

# The Key to Stopping Identity Theft Is at the Tip of our Fingers

When people think of theft, they usually envision material things being stolen. However, imagine if someone stole your identity. They could charge on your credit cards, withdraw funds from your bank accounts, steal your mail, apply for credit in your name and eventually ruin your life. Identity theft occurs when a fraud artist assumes someone's identity for the purpose of purchasing goods and services, obtaining funds and gaining access to private information. This type of fraud is not difficult. It is relatively easy to obtain fraudulent paper and plastic identification along with knowledge of social security numbers and other personal identification information.

It's hard to believe, but with alarming frequency, criminals are assuming the identity of law-abiding citizens by misappropriating their personal information. Identity theft has become the Nation's fastest growing financial crime. The U.S. Public Interest Research Group, a private consumer advocacy group, estimates that up to 500,000 to 750,000 people are victims of identity theft each year.

Fraud is one of the fastest growing crimes in the United States and worldwide today. For example, bank robbery with a gun is minimal compared to bank robbery with a pen. In fact, based on the American Bankers Association year 2000 Fraud Survey Report, fraud losses among community banks increased almost 20 percent, while 100 percent of large institutions reported losses. In check fraud losses amount to approximately \$2.2 billion a year, twice the amount in 1997 according to the A.B.A.

## ***Who Pays for Fraud?***

We all do – in higher fees and growing costs of goods. However, the individual who suffers identity theft pays an even greater price in losing his/her identity and then trying for months to regain it. The US Public Interest Research Group says, “the average amount of time it took victims to resolve their cases was nearly 2 years (23 months). Victims who have not resolved their cases have been dealing with the problem for an average of 44 months and spend an average 175 hours and \$808 out-of-pocket (not including lawyer's fees) trying to fix the problem.

There are also the high administrative investments of designing and implementing systems that are used in the reduction of fraud exposure. At the same time that we need to eliminate fraud in financial institutions we also need to make it easier for the honest person to use the various financial delivery systems. We all know how difficult it is for a consumer to cash a check unless he/she has a deposit relationship with the financial institution.

Yet, fraud affects not only today's checks and credit cards but also tomorrow's electronic commerce and interactive banking. One solution would be to eliminate the acceptance of checks and credit cards across the board and only accept financial instruments from people we know. However, this solution is unrealistic.

### ***We Ourselves Can Stop Identity Theft***

Through the use of positive biometric user authentication systems, identity theft can be virtually eliminated. Yes, positive user authentication through the use of biometrics is the key for our payment systems. Without it, the financial industry can and will suffer substantial fraud losses in the electronic delivery systems of the future. Likewise, consumers will suffer irretrievable damage through identity theft. In the past, a consumer completed his or her transaction in person through a teller or clerk in a store. That was a form of biometric identification. That teller knew you. However, in the future, most transactions will be faceless, completed without human interface, making it open season for the fraud artist.

Today, the consumer relies upon bankcards, PINs, passwords, possession of identity cards, a Driver's License, a key or knowledge of his/her social security number as a means to authenticate himself/herself. Unfortunately, every one of these can be compromised through identity theft. But, nobody can steal your biometrics. After all, only you are you.

### ***The Best Biometric Authentication Solution***

Although positive user authentication through biometrics is the key, it must be easy to use and cost-effective: Therefore, finger imaging is the efficient solution.

Finger imaging is the logical choice because –

- ? Fingerprints are an Internationally recognized form of Identification
- ? Fingerprints do not change over time.
- ? Fingerprints can stop unauthorized access.
- ? All fingers are totally unique to each person and we all have these ten identifiers.
- ? Fingers are quick and easy to use. We don't leave our fingers at home or in the car.
- ? Law enforcement uses and respect fingerprinting systems. Thieves are afraid of them.
- ? Fingerprints are a low cost solution.
- ? Fingerprints protect privacy. They tell nothing about an individual other than who they belong to.

