

# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

## **FINANCIAL IDENTITY THEFT: PREVENTION AND CONSUMER ASSISTANCE**

**MAY 2003  
UPDATED JUNE 2003**

**A PUBLICATION OF THE BITS FRAUD REDUCTION STEERING COMMITTEE**

BITS  
805 15<sup>TH</sup> STREET NW, SUITE 600  
WASHINGTON DC 20005  
(202) 289-4322  
[WWW.BITSINFO.ORG](http://WWW.BITSINFO.ORG)

# FINANCIAL IDENTITY THEFT: PREVENTION AND CONSUMER ASSISTANCE

## TABLE OF CONTENTS

<b>THE BITS FRAUD REDUCTION STEERING COMMITTEE</b> .....	3
<b>ABOUT BITS</b> .....	4
<b>I. EXECUTIVE SUMMARY</b> .....	5
<b>II. FINANCIAL INSTITUTION VOLUNTARY GUIDELINES: IDENTITY THEFT PREVENTION AND VICTIM ASSISTANCE</b> .....	6
<b>III. OVERVIEW OF THE PROJECT</b> .....	7
A. Background.....	7
B. Project Organization and White Paper Availability.....	7
C. Data Gathering.....	7
<b>IV. DEFINITION AND QUANTIFICATION OF THE PROBLEM</b> .....	8
A. Defining Identity Theft.....	8
B. Defining the Environment.....	8
C. Crime Report Statistics.....	10
D. Federal Trade Commission Initiative.....	12
E. Individual Criminal Events and Organized Gangs.....	13
F. Methodologies for Capturing and Using Personal Information.....	15
<b>V. CURRENT AND PROPOSED LEGISLATION</b> .....	17
A. Overview of Existing Federal Law.....	17
B. Proposed Federal Legislation.....	17
C. Overview of State Law.....	18
<b>VI. CURRENT PRACTICES AND RECOMMENDED STRATEGIES</b> .....	19
A. Current Industry Countermeasures and Mitigation Processes.....	19
B. Financial Institution Centralized Approach to Identity Theft Assistance.....	20
C. Financial Institution Voluntary Guidelines.....	21
D. Financial Institutions' Control Systems and Identity Theft Prevention Tools.....	23
E. Credit Bureaus' Identity Theft Prevention Tools and Consumer Assistance Practices.....	24
<b>VII. FRAUD PREVENTION TECHNOLOGIES</b> .....	29
A. Authentication Technologies and Processes.....	29
B. Information Management Technology.....	33
C. Information Security.....	36
<b>VIII. STRATEGIC PARTNERSHIPS</b> .....	37
A. Financial Institutions.....	37
B. Financial Institutions, Credit Bureaus and Law Enforcement.....	37
C. Technology Developers.....	38
<b>IX. CONSUMER AWARENESS AND EDUCATION</b> .....	39
A. Resources.....	39
B. Protective Steps for Consumers.....	39
<b>X. INTERNATIONAL (UK) CASE EXAMPLE: APACS</b> .....	44
<b>XI. RECOMMENDATIONS AND NEXT STEPS</b> .....	46
A. General Recommendations and Next Steps.....	46
B. Know Your Customer Practices.....	46
C. Know Your Employee Practices.....	48
<b>XII. CONCLUSION</b> .....	51

## **THE BITS FRAUD REDUCTION STEERING COMMITTEE**

**CO-CHAIRS:** Shirley Inscoe, Wachovia  
Bob Jones, FleetBoston

**STAFF:** Robin M. Slade, BITS

### **THE BITS FRAUD REDUCTION STEERING COMMITTEE WAS CREATED TO:**

- Reduce payment-related fraud losses.
- Secure a critical mass of financial institutions to participate in a shared account database and standardized data collection process.
- Identify successful strategies for reducing fraud and make those strategies available to the industry.
- Assess fraud risk exposure to electronification and develop strategies to minimize losses

### **WORKING GROUPS UNDER THE BITS FRAUD REDUCTION PROGRAM INCLUDE:**

- **Collections Working Group** – Chair: Jim Regan, The Bank of New York
- **Debit Card/ATM Fraud** – Chair: Laura Sullivan, Citizens Bank
- **Electronification** – Chair: Dick Clausen, Bank of America
- **Identity Theft** – Chair: Joe Triano, Citigroup Inc.
- **Internet Fraud** – Chair: Gayle Helm, Wells Fargo & Co.
- **Legal & Regulatory** – Chair: Maureen Wharton, J.P. Morgan Chase & Co.
- **Shared Databases** – Chair: Jan Otwell, J.P. Morgan Chase & Co.
- **Statistics** – Chair: Rachel Floars, BB&T
- **Successful Strategies** – Chair: Peter Baldassaro, Hibernia Corp.

