

HEIGHTENED SECURITY:

**Can Financial Institutions
Really Know Their Customers?**



SEPTEMBER 2002[©]

The following report was prepared by Star Systems® (STAR_{sm}), a Concord EFS, Inc. subsidiary, in conjunction with Powell Tate. The information contained in this publication is intended for informational purposes only and should not be construed as legal advice.

Copyright © 2002 by Star Systems®, a Concord EFS, Inc. subsidiary. All rights reserved. No part of this publication may be reproduced without the prior written permission of Star Systems.

TABLE OF CONTENTS

- Executive Summary**1
- Introduction**3
- Identity Theft: Old Crime, New Threat**5
 - Identify Theft5
 - Identity Fraud6
 - Combating Identity Theft and Identity Fraud7
- Public Opinion and the Need for Caution**9
- Role of Financial Institutions in National Security**11
 - Combating Money Laundering12
 - Verifying Customers’ Identities13
 - Drivers Licenses14
 - Birth Certificates17
 - Social Security Cards18
 - Immigration and Naturalization Service Documents19
 - Identification Issued by Foreign Governments20
- Considering a National Identification Card**23
- Enhancing Security Today**25
- Looking Ahead**29
- Appendix**
 - Key Provisions of the USA PATRIOT Act for Financial Institutions . . .31
- Acknowledgments**35

**HEIGHTENED SECURITY:
Can Financial Institutions Really
Know Their Customers?**

September 2002

Executive Summary

The current climate of heightened security, crystallized in the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), adds a new sense of national urgency to what has long been a top priority of financial institutions: enhancing security in order to combat fraud – from identity theft and credit risk to identity fraud and money laundering. The USA PATRIOT Act calls on financial institutions to redouble their security protocols, specifically, to share anti-money-laundering information with regulators, law enforcement, and each other, and to intensify their efforts to verify customers' identities at account opening.

As financial institutions anticipate meeting the challenges of these requirements, this white paper discusses pitfalls in the current compliance environment. Financial institutions must exercise caution in selecting the information to be shared, lest they find themselves outside the safe harbors the Act provides. And the identity documents available

at present are fraught with opportunities for fraud and abuse, providing little assurance to the financial institutions that must rely on them to identify customers.

This white paper surveys some of the current deficiencies in identity documents, examines the ongoing debate over a national identification card, and provides an overview of products and technologies that offer interim solutions – not only for financial institutions but also for other settings where identity verification is required.

Star Systems® (STAR_{sm}), a Concord EFS, Inc. subsidiary, through its dedication to the security of electronic payments, contributes to the security of the U.S. financial system as a whole. STAR hopes that the information and analysis provided in this white paper will help financial institutions fulfill their role in heightened national security.★

INTRODUCTION

Financial institutions have been developing and implementing identification and security procedures for many years. A broad range of practices, from confirming the identity of an individual opening a new account or withdrawing funds to verifying the name, contact information and credit-worthiness of a loan applicant, have long been critical to maintaining the safety and soundness of financial institutions. In addition to helping to maintain the U.S. banking system as the strongest in the world, effective fraud prevention measures are key to helping financial institutions fulfill their fiduciary responsibility to accountholders as well as assisting publicly held institutions to fulfill their due diligence responsibility to shareholders

As financial institutions' identification requirements and security methods have become more sophisticated, so too have criminals' strategies to compromise them. A much-publicized result of this escalation has been a rise in identity theft. The consequences – already high when identity theft was essentially a “financial” problem – became far more cataclysmic with the September 11 attacks, financed and carried out by hijackers, many of whom used false identities.

The national climate of heightened security after September 11 engendered strong bipartisan support for the USA PATRIOT Act, which became law on October 26, 2001. Among other things, the Act requires financial institutions to enhance their identity verification procedures, and the financial services industry is rising to embrace the challenge. Until identification documents such as drivers licenses and birth certificates can be made more secure, financial institutions will continue to face an uphill struggle in their efforts to curtail identity theft, whether to protect national security or the security of the institution's own deposit accounts.

This white paper begins by looking at identity theft, its enormous toll on individuals and financial institutions and the new implications for national security. It examines the responsibility placed on financial institutions to protect national security since September 11, particularly as envisioned in the USA PATRIOT Act, which imposes new restrictions to combat money laundering and requires enhanced procedures for verifying the identities of individuals opening new accounts. Finally, the paper discusses the need to make identity documents more secure and reliable and

looks at tools that can help financial institutions overcome those documents' current weaknesses.★

IDENTITY THEFT: OLD CRIME, NEW THREAT

Long before September 11, 2001, the financial services industry was taking steps to prevent fraud, including one of the most damaging kinds – identity theft. Measures included requiring a PIN to get cash from an ATM, putting a cardholder’s photograph on a credit card and participating in databases that help prevent check fraud and identify credit risks. Although these measures are helpful, the continued growth of identity theft and related crimes demonstrates that they are not enough.

Identity Theft

Identity theft, also known as “true name fraud,” generally involves a criminal’s wholesale takeover of someone else’s identity – including name, birth date, Social Security number and financial accounts – primarily for individual financial gain. Between November 1999 and September 2001, the Federal Trade Commission (FTC) Identity Theft Data Clearinghouse received 94,100 complaints from victims. The scope of the identity theft problem has prompted the FTC to offer a downloadable “ID Theft Affidavit” form on

its web site, www.ftc.gov, to assist victims in the recovery process. Within two weeks following September 11, the FTC issued a warning that attempts were being made to steal the identities of individuals killed in the attacks. Indeed, both Sydney’s *The Daily Telegraph* (October 20) and *The Charlotte Observer* (October 31) reported arrests of individuals doing exactly that in Australia and North Carolina, respectively.

