

.....  
AssureTec Systems, Inc.

# Improving Security – Protecting Privacy



.....  
*A Practical Path to Greater National  
Security*

Revised May 3, 2002

*Bruce Monk  
President and COO  
AssureTec Systems, Inc.  
603-641-8443  
Bruce.Monk@assuretec.com*



# Improving Security – Protecting Privacy

*A Practical Path to Greater National  
Security*

## **INTRODUCTION AND EXECUTIVE SUMMARY**

In the aftermath of the terrorist acts of September 11, 2001, public opinion swung toward the approval of increased security measures at the expense of convenience and personal privacy. Governments have spent billions of dollars on labor-intensive activities to minimize the risk of future terrorism, while corporations have sustained major hindrances to productivity, new security costs, and losses of business. How long these expenses can be tolerated is unclear, but there's little doubt that more practical and effective avenues to improved security are needed as soon as possible. Already, just six months later, many of the measures adopted have been abandoned as ineffective.

There has been a strong linkage made suggesting that improved security requires the sacrifice of both convenience and privacy. In fact, this need not be the case for most people. Security or the feeling of being secure comes from a trust that the risks are managed and acceptable. Concerns over privacy come from a lack of trust that personal data will not be misused (e.g. threaten our feeling of security!). Law enforcement officials state that they are interested in an examination of less than 5% of the passengers on most commercial flights. A trusted solution which identifies the 5% to be looked at closer and protects the privacy of all will enhance security, limit privacy concerns, and improve convenience for the vast majority.

One path that has received a lot of attention involves a national ID system with a centralized database. Highly expensive, it would provide little improvement in positive identification unless it was accompanied by a totally new identity verification infrastructure to overcome the dual deficiencies of our current system. These deficiencies include the lack of a credible enrollment process and the inability to validate the individual or ID document back to that enrollment/document issuance. Such a centralized system would require years to implement and many more years to complete a new enrollment cycle – provided that jurisdictional debates or “privacy” litigation did not delay or halt the system altogether! Limited in global scope, it would seem to offer little added security until it was fully implemented.

•  
•  
•  
•  
•  
•  
•  
•

---

*A more practical path to improved security involves the use of existing global identification documents and the decentralized databases that support them. The major components of this approach could be in place within months utilizing automated “smart” imaging devices, local biometric data, and a privacy-protecting ID data routing and query system focused on information validation versus data sharing. It would offer immediate improvements to security, speed, and cost over the manual methods now in use. As data “trust authorities” came on-line for real-time yes/no/maybe document validation, ID verification would be enhanced exponentially. “Watch” or “lookout” lists and privacy-protecting “smart” pattern recognition technologies would provide cross-database alert reporting. As the privacy issues surrounding positive biometric identification methodologies were resolved, positive verification would become even more reliable. Until then, the technology exists to accurately use the photo present on virtually all ID documents as a biometric to link the presenter to the document.*

*Can we pay for the security improvements we need? The answer is yes - through the savings realized from fraud reduction. Although we’ve been highly focused on security issues since September 2001, ID verification is also an essential component in the ongoing battle against identity fraud and the painful personal trauma of identity theft. The global financial loss associated with fraud is estimated to be nearly a trillion dollars per year. According to Interpol, fraud ranks as the second largest crime problem worldwide. Identity theft is the fastest growing crime in the United States. Annual losses for counterfeit goods are estimated at more than US\$250 billion<sup>1</sup>, and losses due to document fraud and counterfeiting (checks, credit cards, currency, etc.) are estimated at more than \$400 Billion<sup>2</sup>. The savings that would accrue from fraud reduction should more than pay for the security improvements we need, and the more we automate the process, the greater the savings will be. Also, identity fraud is a key facilitator of many crimes such as slave trafficking, money laundering, terrorism, drug trafficking, pornography, and smuggling. The financial impact related directly to the ID fraud component is impossible to measure, but certainly substantial. The negative toll on society is huge!*

We are at a critical point in our response to terrorism. Do we continue to bear the huge government and industry costs of ineffective manual security methods while we wait for a costly, partial-solution centralized system to be designed and implemented? Or, do we build on improvements to existing infrastructure and choose an immediate, cost-effective, and privacy-protecting method to improved security? Practicality dictates the later.