### **Finger Image Systems are Popular**

Fingerprinting systems are already used in a myriad of applications worldwide. You will find them at Banks, the FBI's Criminal Justice Information Services Center, many state Department of Motor Vehicles, business, government facilities and on personal computers. In 1973, several banks in California implemented a fingerprinting program with positive results. At the height of the program in the late 1970s, banks in 20 states were using some form of identity verification for non-customers. The practice lasted through the mid-1980s and, then, began to decline. However, with the ever-present threat of fraudulent checks and identity theft, many banks re-instituted their fingerprinting policies. The reason was simple.

Several years ago, the American Bankers Association (ABA) identified a substantial increase in fraudulent checks. They investigated several technology alternatives that would reduce fraud for their association member's depositors. They quickly determined that a fingerprint would be their most effective deterrent in stopping check fraud losses. Thus, they implemented a program called Touch Signature®. The Identicator Touch Signature finger imaging system has been implemented nationally in most banks that require verification of non-customers. These Identicator finger pads differ from the days of old in that they leave a black print on the check but not on the fingers. Customers can easily remove any remaining residue by rubbing the thumb and index finger together.

The Touch Signature program is simple. When a non-customer presents a check for payment, in addition to the regular forms of identification, the individual is asked to place a fingerprint on the front of the check. Of course, criminals don't want to supply their fingerprint because it can be used as evidence against them if the check is fraudulent. They are deterred from writing bad checks.

"Using thumbprinting is a tremendous deterrent to criminals cashing benefits checks," said John Hall, a spokesman for the American Bankers Association (ABA). "It's been highly successful." Several banks have reported measurable results as high as 72 percent loss reduction in the first year of implementing the program. The program has been such a deterrent in several banks that there was an overt migration of thieves to non-participating financial institutions. Banks previously unscathed by check fraud found themselves experiencing rapidly rising losses. Subsequent implementation of the program by some of these banks almost immediately reduced losses to near zero.

Identification isn't the issue. It's a matter of deterrence and verification. By having the Touch Signature system, banks and merchants are not attempting to identify everyone who comes in; rather they are attempting to deter would-be fraud artists and verify identity of the person only if a fraud has been committed.

The results of the programs are astounding:

- Eighty-five percent of the banks that monitored check fraud losses by non-customer transactions reported a reduction in losses.
- Twenty-one percent of banks reported a reduction of up to 20%, 43% of banks reported a 20-50% reduction, and 21% of banks reduced losses by more than 50%.
- Banks reporting reduction in losses- 85%
- Banks implementing bank wide (as opposed to selected branches) 100%
- Banks providing notice of fingerprint requirement 94%
- Banks receiving ten or fewer complaints 94%

The Touch Signature program is simple. When a non-customer presents a check for payment, in addition to the regular forms of identification, the individual is asked to place a fingerprint on the front of the check. Of course, criminals don't want to supply their fingerprint because it can be used as evidence against them if the check is fraudulent. They are deterred from writing bad checks.

"Using thumbprinting is a tremendous deterrent to criminals cashing benefits checks," said John Hall, of the ABA. "It's been highly successful." Several banks have reported measurable results as high as 72 percent loss reduction in the first year of implementing the program. The program has been such a deterrent in several banks that there was an overt migration of thieves to non-participating financial institutions. Banks previously unscathed by check fraud found themselves experiencing rapidly rising losses.

The pads have proven very valuable to other types of merchants as well. Identifier customers now include grocery stores like Kroger, Winn-Dixie, Ralph's; retailers like Wal-Mart and Lowes Home Improvement Stores, and many others such as casinos, check cashing stores, warehouses, convenient stores, anywhere checks are cashed. According to Franchise Coordinator Terry Giancaterino, "These small compact inkless pads have been the most efficient of the various types of print identification products. They are simple to use and very inexpensive. The unique inkless method of Touch Signature thumbprinting really does act as a deterrent to the bad check artist. It reduces losses, offers protection to our honest customers and is recognized by law enforcement officials for providing protection to our owners."