Identity theft is both devastating to its individual victims and also costly to financial institutions.

- Complaints to the FTC of harm from identity theft that did not include money lost or paid as out-of-pocket expenses included 7,000 victims who were denied credit or other financial services as a result of the theft, 3,500 who reported time lost to resolve identity theft problems, and 1,300 who were wrongfully subjected to criminal investigation, arrest or conviction. A separate study, released in May 2000 by the California Public Interest Research Group and the Privacy Rights Clearinghouse, reported an average of 175 hours lost – equivalent to more than a month of 40-hour work weeks.

- More than 2,600 of the identity-theft victims reported money either lost or paid as out-of-pocket expenses, with more than 200 alleging costs between \$5,000 and \$10,000 and another 200 alleging costs above \$10,000.
- Those relatively small statistics on the cost to consumers belie the real economic cost of identity fraud, much of which is borne by financial institutions.
 - According to the American Bankers Association (ABA), losses to check fraud in 1999 totaled \$679 million – up by almost a third from 1997 – of which 29 percent, or \$197 million, was attributable to identity theft.
 - More than half (56 percent) of check fraud at community banks (banks with assets under \$500 million) was attributable to identity theft, according to a February 2002 report by the General Accounting Office (GAO) to the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information.
 - In the credit card arena, the GAO report found that the two major payment card associations alleged that U.S. losses from

identity theft (which the card associations define as account takeovers and fraudulent applications) rose 43 percent from \$79.9 million in 1996 to \$114.3 million in 2000.

- According to a September 2001 report by Celent Communications, it is estimated that losses to financial institutions due to identity theft will exceed \$8 billion by 2004.

Financial institutions have always factored a certain level of fraud into their cost of doing business. With the recent rise in identity theft, however, many of these costs may eventually be passed on to consumers in the form of higher fees for financial services.

Identity Fraud

As costly as identity theft can be to individuals and financial institutions, far more is now at stake, as the events of September 11 demonstrated. A different form of identity theft – increasingly known as “identity fraud” – entails creating a new identity, either from scratch or by cobbling together a name, address, birth date and Social Security number from several

different sources, in order to evade detection and commit crimes. Identity fraud helped some of the September 11 hijackers operate undetected in the United States for months – even years – using false or composite identities to obtain drivers licenses and credit cards and to pay for housing, transportation and flight training.

Combating Identity Theft and Identity Fraud

It is little wonder that combating identity fraud is a major goal of the USA PATRIOT Act, which became law only 45 days after the September 11 attacks. And – because identity fraud in the financial arena abetted the terrorists – Title III of the Act is, in part, a call to financial institutions to redouble their efforts in this area. An appendix on page 31 provides a detailed explanation of key provisions of the USA PATRIOT Act.

Although the USAPATRIOT Act represents a milestone in national security, much of Title III echoes, reinforces and builds upon efforts that are ongoing at financial institutions. For example, many of the tools and techniques that the financial services industry is already employing to enhance security to combat

identity theft and other types of fraud also can be effective weapons against the new threat posed by identity fraud.

Unfortunately, as strong as an individual financial institution’s commitment may be, the lack of secure and reliable identity documents – most notably drivers licenses, but also birth certificates and Social Security cards – considerably hampers efforts to prevent identity theft and protect national security. Given the lack of security and reliability of these documents, financial institutions must depend on experience, common-sense due diligence, and an arsenal of new technological solutions to fulfill their traditional responsibilities as well as their additional role as front-line defenders in the new war on terrorism. ★

PUBLIC OPINION AND THE NEED FOR CAUTION

Policy developments since September 11 have highlighted the significant tension that exists between security needs, which require access to personal information, and privacy needs, which require protecting personal information from access. That tension inevitably will result in repeatedly redefining the balance between security and privacy in laws and regulations as our nation's priorities fluctuate.

This could become increasingly important as the public opinion pendulum – which swung dramatically toward security immediately after the September 11 attacks – swings back toward privacy, as recent polls indicate it already has begun to do. For example, in two polls conducted shortly after September 11, more than two-thirds (Harris Poll, 68 percent; Pew Research Center, 70 percent) of Americans supported a national identification system. In contrast, a *Washington Post* poll conducted in November 2001 found that nearly half (44 percent) of Americans viewed such a system as “an invasion of people’s civil liberties and privacy,” and another poll released in March 2002 by the Gartner Group

found that only a quarter (26 percent) of Americans favored the idea.

In contrast to the *Washington Post* and Gartner Group polls, a second Harris Poll, conducted in March 2002, found support for a national identification system still relatively high, with 59 percent continuing to favor one, down from the September figure of 68 percent. However, that same poll found that only 12 percent of those surveyed remained very confident that U.S. law enforcement would use its expanded surveillance powers in a proper way, down almost two-thirds from 34 percent in September. Moreover, nearly a quarter (23 percent) of respondents were “not very” or “not at all” confident that U.S. law enforcement would act properly, almost double the 12 percent that expressed those doubts in September. And – most relevant to this discussion – those favoring closer monitoring of financial transactions had fallen from 81 percent in September to 72 percent. In future surveys, it will be instructive to see whether the figures continue this trend.