### **INSTITUTIONS THAT PARTICIPATED IN DRAFTING THIS WHITE PAPER**

AllFirst Financial, Inc.	FleetBoston Financial Corporation
Association for Payment Clearing Services (APACS)	Harris Bank
Bank of America Corporation	Hibernia Corporation
Bank of New York Company, Inc.	J.P. Morgan Chase & Co.
BANK ONE CORPORATION	Mellon Financial Corporation
Citigroup Inc.	TransUnion
Comerica Incorporated	US Bank
Equifax	Wachovia
Experian	Washington Mutual, Inc.
FMR Corp. (Fidelity Investments)	Wells Fargo & Company
Firststar Bank	

## **ABOUT BITS**

BITS, the Technology Group for the Financial Services Roundtable, was created in 1996 to foster the growth of electronic commerce, emerging technologies, and payments for the benefit of financial institutions and their customers. Members of this non-profit industry consortium include the CEOs and CIOs of the 100 largest integrated financial institutions in the United States. Throughout its work, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. Major areas of emphasis are security, crisis management coordination, payments strategies, privacy, managing of outsourcers, fraud reduction, and operational risk. BITS promotes the development of superior, market-driven technologies to strengthen the financial institution-customer relationship, to leverage resources and infrastructure across the industry, and to maintain the industry's position at the heart of the payments system. BITS' Board of Directors is composed of the Chairmen and CEOs of some of the largest U.S. financial services holding companies as well as representatives of the American Bankers Association and the Independent Community Bankers of America.

## **BITS**

805 FIFTEENTH STREET NW, SUITE 600

WASHINGTON, DC 20005

[WWW.BITSINFO.ORG](http://WWW.BITSINFO.ORG)

(202) 289-4322

## I. EXECUTIVE SUMMARY

This white paper was created by specialists in fraud management and identity theft under the direction of the BITS Identity Theft Working Group. The Group's purpose is to address identity theft, a specific and costly subset of the overall fraud threats faced by financial institutions.

Identity theft, defined here as “the unlawful capture and/or use of another person's identifiers to impersonate him or her in the commission of a crime to gain financial benefit,” is one of the most serious types of fraud. It can cause extreme distress to victims and, if it continues at its current growth rate, will cost U.S. financial institutions \$8 billion annually by 2005.<sup>1</sup> Clearly, it is worthy of serious attention by financial institutions of all sizes, as well as by other businesses, government agencies, and consumers. The topic has emerged as a pivotal part of discussions with the administration and Members of Congress about reauthorization of the Fair Credit Reporting Act and continuation of uniform national standards for treatment of customer information.

Because a consistent understanding of the problem is essential to finding solutions, this paper outlines the full identity theft landscape, establishing key terms as well as identifying factors that contribute to identity theft. Background about the legislative and policy environment, including existing and proposed laws, is provided as well.

The paper also provides a detailed overview of the technologies, tools and processes that financial institutions are using today to combat identity theft—and offers recommendations for voluntary guidelines (see next page) by which the financial services industry will work to prevent identity theft and assist those who fall victim to it. Preventive measures include precautions taken at account opening, tools for verifying transactions, and employee training. Considered particularly effective in preventing identity theft are authentication methods, which verify the customer's identity before granting access to account information. Various authentication methods are defined and discussed in terms of their proliferation, effectiveness, and technological maturity. Relevant credit bureau mitigation practices, which were provided to BITS from credit bureau representatives, are also outlined.

The paper also includes a discussion of mitigation efforts outside of individual institutions. Among those are consumer awareness and education efforts and relationships with other interested parties and institutions. It is the perspective of the authors that no one technology, nor one piece of legislation, can possibly solve this complex and growing problem. Financial institutions must work together, with other businesses and with their customers, to make the current environment, in which identity thieves thrive, into one in which stealing an identity is extremely difficult and carries with it serious consequences.

Identity theft affects all financial institutions and causes serious harm to their customers. The financial services industry is taking steps to curb the growth of this kind of crime and to assist those who may fall victim to it. It is the authors' hope that the information contained here will help educate all stakeholders on how the problem can best be addressed and help provide a safer environment for everyone.

