactions must be controlled and accounted for at the individual level. (Gordon & Wilcox, 2003)

## BioBanking in the Financial Sector

Control of financial transactions at the individual level is where a technology like BioBanking can really make an impact. The use of individually coded biometric devices to authenticate, audit, and complete financial transactions will greatly reduce the ability of unscrupulous individuals to perform acts of financial fraud.

The greatest benefit will be to financial institutions that are left with the loss in most cases of fraud of any form. Data suggests that fraudulent financial activities cost financial institutions more than $48 billion per year. This is a substantial amount and well worth investing in new technologies to prevent.

## BioBanking for Individual Protection

The second main target market for BioBanking is the individual. Having an identity stolen can be devastating and cause complete upheaval in a person’s life. Getting all their identification papers changed, their accounts closed and reopened, and clearing up their credit reports can take months or years. There are three main types of identity fraud/theft against and individual:

* **Identity Theft** involves the theft of another person’s personal information specifically for establishing an identity for criminal activity or financial gain.
* **Account Takeover** occurs when a fraudster obtains an individual's personal information (account number and social security number), and then uses that information to change that individual's mailing address with the financial institution. Once this is accomplished, the fraudster can perform transactions without the victim's knowledge.
* **Transaction Fraud** includes schemes that may or may not utilize identity fraud. Examples include: Credit Card Fraud, as when someone uses a credit card account without the intention to pay the bills incurred; Check Fraud, which describes various activities such as check kiting, counterfeiting, forgery and writing checks on closed accounts (paperhanging). (Yaeger, 2005)

All of these activities can be combatted with the use of the BioBanking technology. The combination of both biometric authentication and encoded account information make each of these individual fraud mechanisms obsolete.

# Technology Overview

BioBanking is not a singular technology but is a combination of three key components that can initially overlay the current financial transaction network. The three major components of BioBanking are the Insert, the Active Reader, and the Device Encoder. The insert is the part of the system that represents the greatest technological leap forward in security authentication mechanisms. The reader and encoder are modifications to existing technologies to try and account for some industry disruption with the new paradigm.

The patented BioBanking Insert is the heart of the system. This is a 50 mm x 50 mm device that is implanted in the sub-cutaneous area of the finger roughly in the center of the finger print. Figure 2 shows the enlarged view of the product and the associated structures in this nano-scale device.



**Figure 2: BioBanking Patented Insert Device**

The insert has both transmit and receive radio frequency (RF) arrays to perform system actions. These arrays are powered by solar power. This is done to eliminate the need for battery replacement in the device so it is a long-term stable and viable insert. The solar technology used is similar to the Eco-Drive patented technology used in watches. The Insert also has on-board processors and memory for account information and control of the RF transmit and receive. Lastly, the device has ambient temperature sensors to ensure the device transitions to shut down if the user’s finger is severed. The ambient temperature sensors are another layer in the defense in depth security offered by BioBanking.

The second major part of the technology is an active RF interrogation fingerprint reader. This device both reads the swirls and points of the fingerprint as well as reads the RF transmission from the Insert device. The Interrogator allows the opportunity to select active accounts as well as mix accounts, both credit and debit, for payment.



**Figure 3: BioBanking Active Interrogator**

The last major component of the system is the Account Encoder. This device allows banks or financial institutions to transmit RF signals with account information encoded on them. This account information is then encoded in the memory of the Insert device like firmware. Overwriting the account information for a new bank is easily accomplished with the appropriate security overwrite code.

A complete description of the technology is included in Attachment A: Technology Description.

# Financial Industry Transformation

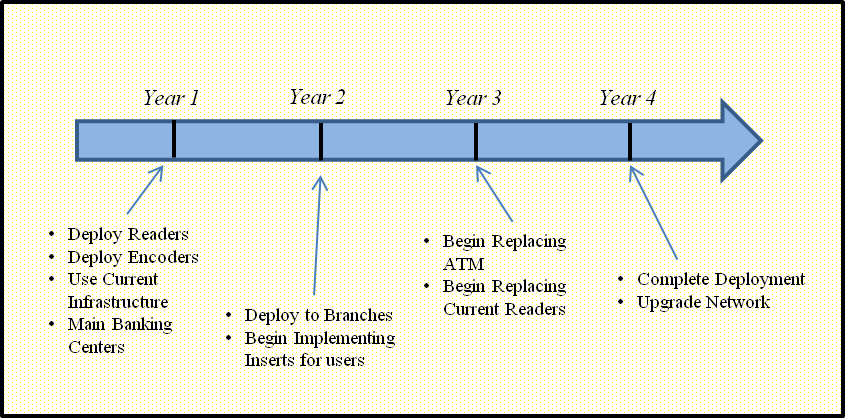
Currently almost all individual financial transactions use a card media and short passcode of some sort*.* Many now offer RF proximity swiping for ease of use. These technologies are convenient to the customer but are extremely convenient to the identity thief as well. Stealing a card and using it is very simple with the advent of online purchasing where the identity of the consumer is anonymous. The RF card material is often picked by a simple RF scanner waved over the user’s person without their knowledge. Since there are no other authentication mechanisms, the card information is now free to use for the identity thief.