Even without the complicating factor of shifting public opinion, it is crucial that

financial institutions ensure that their actions fall completely within the parameters of the exemptions provided in the USA PATRIOT Act, lest they discover that actions taken outside those parameters are not protected. For example, if a financial institution – after receiving personal information under the voluntary information-sharing program established by 314(b) – either fails to protect the security and confidentiality of that information or uses it for any purpose other than those explicitly authorized, it may find that its actions are not protected from the application of the Gramm-Leach-Bliley Act or other privacy protection measures.

It remains to be seen whether a strict reading of section 314 might constrain financial institutions' good-faith efforts to stop money laundering and terrorism and, if so, how an appropriate balance of national security and consumer privacy might be achieved under this section. ★

ROLE OF FINANCIAL INSTITUTIONS IN NATIONAL SECURITY

The financial services industry – arguably more so than any other sector – has long had a business interest in verifying the identity of its customers. Losses from check fraud and bad debts can take a significant toll on financial institutions’ profits. Therefore, verifying the identity of someone who is opening a checking account or applying for a loan is, quite literally, a “bottom line” concern for financial institutions, which have become experienced in developing and implementing comprehensive customer identification and verification procedures. After September 11, those procedures took on new significance as financial institutions were called upon to play a greater role in protecting national security.

The USA PATRIOT Act requires financial institutions to go the extra mile in at least two critical areas: preventing money laundering and verifying customers’ identities. The financial services industry embraces this two-pronged approach to fighting terrorism and takes its new responsibilities seriously. For many financial institutions, however, the Act merely crystallizes a requirement for

which they may already have sufficient policies and procedures in place. Indeed, as financial institutions comply with new regulations to combat money laundering and identity fraud, many will rely on security-enhancing tools already available to detect irregularities and increased risk exposure.

The USA PATRIOT Act comes at a time when the climate in America is more amenable to such measures than it was in late 1998 when banking regulators jointly proposed uniform “know your customer” rules. These rules would have placed financial institutions in a quasi-investigatory role, categorizing their customers’ expected account activity and reporting anything that fell outside those expectations. A wide spectrum of organizations and more than a quarter-million individuals concerned about consumers’ financial privacy opposed the proposal, and regulators withdrew it in early 1999.

“Know your customer” (KYC) was not a novel policy when it was proposed in 1998. Each of the federal banking regulatory agencies has long included its own specific KYC requirements among the “safety and soundness” criteria on which it routinely

examines the institutions it regulates. The 1998 proposal was, in part, an attempt to standardize those requirements across all federally regulated financial institutions.

After the withdrawal of the proposed uniform regulations in 1999, KYC requirements have continued to vary somewhat from one regulatory agency to another. The new anti-money-laundering and identity verification provisions of the USA PATRIOT Act will standardize the KYC requirements on which all federal bank regulators examine the institutions under their supervision. Depending on each agency's current KYC regulations, the new requirements under the Act may – or may not – go beyond the requirements on which the regulator has traditionally examined the financial institutions it oversees.

Combating Money Laundering

Although the USA PATRIOT Act imposes new measures to combat money laundering – specifically requirements regarding shell banks and private and correspondent accounts – anti-money-laundering measures have been in effect for more than 30 years, beginning with the Bank Secrecy Act when

money-laundering prevention became a natural extension of larger risk-management efforts employed by financial institutions.

One of the most effective of those measures is the Suspicious Activity Report (SAR). A financial institution is required to file an SAR “when it detects a known or suspected criminal violation of federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act.” Thus, unlike a Currency Transaction Report (CTR), which is specifically required for currency transactions of \$10,000 or more, the criteria for filing an SAR are somewhat subjective, based on the judgment of each financial institution.

According to Gregg James of the United States Secret Service electronic crimes division, a majority of financial institutions do a good job of filing SARs whenever appropriate, and he encourages financial institutions to err on the side of filing too many SARs, rather than not enough. “The more data our computer systems have to analyze,” says James, “the more likely we are to detect money-laundering trends and patterns that could not be discerned from examining individual reports.”

The Secret Service's efforts depend on intelligence from the full spectrum of U.S. financial institutions, though it works most closely on money-laundering issues with the seven largest ones, which, according to James, account for 70 percent of the country's financial transactions. "Our major focus is on cutting off the head of the snake," he says, "and at the same time we are looking at ways to get the thousands of smaller banks more involved in this effort. Success depends on the cooperation of everyone involved – technical and financial experts from the full spectrum of financial institutions."

A pilot test of the secure Financial Crimes Enforcement Network (FinCEN) mandated by the USA PATRIOT Act began on May 28, 2002, with approximately 30 financial institutions filing SARs electronically at the secure Patriot Act Communications System (PACS) web site. A cross section of financial institutions from around the United States – including large, medium and small institutions and encompassing banks, credit unions, and savings and loan institutions – will use the pilot to test the system and identify opportunities for enhancements and adjustments. Following the 60-day pilot period, FinCEN is

evaluating the pilot's success and determining how best to deploy PACS nationally.

Verifying Customers' Identities

For financial institutions, efforts to enhance security begin with each individual customer. To that end, and within the bounds of privacy concerns, financial institutions have continued to exercise, and steadily increase, due diligence regarding verification of a customer's identity – the "first line of defense" and the foundation for all other security efforts.