---

<sup>1</sup> Celent Communications, *Identity Theft: Impact on the Financial Services Industry*, September 2001.



**FRAUD REDUCTION GUIDELINES  
STRATEGIES FOR IDENTITY THEFT PREVENTION AND VICTIM ASSISTANCE**

**MISSION**

Members of The Financial Services Roundtable and BITS are committed to creating and implementing a set of efficient, effective and consistent procedures to restore a victim's financial identity and to prevent ongoing incidences of identity theft. To that end we, the participating financial institutions, agree to share and implement the following successful strategies.

**PREVENTION**

**Participating financial institutions agree to:**

- Share on an ongoing basis successful fraud prevention strategies in areas that include:
  - Account opening and online transactions
  - Authentication
  - Monitoring Controls
  - Loss tracking and reporting
  - Personnel training to detect suspicious activity
- Provide educational materials to our customers to assist them in protecting their financial identities.
- Provide data relating to identity theft to appropriate law enforcement agencies for trending and analysis of patterns of fraudulent activities and prosecution of fraud rings.
- Join with industry associations and organizations, and consider joining the Identity Theft Assistance Center (ITAC), if such a Center is established, to analyze and pool identity theft data for law enforcement purposes.

**VICTIM ASSISTANCE**

**Participating financial institutions agree to:**

- Establish an internal system that provides victims a single point of contact within the financial institution.
- Provide each victim with educational materials to assist in preventing further instances.
- Utilize an industry-wide Uniform Affidavit.
- Establish a system for disseminating the Uniform Affidavit, as appropriate, to law enforcement, industry organizations, and others, including an ITAC, if such a Center is established and participation is elected.
- While reserving the right to receive additional information from the victim, receive and use a completed Uniform Affidavit from other financial institutions.
- Upon receipt of a completed Uniform Affidavit, contact the victim to seek resolution of affected accounts within their own institutions.

### **III. OVERVIEW OF THE PROJECT**

#### **A. Background**

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies.

Fraud-related crimes involving identity theft are on the rise. This activity has been growing to alarming proportions in the U.S. and internationally. New technologies and the ubiquity of the Internet are among the factors. Collecting personal information has become easier to do, allowing criminals to impersonate individuals and engage in a variety of fraud schemes. With the advent of e-commerce, criminals now have the opportunity to operate across international borders and at Internet speed, while remaining anonymous. However, identity theft is not just an e-commerce problem. It affects all aspects of financial services and commerce.

The BITS Fraud Reduction Steering Committee (FRSC) was asked to examine the problem of identity theft as it relates to financial institutions. This paper addresses the historical issues and growth of identity theft, current and proposed legislation, financial institution and credit bureau practices, technology, authentication models, ways to monitor for signs of identity theft, voluntary guidelines for the industry, the UK's approach to the problem, and consumer awareness and self protection tips.

The *Financial Institution Voluntary Guidelines: Identity Theft Prevention and Victim Assistance* recommended here are intended to suggest ways to prevent identity theft and to assist those who become its victims. These Guidelines were developed by the BITS Fraud Reduction Steering Committee in cooperation with The Financial Services Roundtable.

This white paper was created in order to create the fullest picture possible of the state of identity theft today, the practices being used to prevent it, and the importance of a broad-based cooperative effort in order to successfully address it.

#### **B. Project Organization and White Paper Availability**

This white paper was created under the direction of the BITS Identity Theft Working Group and the BITS Fraud Reduction Steering Committee. Project participants are considered to be specialists in identity theft and represent financial institution, credit bureaus and industry organizations. The paper is being distributed to the BITS membership and will be made available to other interested parties. Because of its value as an educational tool, it is available on the BITS Web site, [www.bitsinfo.org](http://www.bitsinfo.org), in the public area under Fraud Reduction, Publications.

#### **C. Data Gathering**

The data-gathering process was completed by project teams created from participating organizations within the membership of BITS and The Financial Services Roundtable. The teams volunteered to comment on the quantification of the problem, current practices, and

industry recommendations. Each team's response was vetted with the entire group of participants. All of the information gathered is included in this document.

