



# **Bewley Software Productions**

***Networking and Integrating Your Digital World***

Bewley Software Productions, LLC  
2600 East Seltice Way, Suite A, PMB 269  
Post Falls, Idaho 83854  
Phone: (623) 215-8531  
Toll-Free: (877) 897-9052  
Email: [CustomerService@bewleysoftware.com](mailto:CustomerService@bewleysoftware.com)

## **Multiple-Use Passport (Multi-Pass)**

### **Product Proposal**

Created: 7 March 2008  
Revision 1: 15 September 2008  
By: Eric J.V. Bewley  
Copyright © 2008



## **Multi-Pass Proposal**

### **Table of Contents**

1 Introduction.....	6
1.1 Information Security.....	6
1.2 Reductions In Consumed Resources.....	7
1.2.1 Reusing Existing Equipment.....	8
1.2.2 Maintaining Existing Equipment.....	8
1.2.3 Reducing Printed Resources.....	8
1.2.3.1 Multiple Forms of Identification.....	9
1.2.3.2 Forms of Membership & Association.....	9
1.3 Multi-Pass system Support .....	10
1.3.1 Individual & Organizational System Adoption.....	10
1.3.2 Government Adoption.....	11
2 General Multi-Pass Security Features.....	12
2.1 Passive vs Active Security Systems.....	12
2.2 Multi-Pass Card.....	13
2.2.1 Multi-Pass Card Appearance.....	13
2.2.2 User Configurable Security Constraints.....	14
2.2.2.1 Configurable Lock-Outs.....	14
2.2.2.2 General-Purpose PIN.....	15



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

**Multi-Pass Proposal**

2.2.2.3 Special-Use PINs.....16

2.2.2.4 Single-Use PINs.....17

2.2.2.5 Questions & Answers.....17

2.2.2.6 Automatic Age Restrictions.....18

2.2.3 Government-Imposed Restrictions.....18

2.2.4 Guardianship.....19

    2.2.4.1 Activity Monitoring.....20

    2.2.4.2 Change Requests.....20

    2.2.4.3 Secured Documents.....21

    2.2.4.4 Account Closures.....21

2.2.5 Securing Internet Transactions.....22

2.2.6 Financial Institutions.....22

    2.2.6.1 Transaction Monitoring & Notification.....22

    2.2.6.2 Transaction Validation.....23

    2.2.6.3 Account Status Monitoring.....25

    2.2.6.4 Notifications.....25

2.3 Restricting Information Exchange.....25

    2.3.1 Common Use of Personal Information Without Multi-Pass.....26

    2.3.2 Multi-Pass Identity Security.....27



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

**Multi-Pass Proposal**

2.3.2.1 Information Provided Via Request Mechanism.....28

    2.3.2.1.1 Organizational Demands Are Restricted.....28

    2.3.2.1.2 Individuals Remain In Control of Their Identity.....28

    2.3.2.1.3 Improved Data Accuracy.....29

2.3.2.2 Limited Organizational Data Stores.....30

    2.3.2.2.1 Basic Identity Information Only.....30

    2.3.2.2.2 Contacting Individuals.....30

2.3.2.3 Employer Data Stores.....30

    2.3.2.3.1 Reduction In On-Hand Documents.....31

    2.3.2.3.2 Proof of Identity.....31

    2.3.2.3.3 Payroll Information Transfers.....32

2.3.2.4 Preventing Misuse By Organizations.....33

    2.3.2.4.1 Pay-Per-Request Charges.....34

    2.3.2.4.2 Pay-Per-Transmission Charges.....34

    2.3.2.4.3 Publicly Accessible Do-Not-Contact Registers.....34

3 How Multi-Pass Differs From REAL ID.....36

    3.1 Reduces Publicly Visible Personal Identity Information.....36

    3.2 Provides Advanced Active Security Mechanisms.....36

    3.3 Gives Specific Guidelines To Follow In Protecting Data.....37



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

**Multi-Pass Proposal**

3.4 Includes Mechanisms To Prevent Corruption of Issuing Authority Personnel.....37

3.5 Provides Protection Against Known And Suspected Terrorists.....37

3.6 Does Not Reduce The Liberties And Privacy Citizens And Visitors Deserve.....37

3.7 Does Not Permit Unauthorized Tracking of Individuals.....38

3.8 Provides Security To Prevent Organizations From Openly Sharing Member Data.....39

3.9 Compliance Not Limited By Age, Residency Status Or Other Factors.....40

3.10 Does Not Permit Lax Validation Requirements Which Might Reduce Security.....40

3.11 Issuing Authorities Must Provide Authentication of Documents Issued.....41

3.12 Circular References of Non-Authenticated Data Does Not Lend False Credit.....41

3.13 Improves Security In A Cost-Effective Manner.....42

4 Estimated Fees & Rates.....43

4.1 Multi-Pass Member Individuals.....43

4.2 Multi-Pass Member Organizations.....45

4.3 Start-Up Costs & Basic Operating Characteristics.....47

5 Revisions.....49

5.1 Revision 1: 14 September 2008.....49

5.1.1 Correction to Estimated Launch Date.....49

5.1.2 Correction to State Start-Up Costs.....49

5.1.3 Clarification Concerning State Start-Up Costs.....49



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

## **1 Introduction**

The Multiple-Use Passport (Multi-Pass) system by Bewley Software Productions, LLC (BSP) has been designed to provide both individuals and organizations with a way of positively identifying other individuals and organizations. The system was originally designed to operate as a privately-owned system supporting either worldwide or regionalized user bases. Due to the growing concerns identified by the Department of Homeland Security (DHS), BSP is prepared to provide this product as a high-quality, low-cost solution which will initially apply to the US alone. Unlike other proposed ideas, Multi-Pass provides a managed solution which will stand firm against the attempts of counterfeiters.

This document describes only the initial release of a software package which will continue to mature over time. This first-phase package is already undergoing development and testing in preparation for a May 1, 2009 beta launch date. Since the system has been designed to support dynamic growth and refinement with absolutely no downtime, users will continue to see advancements in fraud detection, personal identity security, and useful everyday enhancements at no additional cost.

The Multi-Pass system as outlined in this document will contribute to a process which reduces government spending while simultaneously increasing the security of our nation's operations, the desired quality of life for all citizens and visitors, and most importantly, the security of personal identity information. The manner of operation will be easily understandable by all who participate in the associated programs through on-line access and public documentation. The functionality of the system will be automated in many respects while remaining fully customizable by each and every citizen or visitor.

### ***1.1 Information Security***

History has proven that no matter what technological ideas we may devise to try and secure printed media, counterfeiting artists will always find ways to overcome such controls in a short amount of time. This can be seen in the many ways that organizations have tried to secure computer software, passports, driver licenses, and the various forms of negotiable assets (checks, money orders, currency bills,



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

etc.). Often, it takes far less time to overcome the security features of printed media than it does to design and produce the features.

Instead of using tamper-resistant documents, Multi-Pass employs automated computerized management processes to ensure proper use of the unique Multi-Pass number assigned to each individual and organization. These processes are very similar to those in use by credit card processing companies like Visa™ and MasterCard™. Like most credit cards, Multi-Pass cards will not contain information on the face, rear, bar code, or magnetic strip which can be used to violate the security of the individual's account. This makes the card an item which can be produced via the existing card development systems in use by most government offices (departments of motor transportation, passport offices, etc.).

Most individuals today carry two or more instruments at all times which can be used to identify them with nearly positive accuracy, such as driver licenses, military and/or veteran identification cards, passports, organizational passes/badges, health cards, and banking cards. In addition to these, we carry various other forms of identification which include but are not limited to Social Security cards, insurance cards, donor and medical alert cards, business cards, credit cards, and club/organizational membership cards. Each of these articles could pose a threat to the security of our personal identity information if they were to make their way into the wrong hands. Use of the Multi-Pass card to replace each of these other cards will reduce the occurrences of identity theft and the large amount of government, organizational, and personal funds required to restore a person's fraudulently used identity.

## ***1.2 Reductions In Consumed Resources***

Consider the many forms of identification assigned to each and every citizen and visitor of the country. A vast amount of waste, as well as the use of natural and man-made resources, will be reduced through the use of the Multi-Pass system as designed by BSP. This directly contributes to a major reduction in the amount of funds which are used to produce, manage, track, and replace these identity instruments.



## **Multi-Pass Proposal**

### **1.2.1 Reusing Existing Equipment**

Any issuing authority which currently possesses card printing equipment will be able to continue using that equipment. In many cases, this will greatly reduce the amount of time and cost that issuing authorities fully incorporate into the Multi-Pass system.

The reduced consumption of resources is brought about by the design of the Multi-Pass system by BSP to support information and existing resource reusability. Each governing body which desires to create Multi-Pass cards bearing their own design will be able to do so as long as the instrument displays an unobstructed color photo of the individual which is at least two inches wide by two inches high. Since the Multi-Pass member's number is a publicly visible value, safe, and allowed for use within any third-party organizational database system, members will be able to log into their on-line account and print out a temporary card and/or order a replacement card. The validity of these temporary cards will be easily tested by others through the use of personal identification numbers (PINs), security questions, and/or the comparison of the Multi-Pass card photo to the one displayed on computerized register screens fully supporting the Multi-Pass system.