These technologies are not convenient to financial institutions. The banks have to manage the issue and revocation of cards, manage the personal identification numbers (PIN), and re-issue stolen or lost cards. This is a huge overhead burden considering the number of cards issues in the US. The total numbers of cards issued in the US through the end of 2010 are:

* American Express credit: 48.9 million
* MasterCard credit: 171 million
* MasterCard debit: 123 million
* Visa credit: 269 million, as of Sept. 30, 2010
* Visa debit: 397 million, as of Sept. 30, 2010

Each of these has the potential for identity theft or financial fraud. (Woolsley & Shulz, 2011) An added complexity is that these represent the major financial institutions. There are also many store cards and revolving debt cards that have the same archaic authentication mechanisms.

There is currently a huge financial infrastructure in place with current readers and automated teller machines (ATM). To migrate toward BioBanking for individual financial transactions will require an overlay that works with these technologies until they are phased out over time. Watson MegaTech has a plan for accomplishing this. Figure 4 shows the overall four year timeline to completely overhaul the individual transaction system.

****  
**Figure 4: Timeline for BioBanking Deployment**

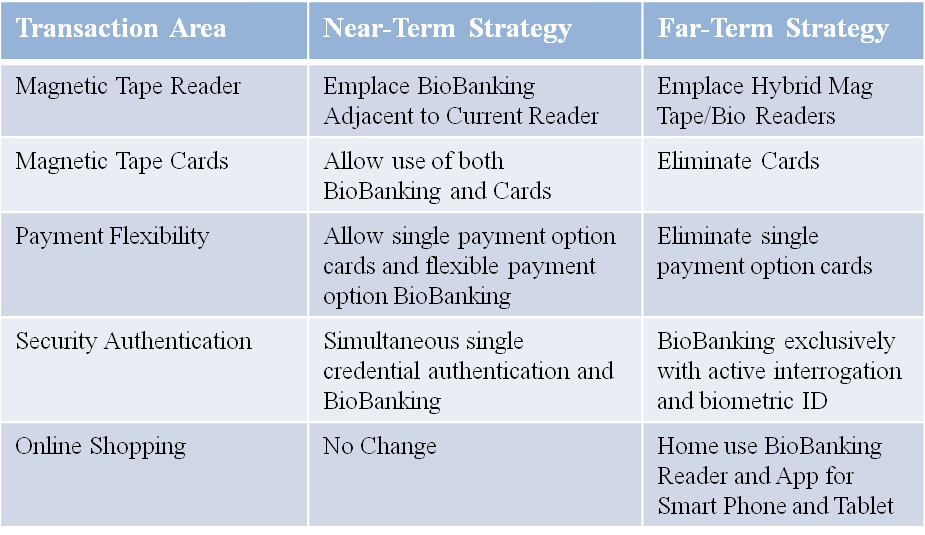
* **Year One** requires the deployment of the readers and encoders at major financial institutions. This will begin at the major financial centers and headquarters. First deployments will reside alongside the current card reader technology but will use the same network infrastructure.
* **Year Two** will begin the deployment of encoders and readers to financial institution branches and to point of sale locations. This will use the same paradigm as year one BioBanking technology will sit next to legacy card readers and use the same network infrastructure. Year two will also see the installation of the BioBanking Inserts into partner banking customers.
* **Year Three** of the deployment will see the ATM network replaced with hybrid card/BioBanking interrogators at all locations as well as beginning to replace point of sale technology with new hybrid BioBanking/card interrogators.
* **Year Four** sees the deployment complete through the US and installs a major network upgrade to raise the reliability of financial transactions and speed up traffic.

Since the financial network is global in nature and the United States attracts many visitors from all over the world, it will likely be impossible to completely replace card readers in the near future. The alternative is to deploy hybrid card readers that also serve as BioBanking point of sale interrogators. This is the technology targeted at the year three and year four efforts.