## IV. DEFINITION AND QUANTIFICATION OF THE PROBLEM

### A. Defining Identity Theft

Identity theft, also called “identity fraud,” is clearly an issue that has the attention of financial institutions, credit bureaus, federal and state legislators, law enforcement, and most certainly consumers. Identity theft is the unlawful capture and use of another's personal identifying information (name, address, date of birth, Social Security number, account information, mother's maiden name or other family identifiers). Some of this information is static, such as date of birth, Social Security number or account information, while other identifiers are more dynamic and can change, such as name (legal name change), and address. This type of identity theft, in which the identifiers belong to a real person, is called “true identity theft,” and is different from creating a false identity, in which there is no “real person” behind the identity. Although there may be inadvertent capture of some true identity information (last name, date of birth, etc.), the target for a true identity thief is the financial history associated with a real person, not just the identity. **Therefore, identity theft as discussed here is directed at true identity (impersonation) for the purpose of committing financial or other crimes.**

United States law 18 USC-1028 defines identity theft as “knowingly [transferring] or [using], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” Other definitions used by various organizations may be appropriate as well. However, it is suggested that the following short definition be used for the purpose of understanding the issues captured here: **Identity theft is the unlawful capture and/or use of another person’s identifiers to impersonate him or her in the commission of a crime or to gain financial benefit.**

### B. Defining the Environment

Data show that there is good reason for financial institutions’ and consumers’ heightened concern. Identity theft accounted for 42 percent of all consumer fraud complaints received by the Federal Trade Commission (FTC) in 2001, and Celent Communications predicts that identity theft will more than triple by 2005—from 500,000 incidents in 2000 to 1.7 million in 2005. Also according to Celent, the cost to financial institutions is expected to increase by 30 percent per year, totaling \$8 billion by 2005—48 percent of this cost is attributed to direct loss from fraud.<sup>2</sup>

---

<sup>2</sup> Celent Communications, *Identity Theft: Impact on the Financial Services Industry*, September 2001.

The ABA 2002 Deposit Account Fraud Survey Report found that four in 10 (39.3 percent) financial institution respondents cited identity fraud as the number one threat against the industry in the next 12 months.<sup>3</sup> In 2001, four percent of super-regional/money center banks' and 34 percent of community banks' total check-related losses were attributed to identity fraud.

---

**2001 Identity Fraud Losses Per Bank\*  
(Bank Assets in Million Dollars)**

---

	<b>Under 500</b>	<b>500 - 4,999</b>	<b>5,000 – 49,999</b>	<b>50,000 or More</b>
Number of cases				
Median	1	3	41	143
Minimum	1	1	4	9
Maximum	30	68	1,291	12,603
Total dollar value				
Median	\$1,820	\$10,000	\$136,674	\$299,486
Minimum	20	150	1968	9,996
Maximum	91,124	186,785	1,726,997	21,825,595
<i>Number of banks responding</i>	<i>37</i>	<i>21</i>	<i>10</i>	<i>10</i>
Identity fraud losses as a percentage of actual gross check-related losses				
Based on number of cases	27.1%	20.9%	12.0%	1.8%
Based on dollar amount	33.6%	19.3%	13.3%	3.7%

---

\*Identity fraud includes account takeover, true name fraud, and fictitious person.

Source: ABA Deposit Account Fraud Survey Report

Further, a March 2002 General Accounting Office (GAO) report, *Identity Theft: Prevalence and Cost Appear to be Growing*, reported that banks are increasingly concerned about the growing sophistication of identity thieves, and that department staffing has grown over the last few years to address increasing fraud losses.<sup>4</sup>

The GAO report also noted a shift in federal agencies away from “street crime” to high-dollar, community-impact cases. Because of this shift, the number of identity theft cases that have been closed has decreased from 8,498 in 1998 to 7,071 in 2000. Because their resources are limited, law enforcement will not address the problem unless it is of a substantial dollar amount.

---

<sup>3</sup> American Bankers Association, *ABA Deposit Account Fraud Survey Report* (2002).

<sup>4</sup> U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: March 2002).

### C. Crime Report Statistics

According to the 2002 GAO report, identity theft-related statistics from the Executive Office for U.S. Attorneys and the FBI:

- The number of cases filed under the Identity Theft Assumptions and Deterrence Act, 18 U.S.C. § 1028, more than doubled from 314 in 1996 to 775 in 2000.
- The number of cases filed under the Fraud and Related Activity in Connection with Access Devices, 18 U.S.C. § 1029, reflects a general decrease, and the most recent figure—703 cases in 2000—is considerably lower than the 924 cases filed in 1996.
- The number of cases filed under the Social Security Act, 42 U.S.C. § 408, reflects a general increase. The number of cases filed increased substantially in 1998, when compared with the previous two years. The number of cases filed in 2000 was more than double the number filed in 1996.