### ***Why it Works***

According to the Bank Security and Fraud Prevention publication of the ABA: *The fingerprinting system is seen both as a deterrent and a method of simplifying banks' responsibilities when it comes to prosecution. Anyone who has ever had their identity taken knows that you're in a position of proving you're innocent, rather than guilty. Having prints on these documents serves this purpose. We have major fraud groups that are highly mobile moving throughout this country. This program is a proactive, joint effort that has the true relationships: to know with whom we are dealing and to have positive proof that we are dealing with the right person.*

The Touch Signature Program is simple, low-cost and saves time for the government, the financial industry and the consumer. Best of all, it works. Law Enforcement Law enforcement agencies have greeted the fingerprint program with enthusiasm. Though banks take it upon themselves to implement a fingerprinting program, law enforcement agencies have become increasingly supportive since their beginning. Many have placed added pressure on banks by expressing a greater willingness to accept check cases in which a fingerprint is present. In fact, 89% of reporting banks said that law enforcement agencies were supportive of their fingerprinting programs. Several measures have been implemented into law in order to prevent the theft of personal identities. Previously, the person whose identity was stolen was not recognized as a crime victim by the law.

An “Identity Theft” bill recently passed in Congress makes identity theft a federal crime and provides penalties for those who engage in it. This bill, introduced by Senator Jon Kyl (R-Arizona), extends the current federal prohibition against theft of personal documents to theft of the information itself, since, in the electronic age, much personal information is accessible via computer and the Internet. This bill also allows restitution for victims for identifiable losses as well as for expenses related to clearing their name and credit rating. In his testimony before Chairman Kyl’s Senate Subcommittee, James Bauer of the Secret Service stated, “Currently, law enforcement must wait for an overt fraudulent act or creation of a fraudulent document before it can intercede in a case solely involving identity fraud. Establishing identity theft as a criminal violation, as the Kyl bill does, would enable law enforcement to prevent the fraud before it starts. It would be a proactive answer to what is now being handled in a reactive manner.”

The Identity Theft and Assumption Deterrence Act of 1998 was passed through Congress on October 30, 1998. Steve Berry, Cellular Telecommunications Industry Association (CTIA) senior vice president of congressional affairs, said, “The new Identity Theft Law will make it easier for the American justice system to find and punish those criminals who steal other people’s names and identification information in order to reap financial gain. With the force of the federal criminal justice system behind the law, new penalties of up to three years imprisonment and fines up to \$250,000 will protect innocent consumers.”

However, it remains more important and less expensive to stop identity theft before it happens than to prosecute it afterwards. That’s why businesses must proactively guard against it. With e-commerce becoming more and more prevalent, today’s need is minute in comparison to the future’s.

### ***The Move Toward Electronic Money***

The financial industry is definitely moving towards electronic transfers. There is a significant increase in the use of smart cards, especially in Europe, which is just now coming into the United States. Relationship smart cards are not only used for payment but for other uses as well. For instance, the U.S. General Services Administration (GSA) initiative calls for one card to be used for travel, payment, data access and physical access. In the GSA initiative, there is also the option to use biometrics in place of PINs. Of the five financial institutions that were recently selected as integrators, three offered finger imaging and the others integrated no biometrics at all. If the key is to produce positive user authentication to reduce fraud and eliminate identity theft, while at the same time expanding customer services, there is little or no reason not to include finger imaging. User authentication links the transaction to the legitimate customer.

### ***Put our Finger on the Solution***

The bottom line is that we need protection from fraud and identity theft. This is important, not only to ensure that one’s good name is not damaged, but also to ensure that one’s financial resources and personal data cannot be attacked. This protection is easily achieved with finger imaging, which provides essential protection for law-abiding citizens, government and business. We will not successfully move into the future of electronic cash without it.