### **1.2.2 Maintaining Existing Equipment**

Card printing equipment can be costly to maintain. In the interest of fairness toward taxpayers, BSP recommends that a rule be put in place which limits issuing authorities to charging a maximum flat rate fee of \$10 to replace lost cards. At this rate, all issuing authorities should be able to adequately cover all costs associated with the printing and all necessary maintenance and/or replacement costs of card printing equipment. Such a rule should eliminate the need for issuing authorities to place a drain on taxpayer-funded budgets for the equipment. The suggested rate would also reduce the number of persons who lose their card and delay in replacing it due to insufficient funds.

### **1.2.3 Reducing Printed Resources**

Organizations can respond via other means, reducing tons of paper resources wasted each month. The Multi-Pass system will contribute largely to such a



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

## **Multi-Pass Proposal**

reduction in the way that it responds through POS keypads, email notifications, instant/text messaging, etc. This resource reduction will grow as other organizations begin utilizing the Multi-Pass or similar systems for electronic communication and validation.

### ***1.2.3.1 Multiple Forms of Identification***

The Multi-Pass number issued to each person is a uniquely identifying value which is safe to use for all forms of identification due to its actively managed security processes. Right away, individuals will be able to purge their wallets, purses, PDAs, etc. of other cards and numbers which do not identify them as securely as Multi-Pass.

Entities such as the motor vehicle departments, Social Security Administration, Veterans Administration, and the branches of military service are just a few which can switch to the use of the Multi-Pass identification system and discontinue printing identification cards which can easily be lost, stolen and/or counterfeited. The amount of savings by having these entities switch to the use of the Multi-Pass system will be very large.

### ***1.2.3.2 Forms of Membership & Association***

Like the savings and conservation of resources mentioned above in relation to identity, a potentially greater amount of conservation and savings can be achieved by organizations making use of the Multi-Pass number to identify membership.

Many citizens are enraged by the amount of information that organizations are maintaining about them without their knowledge, all in the name of "proof of identity". What makes matters worse is that much of this information identifies a person with enough accuracy for others to assume the identity as their own. The most basic reason that this is possible comes back to an attempt to indicate identity via unmanaged, passive, and insecure means.

The managed security of the Multi-Pass system makes it possible for any organization with a right to an individual's data to maintain a link to the data only via the Multi-Pass number and no other information. In later sections,



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

## Multi-Pass Proposal

we will describe the manner by which this public use of a Multi-Pass number is possible and permitted, yet keeps identities secure.

By allowing organizations of all types to make use of the Multi-Pass number, membership cards would be a thing of the past. To gain access or show membership/association credentials, a person needs only to present their Multi-Pass card, enter the correct PIN, satisfy any additional security constraints as they have set forth within their on-line account, and optionally (at the desire of the organization) have their appearance compared to that which is stored within the Multi-Pass system. No longer would a person be required to carry insurance cards, club membership cards, hotel key cards, etc. when they are in possession of a Multi-Pass card.

### **1.3 Multi-Pass system Support**

The Multi-Pass system has been designed with individual identity security placed as the key focus and cornerstone of operation. If the security of each individual is managed at the highest possible level, the strength of those security measures will combine together to form a naturally higher level of security within each participating organization. This is true whether speaking of business organizations, volunteer organizations, military branches, or any governing body.

#### **1.3.1 Individual & Organizational System Adoption**

Adoption of such a system will undoubtedly raise serious concerns with organizations and individuals alike in the beginning. Many individuals will be concerned about losing their individualism and privacy as supported by the Constitution. Organizations may be concerned that one or more government entities are trying to limit their customer and/or employee bases. Participants will need to be educated to understand that the limits imposed by this system as designed by BSP, will only serve to **secure** their identity and way of life through means and methods which have been founded and supported by law from the very beginning.

Through on-line Internet tools provided by BSP within the system, interested persons will be able to answer many of their questions concerning the system and how it relates to their constitutional rights, existing laws, and any new laws



## **Bewley Software Productions, LLC** *"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

put in place to strengthen the system. Our desire is to make text documents, audio files, and demonstrations available on a public basis. BSP is confident that the majority of all citizens and organizations alike will find the system to be a much needed service that is long overdue.

Though the Multi-Pass system may require additional laws and regulations to be adopted in order to ensure the security of data and compliance of system requirements by each individual, the system should not remove any existing rights or impose any new restrictions on the citizens of the nation. The system does have the potential to make law-breakers more visible, which in turn has great potential to improve our society by aiding personal liability and encouraging personal responsibility.

### **1.3.2 Government Adoption**

For such a system to operate at peak efficiency, complete and unified support of the program and its processes must be received at the highest levels. Allowing each state, county, or city to stipulate changes to the system will only serve to fracture the reliability of the data contained and severely degrade its usefulness and performance. Instead, a standardized basic level of participation in the system should be enforced via federal mandates. Likewise, the federal government should define clear classifications of violations and applicable sentencing terms for each.



## Multi-Pass Proposal

## 2 General Multi-Pass Security Features

The Multi-Pass system utilizes a managed approach to providing security. This is what is known as an active system rather than a passive system.

### ***2.1 Passive vs Active Security Systems***

Passive systems in today's world provide little to no protection to the user. They rely on the person to whom the identity instrument is issued to report both the information for the system and its misuse. The number of persons participating in criminal activity against a system with passive security often overwhelms those assigned to govern and enforce applicable laws and regulations. It is thought by many that most criminals participating in such activities are relying on the failures of the enforcement agencies involved with their crimes.

An example of a passive system which has grown too large to bring under control again quickly, is the Social Security program. Much like the Social Security cards are the State-issued driver's licenses, birth certificates and passports. Counterfeiters produce fraudulent Social Security cards daily. These cards are used by illegal immigrants to flood our workforce as well as to steal another individual's identity.

Since there are no active systems in place to accurately monitor the documents used by these passive programs, the problems associated with them have grown too large for our enforcement agencies to get them back under control. These problems can then lead and/or contribute to personal identity theft, in which the victim's life and good name are destroyed for a period of time, often resulting in the victim being the one responsible for the costs of identity restoration. The effects of these crimes are never erased completely (IE Zombie Debt), and often the criminal parties get away without justice ever being served.

In contrast to the passive system, active security systems, such as the one used by Multi-Pass and many credit card systems works to **prevent** the misuse of the cards and numbers. By working to prevent improper use of the Multi-Pass number which uniquely identifies a person, the problems related to fraudulent activity should never be allowed to get out of hand.



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

## **Multi-Pass Proposal**

Furthermore, if federal government agencies will agree to work with BSP to assist in maintaining the security of the system by allowing direct alert interfaces and establishing agreements to immediately apprehend and prosecute offenders, the Multi-Pass system is one which can last for a very long time.

### **2.2 Multi-Pass Card**

The proposed Multi-Pass card is very different from the majority of the identity cards in use today. No specialized technology is used to generate or secure the card, and if it is lost or stolen, no harm is done. The number on the card and the information pertaining to the owner of the card are all held in secure storage within the Multi-Pass system, and monitored closely. Producing such cards without costly tamper-proof features would save our government and taxpayers a large amount of money.

#### **2.2.1 Multi-Pass Card Appearance**

On the face of the card will be a 2 inch by 2 inch color photo of the owner, along with his/her name, approximate height and weight, natural color of eyes and hair, ethnicity, country of citizenship and 19-digit Multi-Pass number. On the reverse is a magnetic strip and a two-dimensional bar code image containing only the member's Multi-Pass number and checksum values (to ensure proper scanning). The remainder of the reverse side of the card is reserved for any text and/or logos which BSP, DHS and/or other government entities may wish to provide.

The limited amount of information visible from the face of the card is designed to make it harder for others to locate the residence of the individual who may wish to keep that information private.

The photo on the card is one of the key elements which others can use to help validate the card-holder's identity. Employers and organizations which feel the need to compare the card-holder's identity to a Multi-Pass system image will be able to view the current photo of the card-holder from the Multi-Pass data stores. BSP would like to encourage DHS and the federal government to pass appropriate laws/regulations which will require that all member photos meet the following criteria:



## **Bewley Software Productions, LLC** *"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

- Full-color photo capable of displaying a minimum of 16-bit color (a digital color palette consisting of 65,535 colors)
- Includes entire head and neck showing full frontal view of face
- All headdress and neckwear, to include hats, facial coverings, jewelry and scarfs be prohibited
- All eyewear which changes the natural color of the eyes, or hides facial features be prohibited, to include glasses with wide/thick frames such as sports wear
- No temporary facial paintings or hair colorings

We are aware that the visibility of the facial area is a very sensitive issue for some, particularly when religious freedom comes into play. The reason for the recommendation is that many facial recognition software packages require the visibility of the base of the ears and at least two inches above the eyebrows in order to produce near positive results. Additionally, if there is no manner by which authorities responding to identity theft complaints can make use of the Multi-Pass system to confirm or deny identity, we fear that a number of these persons may be falsely accused. This is, of course, a recommendation and not a requirement of the Multi-Pass system.