Further, FBI statistics cited in the GAO report show that cases involving identity theft typically are classified by the crimes committed using the stolen fraudulent identity—classified, for example, as bank fraud, wire fraud, or mail fraud.

---

#### FBI Accomplishments Under Identity Theft-Related Statutes, Fiscal Years 1996 through 2001

---

Statute	1996	1997	1998	1999	2000	2001 <sup>5</sup>
18 U.S.C. § 1028 (Identification documents)						
Indictments and informations <sup>6</sup>	33	33	22	55	99	49
Arrests	24	17	20	28	40	43
Convictions	33	27	17	21	50	29
18 U.S.C. § 1029 (Access devices)						
Indictments and informations	90	95	114	96	125	39
Arrests	38	60	78	69	90	35
Convictions	60	80	77	105	74	35
18 U.S.C. § 1014 (Loan and credit applications)						
Indictments and informations	311	290	235	189	206	94
Arrests	58	62	72	38	85	38
Convictions	304	242	170	146	121	50
18 U.S.C. § 1344 (bank fraud)						
Indictments and informations	1,225	1,159	1,305	1,492	1,481	626
Arrests	311	468	579	691	645	311
Convictions	1,121	896	983	1,047	1,112	449
18 U.S.C. § 408 (SSN misuse)						
Indictments and informations	85	75	97	119	98	40
Arrests	25	15	40	48	62	22

---

<sup>5</sup> Fiscal year 2001 numbers are as of April 10, 2001.

<sup>6</sup> Generally, an indictment is an accusation presented in writing by a grand jury, charging a person for some criminal offense, whereas “informations” are presented by a competent public officer on his or her oath of office.

Convictions	61	50	62	64	68	23
18 U.S.C. § 1644 (fraudulent use of credit cards)						
Indictments and informations	11	1	1	1	1	1
Arrests	2	0	1	0	0	2
Convictions	5	2	2	0	0	1

Source: FBI data.

Secret Service data cited in the GAO report showed that the number of arrests decreased 28 percent from 1998 to 2000, and the number of cases closed dropped 37 percent. However, the average actual losses to victims in closed cases rose 71 percent from 1998 to 2000. The average fraud losses prevented rose 48 percent from 1998 to 1999 and rose an additional 101 percent from 1999 to 2000.

### Secret Service Data on Identity Theft-Related Arrests, Cases Closed, and Dollar Losses in Fiscal Years 1998 through 2000

Data Category	1998	1999	2000
Arrests	4,421	3,814	3,163
Cases closed <sup>7</sup>	8,489	7,071	5,379
Average actual losses to victims in cases closed <sup>8</sup>	\$26,922	\$38,078	\$46,119
Average fraud losses prevented in cases closed <sup>9</sup>	\$73,382	\$108,476	\$217,696

Source: Secret Service Data

The Financial Crimes Enforcement Network (FinCEN), which is responsible for the collection of suspicious activity reports (SARs) used to assist law enforcement in detecting and prosecuting financial crimes, reported that from April 1996 through November 2000 a total of 490,595 filings were received. Of this total, 1,030 SARs reported identity theft.

As reported in the GAO report, the U.S. Postal Inspection Service noted that identity theft is a growing trend:

Inspection Service identity theft investigations increased by 67 percent since last year. Identity theft occurs when mail is stolen for the personal information it contains, which criminals use to fraudulently order credit cards, checks or other financial instruments. Mail theft may go unreported if the thief looks for mail containing items such as a credit card payment, and copies personal identifiers and credit card and/or bank account information, and reseals the envelope and returns it to the mailroom. Checks and credit cards may

<sup>7</sup> Cases can be closed for a variety of reasons, such as completion of judicial action, declination to prosecute by the Office of the United States Attorney, or a determination that insufficient evidence exists to identify or charge a suspect.

<sup>8</sup> As defined by the Secret Service, “actual losses” are the amounts of money, goods, or services that were obtained by the criminal or group of criminals through the commission of the crime.