---

<sup>1</sup> International AntiCounterfeiting Coalition (IACC)

<sup>2</sup> F. Abagnale & Associates

•  
•  
•  
•  
•  
•  
•

---

## SECURITY SINCE SEPTEMBER 2001

In the aftermath of September 11, America has deployed a costly and highly manual approach to improve security. This effort has clearly been necessary, not only to act as an initial deterrent to terrorism but also to instill a greater sense of security among the population.

Thus far the government has spent billions of dollars, we've experienced massive travel and trade disruptions, and corporations have sustained major losses of business and productivity. Convenience and personal privacy have also been sacrificed as public opinion has judged that increased security measures are more important.

In this time of crisis, no expense seems too great and no method too impractical if security can appear to be improved. However, at some point the question of cost will need to be addressed, and along with it the question of whether we are getting sufficient security for this cost. It is very hard to quantify "sufficient security." Perhaps a better way of expressing it is in terms of risk reduction and arriving at a point of trust that deems the risk to be acceptable.

We should note that neither government control nor an increase in training or pay can remove the human vulnerabilities in a largely manual system. Humans are subject to weariness, distraction, dissatisfaction, intimidation, corruption, and boredom. If we acknowledge that risk management is only as good as the ID verification capabilities available to our security personnel, it is disconcerting to realize that no real-time verification system currently exists.

How long we can sustain the current approach is unclear, but there's little doubt that more practical and effective avenues to improved security are needed as soon as possible. Recent changes suggest that the futility of redundant human examination of ID documents has already been recognized.

## SECURITY IN THE FUTURE

Theoretically, there is no limit to what can be done to improve security. Risk reduction is best seen as an infinite continuum, and we have located ourselves historically at points where qualitative improvements are loosely related to quantitative costs that we can afford. Whether or not this "de facto" paradigm will work in the future is unclear, mainly because of the difficulty in achieving consensus on "acceptable" risk in the light of recent events. At the moment, at least, there is widespread agreement that an automated ID authentication system is an essential component to any improved security system of the future. The question here, however, is the kind of system that should be implemented.

•  
•  
•  
•  
•  
•  
•

Ideally, we are looking for a system that will:



...the most important requirements may have to do with system implementation. Specifically the speed with which a system can come on-line and the security improvements achievable...

1. Positively identify an individual and his/her authorization to enter/leave, buy/sell, receive goods/services, or carry out specific jobs/activities in real-time.
2. Protect privacy and reveal only information relevant to the transaction, as “de facto” approved by the individual claiming the right/authorization.
3. Minimize the intrusion on daily activities for both the individual and institutions involved.
4. Equally protect our current and future citizenry.
5. Provide law enforcement with the transaction information needed to assess patterns of behavior that are indicative of illegal activity or the potential intent to commit illegal acts.
6. Provide law enforcement with the traceable evidence needed to apprehend and convict people who do commit illegal acts.

In addition to the above listed components, the most important requirements may have to do with system implementation. Specifically the speed with which a system can come on-line and the security improvements achievable are critical to aid in the prevention of near-term acts of terrorism and, perhaps more importantly, to stop the rebuilding of terrorist cells and their future plans for a time when we relax our vigilance or our vulnerabilities can be better exploited. Like patching holes in a leaking water bucket, we need a system that will start filling as many holes as quickly and as affordably as possible from day one.

## A NEW ID SYSTEM

One path that has received a lot of attention involves the creation of a national ID or “smart card” system utilizing a centralized database. This approach may provide some of the elements we need, but there are some serious issues to overcome.