## **2.2.2 User Configurable Security Constraints**

### **2.2.2.1 Configurable Lock-Outs**

Certain categories of items have been identified by credit card companies and banking institutions as high-risk purchase categories. Whenever a thief steals a credit card or otherwise gains illegal access to a person's account, items within these categories are often the first to be purchased. These categories include, but are not limited to: computer equipment, sporting goods, alcohol, firearms, and rental cars. To aid in the reduction of fraudulent purchases in the event a thief obtains a member's Multi-Pass card and general-use personal identification number (PIN), the Multi-Pass system allows its members to lock the account against authorizing purchases of these and any other general type of purchase. The only way for a purchase of items within a locked out category to be authorized by the Multi-Pass



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

## **Multi-Pass Proposal**

system, is for the member to access their on-line account and either remove the lock-out restriction or add a single-use PIN value (see *Single-Use PINs*).

Lock-out configuration items also allow the member to specify how the system will react given certain conditions. For example, if the event the system detects/suspects fraudulent attempts to access a members account by trying multiple PINs, the member can choose how the system responds. Response options will include but not be limited to: temporary lock-outs for a specific length of time, permanent lock-out until all security questions can be answered, and whether or not the system responds with a lock-out message.

### **2.2.2.2 General-Purpose PIN**

Each membership will be issued a randomly-generated personal identification number (PIN) to use in further securing their card. When the card is issued to the member, the initial PIN will be displayed to them via the keypad at the issuing authority's location on the first swipe of the card. In the event that a member needs to be reminded of their PIN value, any issuing authority accessing the Multi-Pass system via a secured and audited connection will be able to instruct the system to display the PIN on the next pass of the card through their terminal's client-side keypad. Issuing authorities will be required to verify the photo of the member and card against that of the member in the system, before requesting that the system present the PIN to the member. At no other time will the system display the PIN, and no one but the member should ever know the value of the member's PIN.

Multi-Pass members will be allowed to change their PIN at will via their on-line account or via an issuing authority. Prior to doing so, the member must be able to provide the correct value of the current PIN and all security questions. Since the security questions are supposed to consist of personal information which others should not be able to discover about the member, this precaution makes it extremely difficult for a hacker to change a user's PIN. By default, general-purpose PINs do not expire, yet members are strongly encouraged to change them periodically to ensure security of the account. See the section on *Questions & Answers* for more information regarding this topic.



## **Bewley Software Productions, LLC** "Networking and Integrating Your Digital World"

### **Multi-Pass Proposal**

Each transaction a member makes/enters into with their Multi-Pass number via a terminal which is connected to the Multi-Pass system will require the entry of the general-use PIN. If the correct PIN is not entered, the Multi-Pass system will not authorize the transaction. After 3 consecutive unsuccessful attempts, the Multi-Pass system will lock the account from further activity in accordance with the member's personal configuration. (Please see the section on *Configurable Lock-Outs* for more information.)

#### **2.2.2.3 Special-Use PINs**

Special-use PINs are personal identification numbers assigned by the Multi-Pass member via their on-line account access for use in authorizing purchases of specific types and/or entry into specific areas. These PINs can **only** be set up and managed via the member's on-line account. This feature can be of great use by adding an additional level of security to one's account in the event that a hacker or identity thief is successful in obtaining a member's general use PIN and creates a fraudulent card whose photo is not examined for accuracy by a vendor.

A special-use PIN can be set up to instruct the Multi-Pass system to refuse the purchase of certain types of goods or services, such as sporting goods, alcoholic beverages, tobacco, firearms, fuel, etc., unless the member first enters a secondary PIN. For example, if the member feels that they may wish to purchase a firearm or ammunition at some time in the future, but would like to restrict these purchases by adding the requirement of a second PIN, they may do so and decrease the likelihood that their Multi-Pass account could be used by unlawful persons to try and purchase weapons by impersonating the legitimate member. This option differs from the configurable lock-out process (see *Configurable Lock-Outs*) which can be used to prevent these types of purchases altogether.

Special-use PINs may also be used to restrict the amount of a purchase for a given type of product. In such cases, the Multi-Pass system will require that the special-use PIN be entered successfully prior to indicating to the vendor that the purchase is to be allowed. An example would be a member who wishes to restrict the sale of sporting goods to a personal limit of \$20, allowing them to purchase small items such as tennis balls, while restricting the sale of larger items such as exercise equipment. Some banking



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

## **Multi-Pass Proposal**

institutions perform similar fraud prevention processes, but these processes typically are of a passive nature.

Finally, special-use PINs may be used on a per-organizational level to decrease the likelihood of fraudulent usage elsewhere by persons who attempt to capture and reuse PINs. Fraud detection systems will optionally watch the use of special-use PINs which are assigned in this manner, in order to provide early warning and enforcement of Multi-Pass security via automated alerts to local authorities.

### **2.2.2.4 Single-Use PINs**

Single-use PINs operate in the same fashion as the special-use PINs above, except that they can only be used once before expiring. The typical use of single-use PINs is to permit a single purchase of items which fall into a category which has been previously locked out. (See *Configurable Lock-Outs* for more information.). For example, a member may lock out their Multi-Pass card from authorizing the sale of sporting goods, in order to decrease the likelihood of such purchases in the event that their general PIN is discovered. They now decided to purchase an exercise bike, so rather than removing the lock-out on sporting goods and having to remember to reactivate it again after the purchase, they may enter a single-use PIN which they will enter during the time of their purchase. This functionality then prevents account access from being left unsecured on their account.

### **2.2.2.5 Questions & Answers**

Members of the Multi-Pass system may elect to increase the security of their Multi-Pass account by supplying up to 10 questions and answers which the system can use to ensure that the member is indeed the person using the account. Along with the questions and answers themselves, the member can indicate how many of the questions are asked at random in order to gain access, how many retries they are given to answer the questions correctly, and whether or not to alert authorities (local police, organizational/facility security personnel, etc.) in the event that the retry count has been exceeded.



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

## **Multi-Pass Proposal**

When in use, the member must first enter their general-use PIN, then successfully answer the number of randomly selected questions they indicated. All randomly chosen questions are asked before testing and reporting success or failure in authorization so that a person attempting to gain fraudulent access will not know to which question they provided an incorrect answer. Any incorrect answer will cause the Multi-Pass system to refuse authorization and in the event that three unsuccessful attempts are made, the system will alert authorities if that option is chosen.

### **2.2.2.6 Automatic Age Restrictions**

The Multi-Pass system will automatically reject purchase authorizations for goods and services which fall within categories that the federal government has restricted according to age. These groups include but are not limited to the purchase of alcohol, tobacco, firearms, pornography, access to adult clubs, restricted movies, etc. Since these restrictions are set by federal authorities, they cannot be overridden in any fashion. The restrictions are automatically removed on the birthday in which the member then falls within the acceptable age range for the goods and/or services. Whenever age restrictions are removed, the Multi-Pass system will automatically attempt to notify the member of the change in restrictions.

The use of Multi-Pass cards to gain access to restricted services and areas can greatly reduce the amount of liability to which a business is susceptible. For example, if a dance club serving alcoholic beverages makes use of the photo-comparison capabilities of the Multi-Pass system to permit or reject individuals, the liability they are under by not detecting the use of other fraudulent forms of identification is greatly reduced. This can contribute directly to a reduction in the amount of infractions of the law by minors, legal responsibility for serving minors, as well as lower insurance premiums for the business, just to name a few.

### **2.2.3 Government-Imposed Restrictions**

The Multi-Pass system natively supports government-imposed restrictions on members according to purchase categories. Government-imposed restrictions are specified as being temporary or permanent in nature. Those restrictions



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

## **Multi-Pass Proposal**

which are temporary in nature will carry a date in which the restriction is automatically lifted. An example of such a restriction might be the revocation of automobile operation licensing due to a charge of driving under the influence (DUI) of alcohol or other substances.

Enforcement authorities have unrestricted access to the automatic age restrictions and government-imposed restrictions which are applicable to a Multi-Pass member. For example, if a police officer pulls over an automobile driver due to excessive speed, they need only obtain the member's Multi-Pass card or number in order to view all restrictions placed upon the member, as well as their insurance coverage, permission to drive the vehicle, warrants, etc. Being able to obtain all of this information from a single source will greatly reduce the number of accidental releases caused by a lack of inter-agency collaboration.

The number of advancements between the use of technological equipment and the Multi-Pass system to reduce the likelihood of unlawful acts is limitless. The federal government may wish to require the use of such advancements to promote safety for the public as a whole. Consider the number of unlawful acts consisting of the use of an automobile may be prevented if automobile manufacturers begin making equipment available to require successful Multi-Pass authorization prior to use. Although some vehicle owners may not wish to incur the costs of such as system within their vehicle, or feel that it would be a burden upon them, those who agree to make use of such devices could be rewarded by lower insurance premiums. Rental car companies may wish to make such a system mandatory for their vehicles in order to lower fleet insurance premiums as well as the likelihood of vehicles being stolen or used beyond the limits of the associated contractual agreements.