<sup>9</sup> As defined by the Secret Service, “fraud losses prevented” is the difference between potential losses and actual losses. The Service defined “potential losses” as the amounts of money, goods, or services that the criminal or group of criminals was trying to obtain through the commission of the crime.

then be ordered in the victim's name. Some identity thieves rent private mailboxes at commercial receiving agencies so he or she can receive the fraudulently obtained cards and checks anonymously.

---

**Postal Inspection Service Identity-Theft-Related Arrests, Fiscal Years 1996 through 2001**

---

Fiscal Year	Number of Arrests
1996	1,287
1997	1,226
1998	1,122
1999	1,267
2000	1,722
2001 (through June 30, 2001)	1,752

---

Source: U.S. Postal Inspection Service

**D. Federal Trade Commission Initiative**

The FTC, under the Identity Theft and Assumption Deterrence Act of 1998, has established an Identity Theft Data Clearinghouse, a depository of consumer complaints about identity theft. The FTC does not compile criminal cases, but rather is a resource for assisting victims in resolving the problems that can result from identity theft. The FTC's Consumer Sentinel network enables access to consumer data by law enforcement agencies to coordinate efforts and consolidate fraudulent activities.

The FTC has also developed an ID Theft Affidavit to be used to alert financial institutions and other companies where a fraudulent account has been opened in the consumer's name. Many financial institutions and companies accept this Affidavit although it is not used uniformly given some inherent limitations in its current form. Under the auspices of the BITS Fraud Reduction Steering Committee, BITS and The Financial Services Roundtable are currently working to resolve these limitations, with the encouragement and cooperation of the FTC. We anticipate completion in May 2003 of a new Uniform Affidavit, based on the FTC's, that will be widely adopted and used throughout the financial services industry. The BITS/FSR Identity Theft Uniform Affidavit is likely to be adopted by the FTC as well and posted on its Web site. A copy of the current Affidavit and a list of participating organizations can be found at [www.consumer.gov/idtheft/affidavit.htm](http://www.consumer.gov/idtheft/affidavit.htm).

From November 1999 through September 2001, the FTC's Identity Theft Data Clearinghouse has received 94,101 complaints from victims. Of this amount, 16,784 complaints were transferred to the FTC from the Social Security Administration. In November 1999, the FTC reported an average of 445 calls per week. By December 2001, the weekly average was about 3,000 calls. However, the FTC noted that the increase of calls may not be attributed to increases in incidence, but rather an increase in customer awareness.

---

**Number of Identity Theft Complaints FTC Received (November 1999 through September 2001) from Leading States**

---

<b>State</b>	<b>Number of Complaints</b>	<b>Percentage</b>
California	16,147	17.2
New York	8,219	8.7
Texas	6,775	7.2
Florida	6,309	6.7
Illinois	4,145	4.4
<b>Subtotal</b>	<b>41,595</b>	<b>44.2</b>
Remaining states and the District of Columbia	45,175	48.0
Other <sup>10</sup>	7,330	7.8
<b>Total<sup>11</sup></b>	<b>94,100</b>	<b>100.0</b>

---

Source: FTC's Identity Theft Data Clearinghouse

**E. Individual Criminal Events and Organized Gangs**

Like many victims of financial crimes, identity theft victims may never know exactly how their identity and personal financial information was compromised and who is responsible. According to the FTC, in more than 61 percent of reported incidents the method used to obtain the victim's information is not known. In only 20 percent of reported incidents, the methods used to obtain information can be tied to specific occurrences (burglaries, thefts, telephone/Internet solicitations, etc.) and/or involve a relationship the suspect had with the victim.

Recent trends indicate that organized criminal gangs are involved in this type of crime. Many financial institutions have seen an increase in incidents involving organized groups, which are often internationally based. These groups obtain enough personal and financial information about an individual to allow them to attempt to deplete account balances through a variety of methods, including unauthorized wire transfer of funds, counterfeit checks, and fraudulent withdrawals. These individuals have not only stolen identities, they have also acquired sufficient information regarding the internal systems and operations of financial institutions to be moderately successful.

---

<sup>10</sup> "Other" refers to identity theft complaints made from U.S. territories and other countries, as well as complaints made by consumers who do not list their location.

<sup>11</sup> The total includes identity theft complaints forwarded from SSA/OIG to the FTC. The total does not include approximately 36,274 calls from consumers who were not identity theft victims but were seeking information about identity theft.