Virtually all the documents that can be used by financial institutions in the United States for identity verification – drivers licenses, birth certificates, Social Security cards, passports, visas – are issued by a government, either local, state, national or foreign. Until relatively recently, checking identity was generally straightforward. It was rarely necessary, for example, to validate information on the license or to do much more than confirm that the individual pictured on a drivers license was indeed the person presenting it as identification. However, the past few years have seen a

rapid rise in identity theft and other types of fraud, prompting financial institutions to become increasingly vigilant and circumspect in dealing with potential customers.

An industry resource guide released in January 2002 by the American Bankers Association's (ABA) Account Opening Best Practices Group noted "the ease with which identification documents can be falsified" and concluded that "the current system is simply not sufficient to catch fraudulent state and federal identification documents." In particular, the Group found four major safeguards lacking in currently available customer identification processes:

- Uniform procedures for official state identifications;
- Governmental verification processes;
- Meaningful biometric identifiers; and
- Real-time commercial verification products.

Drivers Licenses

Originally, drivers licenses were little more than licenses to drive. Early driver-licensing initiatives were simply attempts to ensure that vehicle operators had a certain level of knowledge and ability and to keep

unqualified individuals off the roads. Today, according to a survey conducted recently for the American Association of Motor Vehicle Administrators (AAMVA), 87 percent of Americans use their drivers licenses for other purposes as well. The presence of a photograph, as well as a birth date, an address, and – often – a Social Security number, have made drivers licenses *de facto* identity cards, the "photo ID" of choice used for everything from writing checks to buying tobacco and alcohol and, more recently, to boarding airplanes.

Beyond helping ensure the safety of pedestrians and other drivers, however, drivers licenses were not originally intended as security documents, though that is exactly what they have become. As a result, the lives of more and more people depend on a document that is becoming less and less secure.

For example, at least four states – North Carolina, Tennessee, Utah and Virginia – have been issuing issue drivers licenses to undocumented immigrants, without requiring identity documents such as a birth certificate and Social Security number. Although this practice is not "illegal," it has

prompted the Department of Public Safety (DPS) in South Carolina – one of many states that have traditionally accepted out-of-state licenses presented by drivers license applicants as qualifying identity documents—to stop accepting licenses from North Carolina, Tennessee, Utah and Virginia. In November 2001, Representatives Nathan Deal (R-GA) and Tom Tancredo (R-CO) and then-Representative Steve Largent (R-OK) wrote to the governors of the 50 states and the mayor of the District of Columbia, urging them not to accept licenses from those four states as qualifying identity documents for license applications. Tennessee and Virginia are in the process of tightening their requirements in this area.

California and New Jersey have been the subject of negative media attention for the laxness of their driver-licensing processes and incidents of employee fraud. Among other issues, New Jersey only recently began requiring the inclusion of photographs on drivers licenses, and some valid licenses without photographs are still in circulation, making them even more problematic for institutions that rely on drivers licenses for identification. California began implementing reforms in 2001 and New Jersey's

governor announced plans in April 2002 to overhaul the system in his state.

Most states require a Social Security number in order to issue a license, but few scrutinize it beyond ensuring that it is in the proper format and contains the correct number of digits. Some states will issue a drivers license to an applicant presenting only a taxpayer identification number, and Kansas requires only a photograph. Florida's state-of-the-art underground driver-licensing industry, fed by the millions of underage students who flock there each spring, produces bogus drivers licenses that "are virtually indistinguishable from the real thing," according to Captain David Myers, a fraudulent-identification expert in the Bureau of Law Enforcement of the Florida Division of Alcoholic Beverages and Tobacco. Other state law enforcement bureaus call on the expertise of Captain Myers and his colleagues; about 75 percent of the complaints they handle are from out of state.

In light of the wide variability among states' security procedures, it is not surprising that Washington state recently simplified its reciprocity decision-making by deciding not to accept drivers licenses from any

other state as qualifying documents for Washington drivers licenses. Other states are expected to follow suit.

The AAMVA is committed to strengthening the driver-licensing process throughout the United States. Working with the Social Security Administration, the AAMVA has developed a direct link to an online database that can verify the validity of a Social Security number and whether it was issued to the person presenting it. Integrating the database link into the overall driver-licensing process is a complex undertaking; fewer than 20 states have implemented it so far. AAMVA envisions similar direct links to the National Association of Public Health Statistics and Information Systems (NAPHSIS, the repository of birth and death certificates) and to the Immigration and Naturalization System (INS). The organization also is looking into ways to prevent insider fraud by department of motor vehicle (DMV) employees.

The AAMVA's Jay Maxwell, who has investigated procedures for issuing drivers licenses in Mexico, reports that at least three of the largest Mexican states have instituted a new measure to combat employee fraud. To get a drivers license in these three states,

an applicant must deal with three different clerks. The first one takes the application, the second makes the photograph, and the third administers the written test.

Another approach to tightening the driver-licensing process was suggested in April 2002, when Representative Jim Moran (D-VA) introduced a bill in the House that would set national standards for state-issued drivers licenses, and Senator Richard Durbin (D-IL) announced plans to introduce a similar bill in the Senate. Known as the Driver's License Modernization Act of 2002, the House bill would require each state to incorporate into drivers licenses (and DMV-issued non-driver identification cards) tamper-resistant security features, as well as computer chips and biometric data that can be read by the law enforcement agencies in every state. The bill's requirement that DMVs "accurately document the identity and residence of an individual" would likely end some states' practices of issuing licenses without sufficient documentation. The bill also mandates rapid data sharing among law enforcement agencies in different states as well as between state and federal agencies, and provides funding to enable states to implement such a system within five years.