### **2.2.4 Guardianship**

The Multi-Pass system is an identification system for all ages. Unlike other identification systems which apply only to a select group of individuals, the Multi-Pass system protects each person from birth until death. To facilitate this functionality for those persons who are unable to provide care for themselves, such as minors, the disabled and the elderly, a limited number of functions can be transferred to a guardian acting on behalf of the individual. This is known as guardianship access. Guardianship access can also be granted to individuals of



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

an organization such as the school officials of boarding schools, foster care providers, assisted living or nursing facility administrators, just to name a few.

Guardianship access allows the guardians assigned to an individual to perform one or more of the following functions as configured by the account owner or government authority:

**2.2.4.1 Activity Monitoring**

One of the strengths presented to guardians via guardian access is the ability to monitor the account activity of the person(s) to which they are granted guardianship rights. Many counterfeit documents make use of information from persons which are underage or deceased. The support provided to monitor the accounts of dependents placed under a guardian provides oversight to watch for activity which may be unacceptable for those under their care, as well as to alert authorities to fraudulent access or use of the members Multi-Pass account.

**2.2.4.2 Change Requests**

Guardians of a Multi-Pass account can be granted access to request permanent or temporary changes of postal addresses, residential addresses, email addresses, phone numbers, etc. Such access can be valuable for helping pre-authorized organizations locate individuals for the purpose of addressing mail.

Consider the following example: Jane is a six-year-old child who is going to be spending the summer months with her grandparents while her parents are out of the country temporarily. She has been diagnosed as having asthma, for which she has been prescribed the use of an inhaler. Just prior to her departure, her parents access the Multi-Pass system as her guardian and issue a temporary change of address to show her current residence address as being that of her grandparents. During the following day, the pharmacy in charge of filling and shipping the refills for Jane's inhaler prescriptions, prints out an address label to ship the prescription to Jane. Since the pharmacy has been granted access to Jane's address for this purpose, their system pulls the most recent address from the system and



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

prints that on the label. Rather than the prescription sitting in an inaccessible post box until the parents' return, the prescription is delivered to the grandparents' address in a seemingly automatic manner.

**2.2.4.3 Secured Documents**

Each Multi-Pass member can choose to have the system store documents and pre-filled form information in a secure and optionally encrypted manner to be accessed or transmitted to individually authorized parties at will. In the beginning, this storage space will only be provided to those members who purchase subscription-like access to their on-line Multi-Pass account and will limit the amount of storage space available to each member. As Multi-Pass storage space grows from the revenue received from these paid-member-access agreements, additional features will be made available which makes use of the secured document storage. One proposed feature which will draw upon this support is the secured electronic transmission of payroll information such as pay stubs, many of which are currently printed and mailed to last known employee addresses via unsecured means.

**2.2.4.4 Account Closures**

One of the most widely-used methods of gaining fraudulent access to another person's identity is through the use of accounts and memberships left open and unused. When a member's Multi-Pass number is used in association with account memberships, guardians can be granted access to close accounts which should no longer be used. Members can grant this access to guardians at will. When guardianship is awarded by a court of the United States, the court may also grant such access to the guardian(s) such as cases where the member is no longer fit or capable to willfully grant such access on their own.

When account closures are initiated through the Multi-Pass system, the information is transmitted through secure means and responses are stored for a period of no less than seven (7) years in order to provide creditable proof in the event that the accounts are used by others in a fraudulent manner.



## **Multi-Pass Proposal**

### **2.2.5 Securing Internet Transactions**

A large amount of the fraud which takes place against the identity of an individual, is facilitated by insufficient controls placed on Internet, telephone, and other remote ordering processes. By supporting processes which prevent a large amount of fraudulent actions within this area, the Multi-Pass system will deliver a strong first-strike blow to identity theft as a whole.

Beginning with the initial release of the Multi-Pass system, members will be able to quickly issue themselves single-use PINs for use in remote ordering processes which support Multi-Pass security. Members will be allowed to place an icon on their desktop which opens a very small window that communicates with the Multi-Pass system to issue the single-use pin. After the single-use PIN is used within the transaction, the Multi-Pass system immediately expires the PIN to prevent further use. Organizations and/or web sites which try to capture the PIN and reuse it in a fraudulent manner will trigger fraud detection systems which alert local authorities and/or result in higher per-transmission fees.

### **2.2.6 Financial Institutions**

Special consideration has been taken to design methods which will provide financial institutions with various standardized methods of communicating with the Multi-Pass system. These processes will not be available in the initial release of the application, but rather they are planned to be added at a later date.

#### ***2.2.6.1 Transaction Monitoring & Notification***

Most banking institutions provide their members with detailed transaction listings, yet in many cases, there is some difficulty involved with trying to decipher the cryptic codes associated with the transactions. For others, accounting issues such as typographical errors in transaction amounts go unnoticed until it is too late to correct the error and late charges or overdraft fees are incurred. Finally, there are transactions which occur fraudulently, which bring hardships on the account owner(s) and often result in a loss of funds for one or more parties involved.



## **Bewley Software Productions, LLC**

*"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

Many errors will be reduced by retailers integrating the use of the Multi-Pass system into their point-of-sale infrastructure. For those transactions which take place at a financial institution, it will be necessary for the organization to agree to report transactional data directly to the Multi-Pass system. Each transaction will pass through a series of validation systems which will grow in number and complexity as quickly as they are identified. The Multi-Pass system is not intended to operate as a financial institution in any way, but at the option of the member, may be used to securely store and electronically transmit encrypted financial information, such as credit card data, to support transactions.

Multi-Pass members making use of this monitoring system will be presented with an additional level of security on their accounts. Unlike the fraud prevention systems between financial organizations today, each member will be able to make use of all validation processes, no matter which institution they use, if the institution has agreed to make use of the Multi-Pass system.

In addition to the benefits each Multi-Pass member will received from this transaction monitoring service, the financial institution members will also be able to realize benefits to their own operation. By increasing transactional awareness and reducing software and hardware development costs, many institutions will immediately reduce their liability for certain types of services. For example, if XYZ Bank does not yet make use of a fraud detection system which watches for simultaneous debit card transactions at two distant locations, they may be able to make use of the Multi-Pass system to provide this service. Doing so, could result in saving the bank a large sum of money on software development costs as well as network hardware and fraud monitoring personnel. In some cases, the use of such a system may provide professional liability insurance companies with sufficient cause to apply a discount to the institution's policy, much like a good-driver discount of an automobile insurance company.

#### ***2.2.6.2 Transaction Validation***

Each transaction reported to the Multi-Pass system by registered financial institutions will be stored for a period of no less than 24 hours and immediately examined for validity. Transaction validity is determined according to the configurable rules which the member has put in place per



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

**Multi-Pass Proposal**

account. If the validations pass for a given transaction, a success value is returned to the sending institution, otherwise a data value is returned which indicates the general reason for validation failure and its severity. This transfer of information will take place across highly encrypted data channels.

By default, transaction validation and monitoring will be turned off. After these services are added to the Multi-Pass system, members who wish to make use of them will need to access their on-line account, determine which validation rules they want to put in place for each account, and provide values for those chosen rules which require user input. There will be no additional costs associated with many of the validation processes, as the cost of those processes are covered by the service fees paid by the financial institutions.

Validation rules will fall within two basic groups: simple and complex. Simple rules will be activated for an account by toggling a check box and saving the changes. An example of a simple validation rule is the option to prevent overdraft/over-limit transactions from occurring. When this option is checked, the Multi-Pass system instructs the organization processing the transactions to disallow the transaction from completing when insufficient funds exist, thereby preventing overdraft/over-limit transactions from occurring which might result in additional fees being charged to the member by the financial institution.

Complex validation rules are those which require additional definition by the member prior to activation. The activation of such a rule is toggled by the use of a check box much like that of simple validation rules, yet require the member to provide additional limit values before the rule can be made active within the system. An example of such a rule is the option of preventing transactions which take place outside of a specific region (IE. Zip Code, City, State or even a given Country). When this validation is chosen, the member must specify the region and radius (in miles or kilometers) for which transactions are to be allowed. Once activated, transactions for the indicated account which take place outside of the specified area will fail validation and should be refused by the organization or individual initiating the transaction.



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

**2.2.6.3 Account Status Monitoring**

Account status monitoring is a process by which financial institutions update the Multi-Pass system with basic account information such as opening balance, current balance, annual percentage rates, etc. This feature allows Multi-Pass members to view each of their accounts from one secured location.

**2.2.6.4 Notifications**

Transaction notifications are designed to keep Multi-Pass members in touch with the status of their accounts without needing to log into the Multi-Pass system. Some financial institutions provide similar services, while others do not support such features at all. BSP believes that being informed and forewarned is far better than being caught by surprise when it comes to financial matters.

Multi-Pass members can chose which notifications are sent to them in an account-specific manner. The style of the notification can also be set by the member to provide as much or as little information as they deem necessary. For example, let's say that you would like to be informed whenever your checking account reaches a low-balance threshold value of \$400. Within the Multi-Pass system, you would locate your checking account, and toggle the Low-Balance Threshold notification. The default message for the notification is as such: "The low-balance threshold of \$400 has been exceeded for account 'Personal Checking', which currently shows an available balance of \$240.62." Users who feel that it is a security risk to send so much information about the status may choose to change the message to read "Account 'Personal Checking' has exceeded its low-balance threshold!".