The US has nearly 300 million residents, and there are about 4 million births and 2.3 million deaths each year. Our population is diverse and many are not in the country legally (US Census estimates over 11 million). This year we will add over 1 million new permanent immigrant residents and about 900,000 new naturalized citizens. In addition, we have nearly 600 million border crossings every year.

Clearly, implementing a new ID system will be a huge task that will require tremendous political will and coordination. It will be no quick matter to establish and

•  
•  
•  
•  
•  
•  
•  
•

get consensus on the new system details - particularly if we are careful to protect privacy and jurisdictional responsibilities wherever and however possible. In addition, a new centralized ID system will require a very expensive and time-consuming process to develop a suitable infrastructure and enroll everyone in the system.

For all the effort, a national ID would still not provide much improvement in positive identification unless it was accompanied by a new identity verification infrastructure to overcome the deficiencies of our current system - deficiencies that have allowed identity theft to become prevalent. If we simply use a driver's license, Social Security number, or birth certificate as proof of identity to get a national ID card, the system is not worth its huge cost.

### THE POSITIVE IDENTIFICATION PROBLEM

Currently, there are substantial problems confirming that an individual is not operating under an assumed or stolen identity. We have a system of birth certification that varies from state to state, and sometimes from county to county. In



Whenever there is a human process that is not audited by an unchallengeable authority there can be no true security.

most cases, there are few controls on the issuance of a duplicate certificate or on the verification of the person for whom it is issued. Whenever there is a human process that is not audited by an unchallengeable authority there can be no true security. People can be bribed, physically intimidated, blackmailed, distracted, or get tired or bored. Therefore, without oversight and accountability, there is no real protection to prevent access to someone else's birth record. Besides, there is no real biometric link to the birth certificate, so who is to know if the bearer is the person to whom it was issued?

An application for a Social Security number requires only the testimony of the "parent." The driver's license/state ID, work permit, or college financial aid applications are all linked to the birth certificate and/or the Social Security number. There is no positive link to the person.

The certification/notification of death is even more poorly controlled. There is no flag placed on the birth record and, unless the person had been collecting a Social Security benefit and Social Security was notified of the death, there is no "retirement" of the Social Security number or prevention of someone from getting a replacement by assuming the identity of the deceased.

What about someone immigrating to the U.S, entering the country illegally, or overstaying a legal entry?

The initial identity checks are harder to make and often impossible to verify. The system relies on the judgment of the people who accept or reject the documentation an applicant uses as proof of identity. Without standards and automated authentication/verification procedures, results can be compromised. Therefore, once

•  
•  
•  
•  
•  
•  
•

---

someone has entered the country, the establishment of an identity requires only that contact be established with someone who knows how to work the system.

Even the new alien residence card has little true security since there is no process for verification that it was legitimately issued to the bearer. There is no real burden placed upon employers to authenticate the document or to verify that the bearer is the person to whom the document was issued. This high-security card has had little impact on “green card” forgery since the earlier “green card” issues were never recalled and are therefore still accepted for employment. Why invest in forging a very secure document when a forgery of the earlier issue is just as acceptable?

Additionally there are foreign visitors who enter either with a Visa or from a Visa Waiver country. The issues associated with US Visa issuance, tracking and Passports issued by Visa Waiver countries are well known to the State Department and INS. Recent improvements in communications and information sharing are addressing some of the issues, but issuing countries must tighten up their processes and procedures in order to offer any substantial improvement.

Solving the positive identification problem is no easy task...

Solving the positive identification problem in America is no easy task - to say nothing about the rest of the world.

#### **PRIVACY CONCERNS:**

Until recently, we were not willing to accept a loss of personal privacy for any reason, and it remains to be seen whether the current flexibility can survive for long – particularly if we happen to be blessed with a period of successful anti-terrorism efforts.