Both the House bill and the draft Senate bill, which had not been introduced by mid-July 2002, would address the confusion caused by the more than 240 different drivers license formats that currently are valid in the United States, as would a measure in the National Strategy for Homeland Security, released by the White House on July 16, 2002. Noting that “the federal government can assist the states in crafting solutions to curtail the future abuse of driver’s licenses by terrorist organizations,” the White House proposes that “the federal government, in consultation with state government agencies and non-governmental organizations, should support state-led efforts to develop suggested minimum standards for driver’s licenses.”

These moves toward more uniform state-to-state technical requirements has prompted some privacy advocates to characterize the bills as precursors to a national identification system. Some have expressed particular concern over the proposed incorporation of biometric data into drivers licenses.

The AAMVA’s Maxwell applauds the uniform biometric requirement. “Since September 11, more than 12 million drivers licenses incorporating biometrics have been

issued by six states, including Arkansas, Georgia, Hawaii, Illinois, North Carolina, and West Virginia, as well as the District of Columbia,” says Maxwell. “Unfortunately, the biometrics – which range from index finger prints to facial scans – differ from state to state, meaning that the index finger print on a drivers license issued in West Virginia cannot be read by the facial scanners a few hundred miles away in North Carolina. This needs to be standardized soon, before more states invest more taxpayer money in disparate biometric systems.”

Until reforms such as these are established and implemented, using drivers licenses to confirm identity remains problematic.

Birth Certificates

As with drivers licenses, birth certificates were not originally intended to be multipurpose identification documents. They were primarily public health documents, used to document births, monitor epidemics and manage quarantines in port cities like Baltimore and New Orleans. Today, however, birth certificates are routinely used for issuing drivers licenses and passports and verifying date of birth for Social Security and Veterans Administration benefits.

Unfortunately, the security of most birth certificates today isn't commensurate with the importance society places on them. In many states, duplicate and counterfeit birth certificates are notoriously easy to obtain. A study released in 2000 by the Department of Health and Human Services found that more than 6,000 different entities in the United States issue birth certificates, and that there are more than 14,000 valid versions in circulation. This profusion of formats makes it virtually impossible for all but identity experts to determine whether or not a particular birth certificate is genuine or a fake.

Louisiana operates one of the tightest birth-certificate issuing systems, in which all certificates are uniformly printed with security features including special paper, watermarks, and ultraviolet ink. Every sheet of the paper is tracked, and a certified copy of an individual's birth certificate can be issued only to that individual or to a close family member – and the applicant is photographed. In contrast, New Jersey is purported to operate one of the loosest systems, with more than 500 different agencies issuing birth certificates and no standard paper or format.

To top it off, 13 states that have open-records laws make all their birth and death certificates available on the Internet. Although this openness is a boon to genealogists and other legitimate researchers, it makes it much easier for criminals to create convincing documents.

Social Security Cards

Social Security numbers also suffer from “mission creep.” Originally issued to facilitate and secure the payment of retirement and disability benefits, the Social Security number has become one of the most widely used identifiers, requested on documents from credit card applications to elementary school enrollment forms. Until recently, Social Security numbers appeared on drivers licenses in many states, though that trend is now reversing, and bills recently introduced in Congress would dramatically curtail their use. Social Security numbers have become such a ubiquitous key to identity that gaining access to someone else's Social Security number is often the fastest and surest route to accessing financial account information – and thus perpetrating identity theft.

Even if the use of Social Security numbers becomes strictly limited by law, the potential for fraud remains enormous. Most purveyors of bogus birth certificates also do a booming business in fake Social Security cards. Even more disturbing, perhaps, is this statistic from a Social Security Administration report issued in 1997; of the approximately 269 million Social Security numbers valid at that time, some 10 million were duplicates. Due to a combination of errors by the Social Security Administration and intentional fraud, 10 million Social Security numbers had actually been issued to two or more individuals, meaning they cannot be relied on as unique identifiers.

Immigration and Naturalization

Service Documents

A January 2002 report to Congress by the General Accounting Office (GAO), “Immigration and Benefit Fraud,” referred to May 1999 Congressional testimony that criminal aliens and terrorists manipulate the benefit application process in order to expand their illegal activities, including crimes of violence, narcotics trafficking, and terrorism, as well as entitlement fraud. Testifying before the Subcommittee on Immigration and

Claims of the House Judiciary Committee, Director of Immigration Services William Yates said that a “more problematic purpose of the benefit fraud is to facilitate the operation of criminal enterprises within the United States. . . . [T]he fraud is not the end point but rather the vehicle to support other illegal activities.” The GAO document also reported an increase in the scope and complexity of immigration benefit fraud in recent years, as well as in the abuse of various INS provisions regarding nonimmigrant visas, such as tourist and student visas, that can lead to permanent residency and ultimately to naturalization.

Even before it was revealed in March 2002 that two of the September 11 hijackers were issued student visas six months after the attacks, student visas were becoming increasingly suspect as identity documents. In November 2001, a State Department representative advised the ABA’s Account Opening Best Practices Group not to rely on student visas for identifying prospective customers, and the ABA’s January 2002 Industry Resource Guide “Identification and Verification of Accountholders” advises that “The many challenges associated with the visa and foreign passport identification

systems render them unacceptable for authentication purpose.”