**2.3 Restricting Information Exchange**

In today's world, many organizations misuse personal identity information and contribute greatly to the threat of personal identity theft. Multi-Pass is designed to secure this information once again and restrict its use.



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

## **Multi-Pass Proposal**

By providing a number which is public in nature and uniquely identifying to the individual, there remains little to no reason for organizations to store and/or disseminate personal information. BSP would like to encourage law makers to support this endeavor by passing laws which makes the storage of personal identify information illegal without prior authorization from the Multi-Pass administration.

The next section will describe in detail why organizations should purge their data stores of personal identity information and how they should request and use this data in the future.

### **2.3.1 Common Use of Personal Information Without Multi-Pass**

Many organizations maintain personally identifiable information about individuals within their local data stores. Some of these organizations have never been granted permission by the individual to store this data. Others who have been granted permission to store the data were allowed to do so only after threatening to refuse services to the individual. A large number of these organizations do not secure their data stores in a manner which is sufficient to prevent hackers from accessing the data and stealing identities.

Consider a typical video rental store rental agreement. If a person wants to begin renting movies from the store, they often are required to fill out one or more forms to included their name(s), address, phone number(s), Social Security number and/or driver license number, among other various pieces of information. The store will often state that these values must be provided in order for them to prove the identity of the person desiring to rent movies and that failure to provide the information will prevent approval of the application.

The forms which the new member fills out are often handed to a part-time employee to enter into a computer system and then set aside. Typically, the individual has no idea where or how the information is used from that point forward or if the membership forms are disposed of in a secure manner. In some cases, the information is sent across unsecured data lines to a corporate office. Any one of the members, corporate office service personnel, and software and/or network management personnel can bring up this information at



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

## **Multi-Pass Proposal**

will. To make matters worse, many such systems display this information each time that the account is accessed to rent a movie to the customer and other customers are able to see the data. This happens more often than most people are aware.

Now consider another case which is true for most employers within the United States. Each person who wishes to work for an employer must present one or two forms of identification. The common articles are a Social Security card, driver license, and/or passport. Often, these articles are photocopied and kept on file for years after the employee has left the employer's organization. In many small organizations, these documents are stored in a sheet metal filing cabinet behind a wooden door and low-quality lock. Serious identity thieves are able to pick such locks and copy or steal these documents which go unnoticed until well after the thief is gone. These data stores are one-stop shops for persons who wish to generate and sell counterfeit documents.

Through the use of the Multi-Pass system as is outlined within this document, many of the misuses and theft of personal identity information can be prevented. The remainder of this section will describe in detail how the Multi-Pass system can be used to once again secure the identities of each and every individual.

### **2.3.2 Multi-Pass Identity Security**

The use of the Multi-Pass system will place control of personal identity information back into the hands of the person to whom it belongs – the individual. If organizations and individuals are bound by law to follow the requirements of the system, it is the firm belief of BSP that everyone will begin seeing a positive change in a very short amount of time.

Organizations will be required to remove all personal identity information from their data stores except for that information which they have been authorized to collect by Multi-Pass administration offices. Those organizations which fail to remove personal identity information from their data stores and fall prey to hackers should then be held accountable for the damages that information may cause.



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

**2.3.2.1 Information Provided Via Request Mechanism**

Whenever an organization is in need of information regarding an individual, a request is sent to the individual via the Multi-Pass system to approve the transfer of information.

**2.3.2.1.1 Organizational Demands Are Restricted**

The only information an organization will be allowed to require of an individual will be those pieces for which they have been previously approved for by the Multi-Pass administration. For example, organizations which do not file taxes or interface directly with the Social Security Administration will not be allowed to ask for an individual's Social Security number.

To establish which pieces of information an organization has access to, the organization will need to file an application with the Multi-Pass administration and state all uses for each piece of information it may request of an individual. If the request for information is unfounded or unreasonable, the Multi-Pass administration will refuse those portions and enter into an agreement for the remaining portions. To further aid individuals in understanding why specific pieces of information are required/requested, portions of the information provided in the organization's application will be stored for public viewing.

**2.3.2.1.2 Individuals Remain In Control of Their Identity**

Individuals will be able to research the requirements of an organization before they agree to transmit any information to the organization. If an individual wishes to establish a relationship with an organization, they will need to agree to the data exchange requirements of the organization as approved by the Multi-Pass administration. Organizations refusing to provide services to an individual based solely on that person's refusal to provide information in excess of that approved by the Multi-Pass administration can then be held responsible by having such unauthorized requests made known publicly to other users through currently



## **Bewley Software Productions, LLC** *"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

established Better Business Bureau reporting standards and through ratings on the business' Multi-Pass web page.

Return to the previous example of a video rental store membership. Instead of filling out paper forms which ask for too much information and filter through numerous hands, the customer can scan their Multi-Pass card and enter the general-use PIN. The merchant's system determines that they do not have the Multi-Pass number on file yet, so they ask to create a new membership. The keypad communicates with the Multi-Pass system to display the pieces of information that the merchant requires, and if the customer accepts, the information is transmitted instantly to the merchant's system via secure channels.

Since the process is completed without the need of membership forms, it can execute faster, more accurately, and without allowing others to view personal identity information.

#### **2.3.2.1.3 Improved Data Accuracy**

When data is shared between organizations and individuals via Multi-Pass, there is a tremendous improvement in data accuracy. First of all, the information is transmitted in encrypted form directly from data store to data store, so there is no need to read and key in the information. However, the greatest benefits come from the fact that the only information which needs to remain on-file is the Multi-Pass number.

Typically, the validity of entered data begins to diminish as time progresses, simple because it is hard to remember all the organizations with which a person has shared their information. The Multi-Pass system relieves the burden of updating organizational data stores by supporting on-demand information requests. A video store may only need to access your phone number once within a year, due to a late rental return. Rather than using a telephone number on-file which may be outdated, the merchant's system can request the information from the Multi-Pass system (if previously approved). Suddenly, the need to publish a change of address form or remembering to update personal accounts becomes unnecessary.



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

**2.3.2.2 Limited Organizational Data Stores**

Organizations will now be able to reduce the amount of data maintained about an individual by integrating the use of the Multi-Pass data stores into their local systems. This type of integration supports heightened security of everyone's personal data as well as an increase in the reliability of such data.

**2.3.2.2.1 Basic Identity Information Only**

Rather than storing names, addresses, phone numbers, tax identification numbers, driver license numbers, etc. in organizational data stores for hackers to break in and steal, only the very basic elements of a person's identity need be recorded. In most cases, this is the individual's Multi-Pass number, name and whether the values have been validated against the Multi-Pass system. These values are public in nature and insufficient for use in identity duplication. All other values are used and immediately discarded.

**2.3.2.2.2 Contacting Individuals**

Whenever an organization needs to contact a Multi-Pass member, whether it be via telephone, fax, email, or postal mail, a request is made for the individual's contact information, used immediately and then discarded. This request and transfer of information takes place electronically via secured transmission channels.

**2.3.2.3 Employer Data Stores**

Employer data stores will be restricted in much the same manner as standard organizational data stores. However, employers have needs which go beyond the standard proof of identity.



## **Bewley Software Productions, LLC**

*"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

#### **2.3.2.3.1 Reduction In On-Hand Documents**

In order to reduce the number of documents which are kept on-hand by employers, the Multi-Pass system will provide proof of identity and right-to-work information upon demand. BSP would like to encourage government agencies to relax the laws and/or regulations requiring employers to maintain physical copies of I-9 and W-4 forms and similar information. Instead, employers should be allowed to print out and file a numbered certificate from the Multi-Pass system which indicates the date, time and response concerning the right of the individual employee to work for the organization. These certificates should be renewed every three years for those employees who continue to work for the organization and expired certificates be discarded after a period of no less than seven years.

Right-to-work confirmation certificates contain no personal identity information about the Multi-Pass member except for their name, Multi-Pass number and the certificate number. The certificate number can be used by Multi-Pass and government enforcement agents to examine the validity of the certificate issued. Also contained on the face of the certificate is the name of the organization to which the certificate was issued, thereby preventing the sharing of documents.

#### **2.3.2.3.2 Proof of Identity**

Due to the number of counterfeit documents in circulation, driver licenses, passports and the like are no longer reliable enough to prove identity. The Multi-Pass system will be able to provide far more reliable identity confirmation for employees due to its managed nature.

Whenever a potential employee is considered for employment by an organization, a Human Resources (HR) agent for the organization sends a request to the Multi-Pass system for identity confirmation. The Multi-Pass system responds by asking the potential employee to scan their Multi-Pass card, enter their general PIN and satisfy any other security processes the member has added to their Multi-Pass account. Once the Multi-Pass system receives the correct security information, an electronic



## **Bewley Software Productions, LLC**

*"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

photo, physical characteristics, and right-to-work information is displayed to the HR agent to compare to the person before them.