**Identity Theft Complaints FTC Received (Nov. 1999 through Sept. 2001) and Categories of Methods Suspects Used to Obtain Personal Information**

<b>Method suspects used to obtain information</b>	<b>Number of Complaints</b>	<b>Percentage</b>
Method not known	58,078	61.7
Information not collected (non-FTC data <sup>12</sup> )	16,781	17.8
Method known	19,241	20.5
<b>Total</b>	<b>94,100</b>	<b>100.0</b>

<b>Method-known cases (methods of obtaining personal information were reported)</b>	<b>Number of complaints</b>	<b>Percent based on subtotal<sup>13</sup></b>
Access through relationship with victim	10,101	52.5
Wallet or purse containing identification was lost or stolen	6,615	34.4
Mail theft or fraudulent address change filed	2,577	13.4
Application, financial, or employment records compromised	1,322	6.9
Burglary or break-in	686	3.6
Internet solicitation or purchase	462	2.4
Telephone or mail solicitation or purchase	132	0.7
Other	1,706	8.9
Information about method not provided <sup>14</sup>	572	3.0
<b>Subtotal</b>	<b>19,241<sup>15</sup></b>	

Source: FTC data.

**Relationship of Suspect to Victim in Identity Theft Complaints FTC Received (Nov. 1999 through Sept. 2001)**

<b>Relationship of suspect to victim</b>	<b>Number of Complaints</b>	<b>Percent based on total 94,100 complaints</b>
Family member	4,629	4.9
Roommate/cohabitant	1,137	1.2
Neighbor	1,003	1.1
Workplace coworker/employer/employee	836	0.9
Otherwise known	2,496	2.7
<b>Total</b>	<b>10,101</b>	<b>10.7</b>

Source: FTC data.

<sup>12</sup> Non-FTC data refer to identity theft complaints forwarded from SSA/OIG to the FTC. In these complaints, information about the methods suspects used was not collected.

<sup>13</sup> Percentages add up to more than 100 percent because some victims reported that the suspect used multiple methods of obtaining the data.

<sup>14</sup> In 572 cases, consumers said that they knew but did not specify how the suspects obtained the personal information.

<sup>15</sup> Details exceed 19,241 because some victims reported that the suspect used multiple methods of obtaining data.

## F. Methodologies for Capturing and Using Personal Information

As the previous statistics indicate, many victims of identity theft do not know how their personal information was obtained and compromised. Except in cases in which the thief is caught and reveals his or her methods, and in situations in which the thief is a family member or trusted service provider, victims can only speculate. However, there has been a sufficient number of investigations to provide some insight on how identity thieves work.

The most common methods of compromise are:

- **Mail theft** – Thieves can use mail to access credit card statements, banking statements, utility bills, pre-approved credit offers, payments and “convenience checks.”
- **“Dumpster diving”** – Thieves can collect data from the trash of businesses and individuals. The amount of data collected in this manner can be huge, and can encompass all of the data mentioned in the mail theft category and more.
- **Use of personal Web sites** – Personal Web sites can provide a host of information about an individual from which identity thieves can draw.
- **Theft of wallet or purse** – With one wallet or purse a thief can obtain a driver's license, Social Security card, passport, credit cards, and even written passwords to online accounts.
- **Trusted insiders acting on their own** – These individuals can collect proprietary information trusted to the institution by a customer, or those who act on their behalf for payment, or by coercion.
- **External hacking** – Hackers can penetrate company networks and internal systems, such as a Web site, and walk away with a large listing of customer names and account information. In some instances the hackers establish look-alike Web sites that entice unsuspecting customers to post sensitive information.
- **Intercepting sensitive information** – Hackers can access clear text (unencrypted) information from Internet transactions.
- **Accessing marketing information services companies' data** – These organizations provide sensitive information to others for marketing purposes. The information may not be secure in how it is stored or transmitted, and the person or entity to which they sell it may not be a legitimate business.
- **Family members and trusted service providers** – Relatives, doctors' office personnel, auto dealers, and others with whom people entrust their personal information can take advantage of their access to personal data.
- **Social engineering** – Skilled social engineers have their stories down, know to what most people will respond, and understand that people are often willing to provide information to others if they perceive that it is needed or that they will benefit.

These are just a few methods by which sensitive information falls into the hands of identity thieves. For thirty years, Social Security numbers have been used as employee numbers and driver's license numbers, and are often collected on applications, even if they serve no real purpose. Many states and the federal government are reacting to this exposure by enacting appropriate laws that increase punishment associated with identity theft. In some states, identity theft is being made a felony, and possession of information with the intent sell or give it to identity thieves is being made a misdemeanor or felony. Further, many states have enacted laws to limit the sale of birth and death information and to enable identity theft victims access to free credit reports for 12 months.