Fortunately, a law signed in May 2002 by President Bush promises to enhance the security of visas and some foreign passports by late 2004. The Enhanced Border Security and Visa Entry Reform Act requires that, by October 26, 2004, foreign nationals wishing to enter the United States must have a tamper-proof, machine-readable visa containing a biometric identifier. Countries whose citizens currently do not require visas to enter the United States will be required to furnish tamper-proof, machine-readable passports containing biometric identifiers. As a byproduct of this Act, visas may become some of the most secure and reliable identity documents available.

Identification Issued by Foreign Governments

Section 326(b) of the USA PATRIOT Act requires the Secretary of the Treasury to make recommendations regarding what sort of identification foreign nationals should be required to provide to financial institutions before opening an account. These

recommendations were expected at the end of April, but have not yet been issued.

Because of the number of Mexican nationals living in the United States, one pressing need is a way for them to identify themselves in this country. The default answer currently appears to be an identity document, called a *matricula consular*, which can be issued by any of the 48 Mexican consulates in the United States and thus is relatively convenient for Mexican nationals in this country to obtain. For this reason, the *matricula consular* is gaining recognition with banks, businesses and police departments, most notably in California and the Southwest. So far, Albuquerque, New Mexico, Austin, Texas, and several California locales including Orange County and San Francisco have begun accepting the *matricula consular* as legal identification.

At least three major interstate financial institutions and some airlines have begun accepting the *matricula consular* as well. Financial institutions are generally requiring a second item, such as a passport or credit card, to open accounts, as well as either a Social Security or federal taxpayer-

identification number – although at least one accepts simply a signed Internal Revenue Service form that puts the home address of a nonresident immigrant on file with the IRS.

No state motor vehicle administration has yet begun accepting the *matricula consular* as identification. Realizing the need to accept some form of Mexican-issued identification, the AAMVA is investigating various documents issued by the Mexican government, including the *matricula consular*, passport and voter registration card.

In contrast to the United States – where voter registration cards are among the least secure and reliable documents – in Mexico and in many other countries where election fraud has historically been a concern, voter registration cards are issued under strictly controlled conditions and thus are among those countries' most secure and reliable documents. Visiting Mexico in April 2002 to evaluate the procedure for issuing voter registration cards, the AAMVA's Maxwell was impressed – more so than with the *matricula consular* issuing procedure, which he was scheduled to assess further in June 2002.

Florida's Captain David Myers is working with the Mexican consulates in Los Angeles and Chicago on the issuing procedure for a new, more secure *matricula consular*. This more secure form of the document will eventually be issued by consulates all around the United States.

Regarding which, if any, identification issued by other foreign governments may be accepted at DMVs in the future, Maxwell says “the onus will be on each government agency that issues an identification document to prove that it is secure and reliable.”★

CONSIDERING A NATIONAL IDENTIFICATION CARD

In light of the controversy over a national identification card (national ID), particularly since September 11, the National Research Council (NRC) of the National Academy of Sciences has produced a comprehensive analysis of the issue called “IDs – Not that Easy.” Rather than advocate for or against a national ID, the NRC study analyzes the current privacy/security climate and poses a series of questions that should be asked in contemplating such a system.

- What purpose would a national ID fulfill, and could that purpose be achieved in another way?
- What segment(s) of the population would participate in the national ID program; would participation be voluntary or mandatory; and how would participants’ identities be authenticated?
- What data would be gathered about individuals, and how would the accuracy and quality of the data be established and subsequently confirmed?
- Who would use the system – private sector,

federal, state and/or local government – and what uses would be allowed?

- What legal structures protect the system’s integrity and the subjects’ privacy?

Somewhat analogous to the debate over state versus national ID documents in the United States is the balancing act in the European Union between the driver-licensing requirements of specific countries and those of the entire EU. The licenses issued by European Union countries are interesting hybrids of country-specific and EU-wide documents, reflecting the complex attitudes that prevail toward security, privacy, and – as always in the EU – national sovereignty. According to Harold Kocken, former senior policy advisor in the Netherlands’ Ministry of Transport, Public Works and Water Management and current program director at the AAMVA, European Union Directive 91/439 specifies minimum standards for drivers licenses issued by EU members in four areas: administrative procedures; knowledge, skill and behavioral requirements; medical requirements; and document format. “The only reference to document/system security in EU Directive 91/439,” says Kocken, “is a brief instruction in the

administrative requirements to ‘avoid the risk of forgery.’” Interestingly, while 91/439’s document format requirements currently forbid the inclusion of a computer chip or magnetic stripe on drivers licenses, they also specify that the design of each license must allow room for the possible incorporation of a chip in the future.

Widely considered a potentially powerful identity document, smart cards that incorporate computer chips were somewhat called into question in a May 13, 2002 *New York Times* article reporting that two different teams of security researchers had succeeded in “cracking” some smart cards. One of the teams did so using easily available equipment costing under \$50. Both teams have proposed design changes that would protect smart cards from such attacks.★

ENHANCING SECURITY TODAY

Making identification documents more secure and reliable requires a three-part strategy:

1. The document-issuing process must ensure that the applicant's real identity is the one presented;
2. The document itself must be secure and tamper-resistant; and
3. There must be a way to determine that the document is valid and belongs to the person presenting it.

A number of security enhancements discussed earlier are currently under development and would meet one or both of the first two requirements. In the meantime, what resources are available today to help financial institutions determine whether identification documents and other information are valid and belong to the individuals presenting them?

Fortunately, a number of useful online and software products have emerged over the past few years to help financial institutions better verify the identities of prospective customers.