If the photo and/or physical characteristics of an individual does not match the person in front of the HR agent, the agent can silently notify authorities via the Multi-Pass system to respond immediately. On the other hand, if the comparison is a match, the HR agent can choose to print a certificate of right-to-work examination to keep on file.

#### **2.3.2.3.3 Payroll Information Transfers**

One of the most common documents in existence today which is sent via unsecured channels from employers, is a person's payroll stub. This document often contains several pieces of personal identity information which many would prefer to keep secure, yet it is often delivered via postal mail carrier.

To reduce the likelihood of payroll stubs being intercepted by persons wishing to steal identities, the Multi-Pass system will provide employers with a way of transmitting the information directly to the employee's Multi-Pass account via secure channels. Employees who wish to print out and store the information may do so within thirty days of transmission. After thirty days, the payroll information is discarded from the Multi-Pass system data stores.

Another common document which is often delivered or transmitted via methods which are not secure are tax reporting documents such as 1099s and W-2s. The Multi-Pass system will also allow this information to be received and stored securely. Tax-related information will be maintained in a secured database for up to at least 8 years in order to facilitate the secure transmission and storage of such information.

Instead of transmitting images of documents for the above mentioned transfers, employers will transmit the information as encrypted data values. This manner of transmission reduces the data storage requirements of the Multi-Pass system, passing a savings on to all who use the system. This manner of transmission also allows the Multi-Pass system to perform data validations and reporting to its members. For



## **Bewley Software Productions, LLC** *"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

example, with each transmission of payroll data, the period values and the sums are examined against the previously reported information. If inconsistencies exist, both the employer and the user are informed of the error. The new document will be stored for auditing purposes. At the end of a tax reporting period, 1099 and W-2 forms are also validated against the stored values. This validation increases the reliability of data reported by employers to employees and the IRS.

#### ***2.3.2.4 Preventing Misuse By Organizations***

As the Multi-Pass system matures, several processes will be added in an effort to continually improve the reliability of the data contained within the Multi-Pass data stores and prevent its misuse. In the initial release, two primary processes will exist.

The first is the charges billed to organizations each time information is transmitted to or requested from the Multi-Pass system. Each organization will be required to fund their account in advance to support the costs of the actions requested of the system. If an organization's account does not contain sufficient funds for the transactions requested, the transactions will be refused with a return code which indicates the low or zero account balance. By handling the costs of transactions in this manner, no debts will be incurred which could break down the ability of the Multi-Pass system to support itself. BSP requests that all such fees be considered non-taxable by any and all agencies and be used as deemed reasonable by BSP to support the costs of the the Multi-Pass system software, hardware, licensing, management and expansion of data stores, and the payroll of BSP personnel assigned to the Multi-Pass system.

The second of the two initial processes used to prevent misuse of the information contained within the Multi-Pass data stores is the ability for Multi-Pass members to freely manage the global Do-Not-Call registers by simply toggling check boxes next to each method of contact.



## **Bewley Software Productions, LLC** "Networking and Integrating Your Digital World"

### **Multi-Pass Proposal**

#### **2.3.2.4.1 Pay-Per-Request Charges**

Each time an organization or individual requests information from the Multi-Pass system concerning personal identity information about another member, a fee must be paid. Organizations will be allowed to reduce the costs of such fees by paying in advance for request allowances. These fees are paid directly to BSP and used in the management and expansion of the Multi-Pass system, its data stores, and the employees supporting the system. (See the section titled *Estimated Fees & Rates* for more information).

#### **2.3.2.4.2 Pay-Per-Transmission Charges**

Each time an organization transmits data to a Multi-Pass member's account, a fee will be assessed. This fee applies for both successful and unsuccessful attempts to store data. Organizations will be charged fees according to the type of data transmitted. For example, financial institutions which are transmitting information to update the account balance of a member's account may be charged differently for that transmission than for transmissions of data involving payroll and tax information of an employee. (See the section titled *Estimated Fees & Rates* for more information).

#### **2.3.2.4.3 Publicly Accessible Do-Not-Contact Registers**

Multi-Pass members will be able to add their phone numbers, fax numbers, email addresses, and mailing addresses to Multi-Pass managed registers simply by adding these numbers and addresses to the system and selecting the available options to restrict them. Within the first release of the Multi-Pass system, three options are available: open, restricted and blocked. Additional categories of restricted statuses may be supported in future versions.

Contact information which is listed as "open", the default setting, will not be present within registers, and thereby allows unrestricted access to the number. Information which is listed as "restricted", can **only** be used to contact an individual if there is a preexisting relationship between both parties which was established in a willful manner by the individual.



## **Bewley Software Productions, LLC**

*"Networking and Integrating Your Digital World"*

### **Multi-Pass Proposal**

Restricted contact information is listed within registers with a flag to indicate the status of the restriction. Blocked contact information is listed within the registers with a value indicating its status, and no one should call or send mail to the location.

Inclusion in the publicly accessible registers provided by the Multi-Pass system is guaranteed to occur in less than 8 hours. Removal of a number or address from a register follows the same processes as adding a number.

BSP would like to encourage federal and/or state governments to establish laws which enforce the use of these registers by **all** organizations which desire to use one or more of the listed mediums to contact individuals or organizations. To support this enforcement, the register management system will annotate the member's account to show the date and time that registration of the address or number was completed. To encourage its use, access and use of the various Do-Not registers is free to all users.



## **Multi-Pass Proposal**

### **3 How Multi-Pass Differs From REAL ID**

The REAL ID Act of 2005 has caused major controversy since its beginning. There are many reasons why a REAL ID **should NOT** be your choice of national identification. In order to condense this proposal into an easy-to-read document, only basic descriptions of the differences will be disclosed. The web site supporting the Multi-Pass system at [www.MultiPassID.com](http://www.MultiPassID.com), will provide you with further information.

#### ***3.1 Reduces Publicly Visible Personal Identity Information***

The REAL ID card displays far too much personal identity information on its face and back, increasing the likelihood of identity theft. The Multi-Pass card displays only low- no-risk information on its face, keeping all other information secure behind the multiple layers of security the Multi-Pass system provides. Certain elements of data on the Multi-Pass card by default, can be removed at the member's discretion if they feel the elements reduce their personal privacy. Currently, the list of optional elements displayed are the member's gender, ID bar code, and ID magnetic strip.

#### ***3.2 Provides Advanced Active Security Mechanisms***

Unlike the REAL ID program, which does not make mention of sufficient security mechanisms to protect the identity of its members, the Multi-Pass system openly describes many of its mechanisms. In addition to describing these mechanisms, the Multi-Pass system web site will be expanded to give the reasons for the mechanisms and the options each member has at their disposal to tailor the processes to meet their own needs and restrictions.



## **Multi-Pass Proposal**

### ***3.3 Gives Specific Guidelines To Follow In Protecting Data***

The Multi-Pass system provides guidelines which individuals and organizations of all types must adhere to, and the reasons why they are in place. The REAL ID program does not appear to hold its members to clear guidelines, but rather relaxes the rules whenever the process may initially be considered a burden. The task of providing security is often a burden, but this does not excuse the need to enforce it.

### ***3.4 Includes Mechanisms To Prevent Corruption of Issuing Authority Personnel***

Many citizens and groups rightfully feel that the possible corruption of issuing authorities can lead to disastrous results – even to the point of destroying the REAL ID program as it is currently designed. The Multi-Pass system has built-in audit processes which reduce the likelihood of issuing authority corruption and increases personal accountability.

### ***3.5 Provides Protection Against Known And Suspected Terrorists***

In order to provide the maximum level of national security, the Multi-Pass system allows government agencies to identify those individuals who are either known terrorists or known to be in active support of terrorism against the nation. Through such support, national borders can be better protected by early warning systems. The REAL ID program does not seem to support any type of early warning systems such as this.

### ***3.6 Does Not Reduce The Liberties And Privacy Citizens And Visitors Deserve***

Many believe that the current design of the REAL ID program violates the securities, liberties, and rights of privacy which we and our forefathers have fought



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

so hard to obtain and protect. In direct contrast, the Multi-Pass system is built upon protecting individual personal identity information to the fullest extent possible, which will, in turn, work to once against secure and ensure the existence of individual rights. By securing the rights of each individual, the Multi-Pass system supports the same for the nation from the foundation on up.

In addition to the privacy and liberties which citizens feel they will lose via the REAL ID program, the cost of such a program outweighs its usefulness. A large amount of start-up costs will be required from each state/region which agrees to participate in the program, followed by the need for continual funding in order to support the processes and counter attempts of fraud. This can only lead to additional taxation which does not remain in line with the use of the individual.

On the other hand, the Multi-Pass system is designed to be self-sustaining without the continued funding from government budgets. Every person within our borders, as well as those desiring to enter our borders, can be assigned a Multi-Pass card without incurring any additional taxation. In its initial form, the card provides a minimal amount of security, yet members are allowed to pay monthly or discounted annual fees per person to manage their account and add additional levels of protection. Members will be allowed to activate and discontinue their on-line account access at will without losing the security applied to their ID card. This design should provide ample support for all Multi-Pass processes in a manner fair for all.