At the heart of a new National ID system would be a centralized database, and without a doubt this raises the specter of “big brother” to the public. There are legitimate concerns, of course, over the centralized collection of information and the potential dissemination of personal preferences, lifestyle choices, and data that can be used to target people for crime, abuse, or unsolicited marketing efforts. However, these concerns are somewhat irrational when we consider that much of our personal information can be found in databases that are in less reliable hands than our government right now.

If properly implemented, a centralized ID database could go a long way toward improving security, but such a system requires a huge shift in the public mindset. Not only would it take more than a few years to implement (some estimates as high as 10 years), but “privacy” litigation could easily delay or halt a new system altogether.

---

## A MORE PRACTICAL PATH

A more practical path to improved security would involve the use of currently existing global identification documents and the decentralized databases that support them. Essential to achieving the maximum risk reduction is to simultaneously undertake critical improvements to the enrollment processes for these documents. Improvements in security features and the addition of additional machine-readable biometrics become less critical if the path is closed back to the Issuer for validation of the document and, hence, verification of the presenter's identity.

Utilizing automated "smart" imaging devices, local biometric data comparison, and a privacy-protecting ID data routing and query system focused on alert reporting, provide the necessary tools for an immediate solution. Major components of this approach could be in place within months, offering automated improvements to security, speed, and cost over the manual methods now in use.

Standardized communication protocols would provide real-time yes/no/maybe document validation on-line from appropriate ID data "trust authorities". "Watch" list and privacy-protecting "smart" pattern recognition technologies would provide cross-database alert reporting to both intercept attempts to gain access to restricted goods or services, but also provide collection of important intelligence information that might be used to prevent attempts to harm people and property.



### Four major elements:

- Data Collection
- Data Analysis
- Real-Time Query
- Risk Assessment

Interestingly the elements needed to issue a risk-rated ID document are the same as those used to assess the risk when verifying the identity and authorization of the presenter

using such a document. The more information that is available and the higher the certainty that the information is accurate, then the lower the risk will be.

How would it work? Let's take a look at the four major elements: data collection at the transaction point, local data analysis, real-time "smart" query, and risk assessment.

### DATA COLLECTION:

**AT THE POINT OF USE:** There are only a limited number of classes of documents used for traveler identification. These documents have several hundred issuers and sub-classes. In the US, state issued IDs, resident alien cards, border crosser cards, passports and visas represent virtually all accepted IDs. Unfortunately, readily available color copiers, PC scanners and other advanced office equipment make document alterations possible. Often, these forgeries are impossible to detect by the unaided human eye, but a "smart" imaging device would catch many if not all of them.

Every document being presented for proof of identity and/or authorization would first be identified. A "smart" imager would be used to automatically "recognize" the

•  
•  
•  
•  
•  
•  
•

document as a travel document, driver's license, alien residence card, INSPASS card, etc.

Once the document is classified, the inspection criteria, layout, security features, and intrinsic characteristics of the master document will be known. Using this



The technology exists today, and it can be upgraded to support any biometric or improvements in the identity infrastructure that might be contemplated.

knowledge, an information set which includes data and images (or any other biometric data) would be captured. The data would come from both human-readable areas protected from forgery and tampering and from regions that are covert and/or intended for machine-readability. Images would be captured using a broad variety of excitation sources and sensors. Only the information that was needed would be collected.

Additionally, an image of the ID presenter would be captured by a camera to compare to the image on the ID being presented (if any). The technology exists to do this today, and it can be upgraded to support any biometric or improvements in the identity infrastructure that might be contemplated.

***AT THE POINT OF ENROLLMENT:*** In the application process for a primary identity document such as a state issued driver's license or a passport, it is critical that a baseline identity be established. Time and effort spent at this point in the cycle of identity verification, decides whether a valid ID will be issued to a true or false identity. Further, it is the logical point for establishment of an initial risk assessment based on that identity.