- Several products use one or more of these externally available tables to check the authenticity of information:
 - The Office of Foreign Asset Control (OFAC) list of foreign nationals, narcotics traffickers, terrorists, vessels, companies, or businesses on which economic sanctions have been imposed;
 - Directories of non-traceable phone numbers such as cell phones and pagers;
 - Drivers license codes and formats for all 50 states and the District of Columbia;
 - Charts that can help determine the validity of Social Security numbers and the likelihood that a particular number corresponds with an individual's age;
 - The death master file of Social Security numbers belonging to deceased individuals;
 - Mail drops such as post office boxes, mailbox rentals, hotels/motels, and prisons/correctional facilities, as well as voicemail/answering services;
 - Valid employer identification numbers;and
 - Correlated area codes, phone prefixes and zip codes.

- Some products also access information from check verification vendors, historical retail fraud lists and check printing services.
 - Credit bureaus that offer identity verification services check information against their own databases, which they generally augment with one or more of the external tables described above.
 - Another vendor uses external tables and a proprietary national data repository to detect invalid, inconsistent, duplicate or otherwise suspect information – two individuals with the same name and different addresses, for example, or with the same address and different names, or a Social Security number or date of birth used elsewhere in connection with another name. Tested using information about the nineteen September 11 hijackers that was released publicly following the attacks, this system was able to flag as “suspicious” eleven of the twelve hijackers for whom more information was available than simply a name.
 - One vendor offers a small desktop or handheld scanner that reads the magnetic stripe and 2-D barcode on a driver’s license to determine whether the license is authentic and whether the encoded information corresponds with the information printed on the license and with the physical characteristics of the individual presenting it. This product offers an optional thumbprint scanner.
 - There also is a growing selection of identification and authentication (I&A) products available, including digital signatures and public key infrastructure. Though developed primarily for authenticating the identities of parties to Internet transactions, these I&A solutions can be adapted for use in the physical world.*
- Clearly, although circumstances are not yet ideal, financial institutions have a wealth of identity verification options at their disposal today. Along with these options, financial institutions have the opportunity – perhaps even the implied obligation – to obtain and deploy an appropriate combination of

* For an overview of various I&A methods, refer to STAR’s June 2001 white paper, “Identification and Authentication: Challenges & Opportunities.” Like all STAR white papers, it is available online at www.star-systems.com (click on “news and statistics” and then on “industry research”).

available tools. It may be worth considering how customers, the market, policymakers and regulators might react if major security lapses in the future are followed by the recognition that some prevention tools were available but not used. The question, then, is how to choose which one is best for each institution's needs.

Part of the answer is that no single product is likely to suffice. Just as most military wars employ ground troops, air cover and naval support, combating identity fraud requires an arsenal of weapons. A comprehensive combination will enable institutions to greatly enhance their fraud prevention and risk reduction efforts, at the local branch level, across the nation and around the world. But first, each financial institution must evaluate its own needs before determining which combination of available products best fulfills them.

Once specific needs are defined, a list of selection criteria can be developed, based on those needs and on asking questions such as these:

- How “clean” is a particular database and how frequently is it updated?

- Does the vendor routinely “challenge” its product's performance and, if so, how?
- Does the vendor provide an employee training program?
- Where in the identity verification process does the product apply, and which functions does it – or does it not – perform?

As important as it is for each financial institution to select an effective combination of products for its needs, one of the most critical steps is to implement such a system without delay. Just as identity documents today are not perfect, neither is any identity verification system. With the range of tools currently available, however, every financial institution can find a solution adequate to its needs. And each one has a responsibility to do so – for its accountholders, its shareholders, and the U.S. financial system, and now, also, for America's national security.★

LOOKING AHEAD

Security has long been a cornerstone of financial institutions' commitment to fulfilling their responsibilities to account holders, shareholders and the American economy. The recent and continuing rise in identity theft – with more than 94,000 consumer complaints in less than two years, and financial institutions' losses projected to exceed \$8 billion by 2004 – has further underscored the importance of security, and particularly of verifying identities. And now, identity fraud and its tragic consequences have overlaid the new urgency of national security onto the continuing imperative of financial safety and soundness.

Financial institutions, charged by the USA PATRIOT Act with redoubling their long-standing efforts to combat money laundering and verify customers' identities, embrace the challenge. This challenge is made even more problematic by the almost ubiquitous lack of secure, reliable identity documents and the absence, so far, of useful counterterrorism information flowing from regulatory and law enforcement agencies. Financial institutions cannot fulfill their responsibilities in a vacuum or with inadequate tools.

The short-term solution is a combination of available products and technologies that can help financial institutions sort through the morass of identity documents and see through the fraudulent ones. Many of these products and technologies – most of which were developed for and used to some extent by financial institutions long before September 11 – may also be applicable to other security needs, such as verifying airline passengers' identities before boarding.

Over the longer term, however, the agencies that issue identity documents must implement more secure procedures that ensure reliable documents and protect national security. Already beginning in some quarters, this process must both expand and accelerate to encompass myriad critical needs in a rapidly evolving environment of national security challenges. ★

APPENDIX

KEY PROVISIONS OF THE USA PATRIOT ACT FOR FINANCIAL INSTITUTIONS

The provisions of the USAPATRIOT Act that affect financial institutions are found in Title III, the “International Money Laundering Abatement and Anti-terrorist Financing Act of 2001.” Three sections – 314, 326 and 352 – have particular impact on financial institutions and their security precautions.

Section 314: Cooperative Efforts to Deter Money Laundering

Section 314(a)(1) requires the Secretary of the Treasury to adopt regulations “encouraging regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities.”