### ***3.7 Does Not Permit Unauthorized Tracking of Individuals***

The REAL ID program does appear to implement sufficient constraints on the data which can be collected by organizations and used to track the history, habits and whereabouts of the individual. This is a fault which should not be allowed due to the fact that it decreases personal privacy and increases the risk of personal identity theft.

The Multi-Pass system will not allow its transactions to be used in a manner to view the current or past actions of any member without either 1) the member voluntarily agreeing to the surveillance or 2) the requesting organization securing a court order in the form of a warrant for such information. In the interest of personal privacy and



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

## **Multi-Pass Proposal**

security, if such a warrant is obtained and not accompanied with an applicable gag order, the Multi-Pass system will attempt to inform the member of warrants placed against the individual/account(s) for which access is being granted.

According to the contract to which all organizations must agree and adhere, all transmissions requesting or transmitting personal identity information are required to be protected by a minimum of 40-bit encryption. Where easily obtained and not prohibited by law, a minimum of 128-bit encryption will be required. Currently, the Multi-Pass system is configured to support a maximum of 256-bit encryption.

Unlike the manner of transmission of standard credit card systems, which will authorize transactions through multiple levels of processing organizations, each adding an additional level of risk, the Multi-Pass system requires that all transmissions to/from the Multi-Pass system take place via direct communication from the originating organization or individual and the Multi-Pass system servers. Organizational entities, including but not limited to branch offices, child organizations, or those bearing a corporate and/or other legal registration (i.e. Limited-Liability Corporation), may not transmit or receive Multi-Pass transmissions via any other organization. This restriction allows the Multi-Pass system to accurately detect fraudulent activity, assess risk, and report violations against the proper entities.

### ***3.8 Provides Security To Prevent Organizations From Openly Sharing Member Data***

The REAL ID program does not describe in sufficient detail, any processes by which organizations will restrict and protect the data which it collects and/or maintains in its data stores. This presents an unreasonable number of vulnerabilities to individuals concerning their personal identity.

All organizations which apply for a Multi-Pass account and can provide sufficient proof of their organizational identity, will be issued an organizational Multi-Pass account. This business account will be used by the organization, in combination with the credentials of the individual employed by the organization, to request and submit data pertaining to personal and organizational identity. No legitimate organization will be refused a Multi-Pass.



## **Multi-Pass Proposal**

Multi-Pass members which have active access to the Multi-Pass system will be able to research the level of compliance of each organization with which they may desire to do business. Organizations which violate the acceptable use policies of the system, and/or are found to have been the source of lost or wrongfully shared personal identity information, will be identified so as to better inform active members of the level of risk to which they may be subjecting their identity when conducting business with that organization.

### ***3.9 Compliance Not Limited By Age, Residency Status Or Other Factors***

The REAL ID program provides individuals with lengthy time allowances to comply with program expectations and requirements. In some cases, persons of specific age groups are allowed to delay compliance for a period of up to ten (10) years. These lengthy allowances diminish the strength of the program and make it possible for terrorists to tailor their behavior in ways which will continue to go unnoticed.

The Multi-Pass system will require all individuals to comply with the minimum requirements of the system within a reasonable amount of time or be considered as providing adequate levels of suspicious behavior to warrant an investigation by authorities into the legality of their residency, employment, etc.

### ***3.10 Does Not Permit Lax Validation Requirements Which Might Reduce Security***

The Multi-Pass system does not permit organizations or government agencies to relax the validation of documents in order to reduce the burden of proof and cause the Multi-Pass system to falsely assume they are valid. In some cases, the Multi-Pass system will allow documented processes to lend credit to the validity of personal identity information, such as the initial permanent address of a member. However, these identity values will be marked as assumed information and may be considered fraudulent in nature if proof is later obtained which lends the Multi-Pass system to consider the information as false.



## **Multi-Pass Proposal**

### ***3.11 Issuing Authorities Must Provide Authentication of Documents Issued***

In conjunction with the REAL ID system, the Department of Homeland Security is described as permitting other agencies to forgo authenticating their documents or allowing less creditable documents/processes to be lent too much proof toward the validity of documents. One such case is that of the Social Security Administration which does not appear to be required to provide irrefutable proof of Social Security Number validity. Issuing authorities of REAL ID cards are permitted to validate a Social Security Number against a provided name and consider the ambiguous results as sufficient proof of authenticity and proof of identity. Forgers of documents are already aware of the vulnerabilities of this service and have been providing fraudulent documents which will pass these tests.

The Multi-Pass system will not consider such ambiguous processes as proof of authenticity nor proof of identity, but will use them to indicate sufficient cause to consider a supplied value as being fraudulent in nature.

For example, there may be one-hundred persons within the United States which are legally named "John Smith". This would then yield a positive result to a test of a minimum of one-hundred Social Security Numbers. Due to the ambiguity of the positive result, the Multi-Pass system cannot make use of this test to lend credit to or prove authenticity of the number as being assigned to a specific individual. It certainly cannot use such a test to prove identity, as John Smith born on 1 January 1990 could provide the Social Security Number of John Smith born on 1 February 1980, and not be seen as providing fraudulent data. On the other hand, the Multi-Pass system **can** use this service of the Social Security Administration to indicate that a number of 123-12-1234 provided by a John Smith is fraudulent in nature when the service matches the value to a Jane Smith and returns an error.

### ***3.12 Circular References of Non-Authenticated Data Does Not Lend False Credit***

Another issue which has been raised by some concerning the REAL ID system is, under current guidelines, false data can be identified as having been authenticated if sufficient references to the data can be provided by the individual. For example,



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

## **Multi-Pass Proposal**

under section 37.11(e) of the Department of Homeland Security's final rule, an individual who claims to be John Doe with Social Security Number 123-12-1234, need only to provide a Social Security Card with that name and number on it which does not appear to be a forgery, or a pay stub which bears the name John Doe and a Social Security number of 123-12-1234 on it as proof of identity!

Documents such as pay stubs are often printed on simple printers and bearing little to no security mechanisms to prove authenticity. This rule allows forgers to easily create duplicates which will satisfy the ruling and permit issuing authority personnel to state that the individual has proven his/her identity. This is sometimes known as a circular reference because one unauthenticated article lends proof to another unauthenticated article which in turns lends proof to the first article in which both articles may actually be forgeries. The Multi-Pass system will not accept such unauthenticated articles to allow a person to assume an identity.

### ***3.13 Improves Security In A Cost-Effective Manner***

A wide range of values have been stated by various government agencies and other reliable sources pertaining to the cost to implement the REAL ID system. Some reports place the total value of the fifty (50) States of the United States as high as \$14 billion.

We believe that the Multi-Pass system can be successfully implemented in a staged approach over a period of twelve (12) months from the date of total funding which will include all fifty (50) US States for a one-time tax-free fee of \$750 million. After this initial funding, the Multi-Pass system should be able to support itself from the monies received from on-line Multi-Pass account access fees and fees charged for extended services.

By reducing the impact on government budgets and eliminating the need for additional taxation, a large amount of effort can be removed from expensive government processes and placed under the management of a single corporation which is working to support all parties. With this proposal, Bewley Software Productions (BSP) is agreeing to provide the management, software applications, and support of this project.



## **Multi-Pass Proposal**

### **4 Estimated Fees & Rates**

The Multi-Pass system is designed to operate with little to no additional funds received from government bodies beyond the initial start-up costs. Each member, whether an individual or organization, will be responsible for the costs associated with the types of transactions they request from the Multi-Pass system. Although the system does not require individual members to pay any additional fees in order to be a member and receive basic levels of identity security, it is expected that an estimated 80% of all individuals between the ages of 18 and 65 will voluntarily pay the on-line access fee in order to configure and make use of the available additional security features.

All of the fees described below are estimations of the fees to be charged during the first year of Multi-Pass system operation. Additional fees may be added to cover costs associated with management, expansion, and maintenance of a given subsystem. All fees are requested to be considered non-taxable revenue of Bewley Software Productions, LLC. Fees which are not paid in advance and are more than ninety (90) days past due may be reported to applicable government and/or collection agencies. No refunds will be issued for partial-period charges or unused portions of reduced fee allowances. Fees paid for transactions which are processed by the Multi-Pass system are not refundable, whether the transaction receives a response, is denied a response by the target Multi-Pass member, or receives a response which differs from the requested response as allowed by the system.

In order to protect a minimum required level of operation, the Multi-Pass system may automatically and periodically reject the requests received from members who appear to be using the system in a fraudulent manner. For example, if a Multi-Pass member account is being used to request information in a manner which the system deems as an attempt to flood the system with invalid calls, the associated Multi-Pass account may be temporarily blocked from use in an effort to maintain system stability.

#### ***4.1 Multi-Pass Member Individuals***

The following is an estimated fee schedule which applies to all individual members of the Multi-Pass system. Members may fund their accounts in advance or be required to pay for services on a per-request basis. Some charges/fees may be discounted at the discretion of the Multi-Pass Administration.