If there is a lot of data collected and verified about the applicant that validates their claim to a specific identity then there is a high level of confidence that the ID will be issued to a "true" person. Conversely, if little information is available and/or the data cannot be verified, then there is a substantial doubt as to the identity claimed. If there is a contradiction in data or lack of data under circumstances where the data should be available and verifiable, then the ID should not be issued. If an ID is issued where there is a risk associated with the lack of verifiable information then that risk should be noted in some fashion on the document and/or in the Issuer database.

An application form, biometric capture (at least the photo), and possibly a system prompted query/response replace the ID document that are used for data collection versus the imaging and analysis done at the point of use. This data collection process can be highly automated and would take less time than current processing methods.

•  
•  
•  
•  
•  
•  
•



**DATA ANALYSIS:**

**AT THE POINT OF USE:** The information collected would then be analyzed and compared with the known characteristics of the master document. This would include the processing of the data to verify consistency, age, expiration date, check-digits, form, and format.

Images would be processed to check the composition of the document; characteristics of the materials, and evidence of any alteration. Also, document classes with known forgery characteristics would be specifically examined in the sensitive areas. Some of the tests would include the inspection of the surface of the document for the presence of security features or cuts. Additionally, an ID photo (if available), or any other biometric information contained and protected on the document, would be compared to actual data collected at the inspection point.

Depending upon the availability of real-time document inquiry, conclusions about the authenticity of the document (at this point) would be presented to the appropriate authorities or control agent for action in the form of a “SCORE”. Below this practically established SCORE, the document and bearer would be automatically referred to a secondary processing station for a closer forensic examination.

**AT THE POINT OF ENROLLMENT:** Information collected at the application point (or pre-collected centrally) would be analyzed for consistency and compared against existing data sources for accuracy. This “life profile” analysis would be carried out under the same guidelines for privacy protection using trust authorities to validate data as opposed to data sharing or data mining.

Pragmatically, in the United States and Canada where the primary domestic ID is issued by each state or province, data capture and analysis represent the most efficient means by a central ID Clearinghouse, with oversight by an organization such as the American Association of Automobile Administrators. Such functionality can be provided without retention or dissemination of personal information.

**REAL-TIME “SMART” QUERY:**

**AT THE POINT OF USE:** Although a definite improvement over manual ID verification would be seen prior to this point, the most effective part of the system involves a real-time inquiry to appropriate ID Trust Authorities and other relevant databases (known suspects, stolen documents, forgeries, other “watch” lists, etc.). Let’s take a closer look at ID “Trust Authorities” before we briefly cover the process.

As we’ve previously noted, “Issuance Authorities” exist around the world to issue ID documents. Within the US they include the US State Department, the INS, and various state/provincial drivers’ license issuers. ID “Trust Authorities”, on the other hand, are entities that are specifically charged with the responsibility of validating information to an acceptable level of confidence and providing limited, privacy sensitive access to the information by authorized inquirers through a standardized protocol.

•  
•  
•  
•  
•  
•  
•  
•

---

Where they do not yet exist, identification “trust authorities” would need to be established at both state and federal levels. This is not a huge or costly task - the infrastructure and the people are in place, and the data has already been collected with some degree of confidence in its accuracy. (The successful “Motor Voter” legislation in recent years is an example of how this would work). In addition, the network support for accessibility, database structures for information management and encryption technology to protect the data are readily available.

Trust authorities would have the capability to answer real-time yes/no/maybe validation questions based on the data obtained at the transaction point. An impersonal ID number that is validated at the time of the transaction and the history of transaction results (not details) associated with that number is all that should be shared by anyone unless specifically authorized by the individual for a limited time and for a given purpose – similar to driving records, health records, criminal records, and educational history. None of these records would require any sensitive personal information to be linked to them. The confirmed identity check could be made through the Trust Authority any number of ways, including biometrically supported call-back mechanisms over secure network connections.