Section 314(a)(2) specifies three types of information to be shared among and between

financial institutions and regulatory and law enforcement authorities:

- “matters specifically related to the finances of terrorist groups, the means by which terrorist groups transfer funds, . . . and the extent to which financial institutions in the United States are unwittingly involved . . . and . . . are at risk as a result”;
- “the relationship, particularly the financial relationship, between international narcotics traffickers and foreign terrorist organizations”; and
- “means of facilitating the identification of accounts and transactions involving terrorist groups and facilitating the exchange of information concerning such accounts and transactions between financial institutions and law enforcement organizations.”

Section 314(b) permits – but does not require – upon notice provided to the Secretary of the Treasury, “two or more financial institutions and any association of financial institutions [to] share information with one another regarding individuals,

entities, organizations, and countries suspected of possible terrorist or money laundering activities.” It further grants these institutions a broad exemption from liability “to any person under any law or regulation of the United States, any constitution, law, or regulation of any state or political subdivision hereof, or under any contract or other legally enforceable agreement, for such disclosure or for any failure to provide notice” to the subject of the disclosure.

Section 314(c) is more specific, stating compliance with the information provisions of this title “shall not constitute a violation of the provisions of title V of the Gramm-Leach-Bliley Act.”

Section 314(d) requires the Secretary of the Treasury to publish, at least semiannually, “a detailed analysis identifying patterns of suspicious activity and other investigative insights derived from suspicious activity reports and investigations conducted by Federal, State, and local law enforcement agencies” and to distribute it to financial institutions.

On February 26, 2002, the Department of the Treasury issued a proposed rule

implementing section 314(a) and an interim rule implementing section 314(b).

The proposed rule implementing section 314(a) gives federal law enforcement the ability to locate accounts of, and transactions conducted by, suspected terrorists or money launderers by providing their names and identifying information to the Financial Crimes Enforcement Network (FinCEN), which will then disseminate the information to financial institutions so that a check of accounts and transactions can be made. FinCEN’s new, highly secure network, the PATRIOT Act Communications System (PACS), will make it possible for federal law enforcement agencies and financial institutions to exchange vital information rapidly and securely, without compromising pending investigations. Section 314(a) will not be implemented until the final rule – which will consider comments received on the proposed rule during the comment period that closed on April 3 – is issued later this year.

The interim rule implementing section 314(b) requires financial institutions that decide to share information with each other

under this provision to file a yearly certification of intention, which can be completed online at FinCEN's Web page (www.treas.gov/fincen). It further requires them "to maintain adequate procedures to protect the security and confidentiality of such information" and to use it only "for identifying and reporting on activities that may involve terrorist or money laundering activities, or determining whether to close or maintain an account, or to engage in a transaction." This interim rule became effective immediately upon issuance.

Some financial institutions had anticipated that, under 314(a), federal regulators and law enforcement agencies would provide them with more than simply a list of accounts and transactions to be investigated and reported back on. They had hoped, for example, that the federal government would share an analysis of current crime trends. The absence of this from the proposed rule has engendered concern among many financial institutions that Treasury may envision information flow under 314(a) to be primarily one-way – from financial institutions to the federal government. This concern is reinforced by the fact that Treasury has

not yet distributed to financial institutions a detailed analysis identifying patterns of suspicious activity and other investigative insights, as 314(d) requires it to do twice each year.

Section 326: Verification of Identification

Section 326(a) requires that the Secretary of the Treasury prescribe minimum standards and procedures to ensure that financial institutions adequately verify the identity of customers opening new accounts. This must include maintaining records of the information used to verify persons' identity, including name, address and other identifying information, and consulting government lists of known or suspected terrorists or terrorist organizations to determine whether a person seeking to open an account appears on any such list. It will not be clear exactly what the new requirements are or how broadly this section defines the term "account" – for example, whether or not it encompasses credit card accounts – until the new standards and procedures are spelled out. The deadline for prescribing them is October 26, 2002.

Section 326(b) requires the Secretary of the Treasury to make recommendations to Congress on a number of practices, including: the most timely and effective way to require foreign nationals to provide financial institutions with appropriate and accurate identity information, comparable to that required of U.S. nationals; requiring foreign nationals to obtain an identification number similar to a Social Security or tax identification number before opening an account; and how financial institutions can review information maintained by government agencies to verify the identities of foreign nationals seeking to open accounts. These recommendations, which were due at the end of April, have not yet been issued.

Section 352: Anti-Money-Laundering Programs

Section 352 requires financial institutions to ensure that they have anti-money-laundering programs in place that include, at a minimum, the development of internal policies, procedures and controls; the designation of a compliance officer; an ongoing employee training program; and an

independent audit function to test programs. The deadline by which financial institutions were required to have these programs in place was April 26, 2002.

Section 352 gives the Secretary of the Treasury authority to prescribe additional minimum standards for financial institutions' anti-money-laundering programs, to exempt financial institutions that are not subject to the Currency and Foreign Transactions Reporting Act, and to consider the extent to which it applies to other financial institutions based on their size, location or activities. To date, no additional standards have been prescribed.★

Acknowledgments

STAR is grateful to the following organizations for contributing their time, wisdom and insights to this paper.

American Association of Motor Vehicle Administrators

America's Community Bankers

Fraudulent Identification Section, Bureau of Law Enforcement, Florida Division
of Alcoholic Beverages and Tobacco

IBM

National Association for Public Health Statistics and Information Systems

Privacy Times

United States Secret Service