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

**Multi-Pass Proposal**

- On-line Account Access Fee  
On-line account access fees are charged upon the first attempt to gain access to an account which is not currently listed as being active. Any individual or organization may pay the access fee for an individual, yet this will not gain them access or imply any additional rights, requirements or restrictions upon the individual member. Access is granted to the member beginning the moment payment is received and expires automatically at the end of the purchased period if additional payment is not received. No late fees or back-dated charges apply if there is a lapse of purchased access to an account. An account does not need to be active for an individual in order for employers, financial institutions and/or other registered organizations to transmit information to a individual's account, such as secured payroll information.
  - Standard Access \$9/month or \$96/year  
Standard access rates apply to all persons between the age of 18 and 85.
  - Minor/Senior Access \$4.50/month or \$48/year  
Minor/Senior Access rates apply to all persons less than 18 years of age or who have reached an age of 86 years or greater. Although BSP would like to begin the senior access rate at age 65, the number of attacks on persons between age 65 and 85 is estimated to be sufficient enough to place increased demands on the system. If a sufficient number of members within the 65 to 85 age group optionally allow BSP to gather statistical information in order to identify age-related system demands, the starting age of 86 may be reduced after the first year of operation.
  - Student/Military Access \$7.50/month or \$84/year  
Student/Military access rates apply to all persons who are reported as being a student of an accredited school, technical school, serving on active duty in a branch of the military, or any person working in a contract position for a branch of the military.
- Personal Identity Requests \$0.10/request  
Applies to any request to validate the personal identity of an individual. The member for whom the identity is being tested may refuse to respond to the request. Charges are billed on each request and failed or ignored requests will



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

not receive a refund. Charges for failed requests prevent members from intentionally flooding the system in an attempt to cause system instability.

- Contact Information Requests \$0.05/request  
Applies to any request made by the member to receive contact information regarding another member (target). The target member may respond with information other than that requested by the requester, such as to respond with a postal address rather than an email address. Charges are billed on each request and failed or ignored requests will not receive a refund. Charges for failed requests prevent members from intentionally flooding the system in an attempt to cause system instability.
- Expanded Data Storage \$1.00/month  
Expands the data storage area of the member by one megabyte (approximately 1 million characters of data). Payroll and tax information is stored until space is needed for the storage of new data, at which time items are purged according to age and priority.

## ***4.2 Multi-Pass Member Organizations***

The following is an estimated fee schedule which applies to all organizational members of the Multi-Pass system. Members may fund their accounts in advance or be required to pay for services on a per-request basis. Some charges/fees may be discounted if sufficient funds exist in the account to cover the cost of the transaction prior to the start of the transaction. Some processes may support batch processing at a discounted rate.

- Annual Membership Fee \$250.00/year/100 employees  
Annual on-line access fees are charged upon the first attempt of an organization to gain access to their account within a given annual period. Only payments for full annual-length agreements are accepted. Annual account includes an allowance of (5) identity requests. Any individual or organization may pay the access fees for an organization, yet this will not gain the individual any access to or imply any additional rights, requirements, or restrictions upon the organizational member. Access is granted to the organizational account beginning the moment payment is received and cleared, and expires exactly one year from the date and time of payment. No late fees or back-dated charges apply if there is a lapse of access to an account. No refunds are available for unused portions of an account.



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

- Financial Institution Transaction Validation Fee \$500.00/1 million validations  
This fee is charged to financial institutions per each one million validations processed by the Multi-Pass system. The number of validations granted per each allowance block may be extended at the discretion of the Multi-Pass Administration if more than one block of validations is purchased at a time.
- Identity Requests Related to Sales \$.01/request  
Applies to any identity request related to the sale or transfer of goods between an individual or organization and this organization. The member for who the identity is being tested may refuse to respond to the request, but this will not constitute sufficient cause for a refund of any fees associated with the request.
- Identity Requests Related to Employee \$1.00/request  
Applies to any request to validate the personal identity of an individual employee. The member for who the identity is being tested may refuse the request. If the individual agrees to respond, right-to-work information and other available background data related to employment will be transmitted.
- Identity Requests Not Related to Sales or Employees \$.10/request  
Applies to any request to validate the personal identity of an individual. The member for who the identity is being tested may refuse the request, yet no refunds will be submitted for any fees incurred.
- Contact Information Requests \$0.05/request  
Applies to any request made by the member to receive contact information regarding another member (target). The target member may respond with information other than that requested by the requester, such as to respond with a postal address rather than an email address. This difference of requested information or the choice of the target member to ignore the request, does not constitute sufficient cause for a refund of any fees.
- Employee Payroll & Tax Reporting Transmissions \$0.10/transmission  
Applies to any incoming transmission to the Multi-Pass system which is used to report or request payroll and/or tax information for an employee.
- Employment Right-To-Work Certificate Issuance \$1.00/request  
Applies to a request to issue a Right-To-Work certificate which indicates an employee's right to work for an employer without disclosing any personal identity information. It is recommended that these certificates be kept on-file in lieu of copies of documents showing personal identity information.



**Bewley Software Productions, LLC**  
"Networking and Integrating Your Digital World"

**Multi-Pass Proposal**

- Employment Right-To-Work Certificate Review \$0.50/request  
Applies to a request to review/reprint a Right-To-Work certificate issued to an employer for the indicated individual.

### **4.3 Start-Up Costs & Basic Operating Characteristics**

The Multi-Pass system has been designed to function as a single collection of applications and services executed in a global manner. All users will access the system via the same Internet address of [www.MultiPassID.com](http://www.MultiPassID.com), whether they are representing themselves or an organization.

If the Multi-Pass system is approved and supported by the United States government, the system will be brought on-line in an incremental approach until all States are on-line. This start-up phase is not expected to exceed twelve (12) months from the date in which the full amount of the initial start-up fees is received.

The Multi-Pass system has been designed to operate in a flexible manner, yet all regions must be contained within the same network to function efficiently. For this reason, a build-up of server components, personnel, and licensing will need to occur as the system is expanded to fulfill the needs of the nation.

- One-Time Start-Up Fee \$15 million/State  
Start-up fees are assessed and used to procure the necessary components, licensing, facility costs and payroll demands of initializing and maintaining the Multi-Pass system for the first three years of operation. After start-up, the fees charged to individuals and organizations for their memberships will be sufficient to continue operation with no further costs to either regional or federal governing agencies.
- Auditing Fees \$500.00/hour/person  
All auditing actions requiring the involvement of Multi-Pass system support personnel in any manner will be billed to either the federal or regional governing bodies at the rate of \$500 per hour for each individual involved in the process. The billing will occur in single-hour increments, and used to cover the costs associated with the delays experienced during the audit actions. Auditing actions are defined as any action which provides access to a Multi-Pass facility, server or data stores for the purpose of investigating, validating, or measuring



**Bewley Software Productions, LLC**  
*"Networking and Integrating Your Digital World"*

**Multi-Pass Proposal**

the operations or data of the Multi-Pass systems. These charges will apply whether the actions involve BSP or any of its associated partners/contractors. Operations which are performed without the involvement of Multi-Pass, BSP or partnership personnel, are exempt from auditing fees.

■ Internet Connectivity & Service Fees

Each facility supporting Multi-Pass operations will be serviced by a minimum of three independent Internet service providers (ISPs). Each ISP will be contracted to support the Multi-Pass system in an unlimited bandwidth fashion.

■ Facility & Security Fees

All facilities supporting Multi-Pass operations will be secured by armed security personnel at all times. As Multi-Pass systems and operations grow, an increase in network security specialists, data security specialists, software developers, customer service specialists and other supporting personnel will be added to ensure the security and continuous operation of Multi-Pass systems. During the initial start-up phase, the Multi-Pass system will operate from a single location. Soon after the start-up phase has been completed, a second facility will be opened to mirror the operations of the first facility. This system and data replication will allow for BSP and its partners to provide a consistent, reliable network from which to operate even during periods of extreme weather and/or area-wide Internet service outages.



## **Multi-Pass Proposal**

### **5 Revisions**

From time to time, this document will undergo changes in order to improve clarity and correct typographical errors. Additions and/or changes to the description of services may also occur as processes are identified which could improve the functionality of the system. All changes to this document will be identified within this section and require the approval and signature of Eric JV Bewley in writing before they are to be considered binding in nature.

#### ***5.1 Revision 1: 14 September 2008***

The following items were changed/added to the document released on 14 September, 2008.

##### **5.1.1 Correction to Estimated Launch Date**

A typographical error has been corrected which incorrectly listed the estimated launch date of the system as 1 May 2008. The value has been corrected to read 1 May 2009. Please note that this date is contingent upon BSP receiving the necessary funding state and/or federal government agencies or donations from other sources.

##### **5.1.2 Correction to State Start-Up Costs**

The total amount of start-up costs for the fifty states within the United States, as described in section 3.3, contained a typographical error. This value has been corrected to read "\$15 million/state".

##### **5.1.3 Clarification Concerning State Start-Up Costs**

It has been identified, that further clarification of the use of the initial start-up costs should be added to section 3.3 in order to provide an understanding to the reason that all states are required to pay the full \$15 million. Some believe that smaller states should be responsible for a smaller amount.