Since the Trust Authorities do not have to provide any information concerning the identity of the bearer unless there were sufficient reasons to suspect illegal activities, there would be few privacy issues. This is very important in gaining the support of foreign governments to remotely validate their documents - their response would simply be OK, no record, or problem (such as warrant/detain, stolen, revoked, expired, data/image mismatch, etc.). None of this activity would require access to specific identity data.

***AT THE POINT OF ENROLLMENT:*** An anonymous “datametric” can be created from the non-personal data collected from the application form and encoded for use very much the way a biometric template is generated. This would be indexed by the original application transaction code and used for comparison against each new applicant in order to detect attempts at identity theft or assumption of multiple identities.

Only in instances of suspected identity theft or an attempt to create a duplicate identity (for example, to obtain a second driver’s license or replace one that has been revoked or to establish a “new” residence to avoid child support) would there be a justified need to communicate between the states during the enrollment process.

#### **RISK ASSESSMENT:**

***AT THE POINT OF USE:*** The information at the transaction point in combination with the information available in the various Trust Authorities databases constitutes a distributed Knowledgebase on the background of both the individual and the

•  
•  
•  
•  
•  
•  
•  
•

document. The responses received in real time from the Trust Authorities represent their individual assessments of how consistent the query data is with their information. The responses also reflect the level of interest or risk that each Trust Authority has in the individual.

An assessment of the net risk can be made using these responses and a relative “score” can be derived to determine the appropriate action to take. For example, Trust Authority data analysis could include comparison of the information to models of questionable travel behavior and data combinations such as arrival/departure locations and travel patterns. This process would be particularly weighted as a higher risk for non-citizens and comparing entry/exit information to the stated purpose and plans for each visitor. Obviously, factors such as history of violent behavior or recent issuance of the ID document might also be used in determining a Trust Authorities’ assignment of the category of risk. In addition to the category of risk, the response might also include an action request to apprehend, question, or notify someone. Actions taken would be according to rules established by the appropriate control authorities.

This approach has many practical benefits, in addition to heightened security. For example; “smart screening” techniques could be employed in passenger processing—resulting in more thorough checks for some passengers and baggage while improving overall speed for everyone. Best of all, perhaps, there would be less need to resort to public profiling based on race, nationality, or ethnicity. Also, there would be a substantial economic benefit derived from more efficient use of people, space, and equipment.

***AT THE POINT OF ENROLLMENT:*** A very similar process to the one described for the transaction point would be used to SCORE the risk that the person applying for the ID is who they say they are. By requesting a lot of diverse data on the application form and automatically scoring each data field for its accuracy there will be sufficient data points available to mitigate problems of data entry errors, poor memory by the applicant, and normal omission mistakes.

As with the capture of data to build or match against a biometric template, the number of features (data points) and the accuracy of the measurement determine the confidence level. However, a datametric has the advantage of there being absolute immutable reference points, whereas a biometric does not! Hence, there are no issues of aging, injury, missing fingerprint, square iris, or poor measurement practice/calibration.


Blatant omissions in this life profile versus expectations are clear elements that would indicate increased risk or might even be cause for rejection. Information that cannot be validated such as foreign birth certificates would also lower confidence.

Non-personal information collected from this process could also be randomly selected to form queries to the applicant at the transaction point as opposed to online queries of commercial databases that would represent severe privacy concerns.



**SYSTEM IMPLEMENTATION:**

It is estimated that there would be an immediate benefit (90 to 120 days) from stand-alone local document authentication and information capture. Access to databases



...the entire process could be put in place within 12-18 months.

such as IBIS, INS and the State Department should be possible in the same time period closely followed by state Driver’s License information online. *Most significantly, the entire transaction point process could be put in place within 12-18 months. The enhanced enrollment process would take somewhat longer to fully deploy based on governmental decision cycles and not technology!*

In addition to rapid implementation time, the system would be quick at the inspection point, easy to use, upgradeable, and cost-effective. It would also have a much lower potential for implementation delay due to personal privacy issues.