# Technology Disruption

By virtue of the technology and implementation there will be some current technologies that will be displaced. This is inevitable as innovation marches on and new paradigms are developed. Watson MegaTech is sensitive to the economic impact of the technology disruptions and has devised a strategy that will allow near-term harmony among all the technologies with a gradual phase-out of some current methods. Table 1 generally outlines the perceived technology disruptions and the near and far-term strategies for them.

**Table 1: Technology Disruption Efficiency Strategy**



* BioBanking will cause great upheaval in the current magnetic stripe card readers for point of sale devices and ATM. The single thread payment options and single method security contribute to their lack of utility and potential for identity theft. However, in the near-term BioBanking readers will reside adjacent to magnetic card readers then become integrated with them. Magnetic cards will become obsolete in the far-term and this industry will need to look at other markets.
* The deployment of BioBanking will also change the network protocols because of the mixed payment capability. The networks will have to be much faster because the consumer can use up to five different accounts to pay for an item. This requires balance checks and authorizations quickly. In the far-term single payment option cards will go away.
* Security will fundamentally change with BioBanking. For the short-term the single authentication cards will still be allowed on normal readers. In the far-term all financial transaction security must be active interrogation with biometric authentication.
* Lastly, the current methods for buying online will remain the same. However, Watson MegaTech has a design and plan to develop a home BioBanking receiver that will plug into the computer to offer the same level of protection for online as in-store shopping.

# US Patent and FDA Compliance Report

The BioBanking technology is the subject of a US patent offering seven years of competition protection or franchising rights. The Insert device is the subject of US Patent 9,998,473 since it is the most technologically complex part of the system. The patent was awarded December 15, 2009.

Since the BioBanking system relies on implanted devices and radio frequency, the US Food and Drug Administration (FDA) has strict governance over these type devices under Sections 531 through 542 of the Radiation Control for Health and Safety Act of 1968. Additional governance is located under 21 CFR 814 over clinical trials of the device and proof for three years that it has caused no human illness. Watson MegaTech applied for a US FDA Pre-Market Approval (PMA) to manufacture and distribute the BioBanking Insert device. PMA approval was granted under PMA P091462 on December 1, 2011.

Both of these documents are on file for reference as part of the technology development package.

# Long-Term Technology Plans

There are two major market segments that can be penetrated for significantly more growth in the BioBanking segment. These are the international market segment and the home network personal online shopping segment.

Since many US financial institutions do business around the globe and have reciprocal relationships with overseas banks, expansion into the global BioBanking market is a planned future endeavor. If magnetic cards are deleted from financial institutions in the US, there is still a problem with Americans traveling abroad where the technology is not available. Expansion into the global financial market will allow complete eradication of magnetic card banking and mostly terminate individual identity theft.

Many consumers are now buying online and the use a BioBanking for these type purchases will be prohibitive. To combat this the next easy growth step is to develop personal BioBanking readers for home use. These would be peripherals just like a printer and attach via something like Universal Serial Bus (USB) connection on the home computer. To maximize the utility, the most likely progression will be to develop an application for Smart Phones or Tablets so online purchases can be executed via a BioBanking Insert on the customer’s phone. This will represent a giant leap forward in utility for the product and will be a natural extension for very little capital investment.

The last area for long-term migration of this technology could be in the field of personal records. This could include all medical records and, in some cases, criminal records. The encoding in the device would allow interrogators on different frequencies to access the correct set of information. This could represent a huge potential market segment.

# Concluding Remarks

Identity theft and financial fraud are significant problems for individual and corporate entities. An Identity theft can destroy a person’s life very quickly and requires hundreds or thousands of hours to correct. Identity theft and non-payment of debt accounts can cost financial institutions billions of dollars. Combatting this requires a new approach and a new technology.

BioBanking is that new paradigm for financial transaction security. This is a patented and FDA approved technology that requires an unprecedented level of account and personal security authentication. Watson MegaTech has a sound strategy for fielding the system without disrupting the current paradigm. Lastly, Watson MegaTech has a solid roadmap for future development of the market.

We recommend that you strongly consider becoming a partner in this world-class venture to eradicate identity theft and individual financial fraud.

# References:

Gordon, G., & Wilcox, N. (2003). *Identity Fraud: A Critical National and Global Threat.* Utica, NY: Lexis Nexis and Utica College.

Woolsley, B., & Shulz, M. (2011, July). *Credit card statistics, industry facts, debt statistics* . Retrieved Feb 2012, from Credit Cards.com: http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php

Yaeger, C. (2005). *Identity Fraud – Impact for Financial Institutions.* Atlanta: Benchmark Consulting Inc.

**Attachments**:

Attachment A – BioBanking Technology Description