With this practical approach, there is a great deal that can be accomplished quickly to recover the throughput capacity at our borders and airports while substantially improving security. This system would enable better utilization of existing technology components and move forward with a scalable, open and continuously-improving system. This would greatly benefit our way of life and economy.

**PAYING FOR IMPROVED SECURITY**

Though we’ve been focused on security issues since September 11, ID verification is also an essential component in the ongoing battle against fraud. The global financial losses associated with fraud is estimated to be nearly a trillion dollars per year, and even if we were able to eliminate only a portion of that, it would go a long way economically to pay for the security improvements that we need. The more that we automate the process - and the faster that we plug the fraud “holes” - the greater the savings will be.

According to Interpol, fraud ranks as the second largest crime problem worldwide. Annual losses for counterfeit goods are estimated at more than US\$250 billion<sup>3</sup>, and losses due to document fraud and counterfeiting (checks, credit cards, currency, etc.) are estimated at more than \$400 Billion<sup>4</sup>. In a recent national survey, nearly three-quarters of Americans believe identity fraud is an increasing problem and 78 percent are concerned it poses a serious personal threat in today’s world. ... Identity-fraud

<sup>3</sup> International AntiCounterfeiting Coalition (IACC)

<sup>4</sup> F. Abagnale & Associates

•  
•  
•  
•  
•  
•  
•

cases cost \$450 million in 1996 and \$745 million in 1997...<sup>5</sup> (This survey was taken prior to the September 11 attack on The World Trade Center and Pentagon).

In the U.S. there is more than \$15 billion in annual check fraud. Also there is more than \$1.5 billion in credit card fraud and more than \$3 billion in real estate fraud related to falsified applications.

In addition to financial loss, many criminal acts are enabled by fraud including child abduction, slave trading, smuggling, and drug trafficking. Clearly, the cost to society for these acts is not trivial. In many instances there would be a great willingness on the part of institutions and individuals who bear the cost and assume the risk for these fraud prone transactions to subsidize the infrastructure in return for their risk/cost reduction. A “click” fee, application surcharge, or periodic service fee could be used to distribute the cost to those with the greatest benefit.

Can we pay for improved security? Yes, and depending upon the approach we choose, the news could be surprisingly good.

## CONCLUSION



...we must continuously improve security while protecting as much of our personal privacy and way of life as possible.

The INS has been evaluating ways to automate the inspection process for several years, and had something been in place, it might have played a significant role in detecting the September 11<sup>th</sup> plot. We can't change the past, but we can influence the future, and intelligent decisions must be made as soon as possible.

Do we continue to hope that our manual security system alone will be sufficient to do the job, or do we start to automate the ID verification process right away to improve accuracy and speed?

Do we wait for a totally new ID system to be designed and implemented, or do we make more effective use of the ID documents and systems that currently exist?

Do we gamble that a new centralized ID database won't be delayed by privacy litigation, or do we move forward with a privacy-sensitive data validation system that has a higher probability of public acceptance?

Practicality would seem to suggest the later path in each case.

Whatever we decide, this much is clear - we must continuously improve security while protecting as much of our personal privacy and way of life as possible. A great deal is at stake if decisions are prolonged and solutions are unnecessarily delayed.

<sup>5</sup> Nashua Telegraph, PG 1, “FBI on lookout for suspected counterfeiter,” Wednesday, January 03, 2001



***BRUCE MONK** is President and Chief Operating Officer of AssureTec Systems, Inc., a company that specializes in versatile imaging- based document authentication devices and systems. Mr. Monk has more than 20 years of senior management level experience in engineering, marketing and sales management in the high technology field. In February 1991 Mr. Monk founded Imaging Automation, Inc. Until November 2000, Mr. Monk served as an officer and director for the developer of document recognition and authentication products. Prior to founding Imaging Automation, Mr. Monk founded Chorus Data Systems and also served in development, engineering and sales positions with Analogic, Sanders Associates and Hewlett Packard.*