Like Social Security numbers, “shared secret” information, including mother’s maiden name, place of birth, and high school or college attended, have been so widely used and shared among so many institutions that they are no longer secret. Most of that information can be uncovered through other sources or has been shared with institutions who may not have kept it secret after the business relationship ended. And, when there is no means to validate its authenticity, an identity thief can simply make up that information. “Alternative shared secrets,” such as favorite color or a pet’s name, only serve to validate a person once he or she has opened an account, they do not prevent identity theft. An account takeover will most certainly involve the capture of that information; therefore the provider of that data must remember to protect the information as much as he or she would protect their personal identifiers.

## V. CURRENT AND PROPOSED LEGISLATION

### A. Overview of Existing Federal Law

Policy makers have addressed identity theft with legislation for at least two reasons. The first is the rapid growth in reported cases; the second is that the individual victims feel particularly vulnerable and violated, especially those who have substantial difficulty cleaning up their credit records. In 1998 Congress enacted the current federal identity theft statute, the Identity Theft and Assumption Deterrence Act of 1998 (18 U.S.C. § 1028 (a) (7)), which makes it unlawful to:

...knowingly transfer...or..., without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law, if the identification document in question was or appears to be, issued by the United States or the offense involved the use of the mails or affected interstate commerce.

The existing statute has a sweeping substantive breadth that reaches all identity thefts that have a federal interest, even those that involve state law felonies. The U.S. Department of Justice reports that identity theft is one of the fastest-growing crimes and one of the most costly to business. However, prosecutions under this statute are rare. This is true for a variety of reasons, one of which is that the crime is always a derivative offense committed in conjunction with another crime.

Other federal legislative efforts addressing identity theft are the Enhanced Border Security and Visa Entry Reform Act of 2002, which requires travel and entry documents to include biometric identifiers (see Section VII, Fraud Prevention Technologies), and the USA Patriot Act, which requires the development of technology standards to confirm individual identity. Aimed more at domestic terrorism than identity theft, questions exist as to how these Acts would be implemented and whether or not they would be effective in financial institution efforts to prevent identity theft.

### B. Proposed Federal Legislation

Legislation sponsored by Senator Dianne Feinstein (D-CA), S. 153, would add to the current law by enhancing the penalties and simplifying the proof requirements for identity theft crimes. The bill would create the crime of “aggravated identity theft,” defined using the predicate offenses usually committed along with identity theft, including all of the most serious and frequently occurring offenses. One result would be to allow increased punishments for these kinds of crimes. Moreover, the bill would amend existing law to prohibit the possession of someone else’s identity information with the requisite criminal intent, in addition to current law that prohibits the transfer or use of another’s information. Enactment of this legislation would help state and federal law enforcement officials in pursuit of identity thieves. The bill has passed the Senate and is pending in the House of Representatives.

In the House of Representatives, H.R. 2035, introduced by Representatives Steve LaTourette (R-OH) and Darlene Hooley (D-OR), has attracted 43 cosponsors. The legislation requires credit and debit card truncation by retailers, has requirements that credit card issuers verify change of address requests before sending out new credit cards, and provides the companies put in place reasonable procedures to ensure that a customer requested an extension of credit is who they purport to be if a fraud alert appears in his or her credit report.

Legislation to restrict the use of Social Security numbers has been pursued in the U.S. Senate in response to a highly publicized case of identity theft that resulted in a fatality. The bill, S. 848, the Social Security Number Misuse Prevention Act of 2002, sponsored by Senators Feinstein and Judd Gregg, prohibits the display, sale or purchase of any individual's Social Security number without providing notice and receiving an opt-in consent from the individual. Although exceptions are provided for business-to-business activities, the legislation could present problems for many financial institutions.

Other serious legislative efforts seek to assist identity theft victims by requiring that the victim have access to information from financial institutions. The reported purpose of requiring such access is to enable the victim to build a case to present to law enforcement authorities.

Both reauthorization of the Fair Credit Reporting Act and continuation of uniform national standards for the treatment of customer information are being tied to discussions of identity theft in the current legislative and policy environment.

### **C. Overview of State Law**

Almost every state has some form of law addressing identity theft. Forty-four states have passed identity theft statutes since 1996, while five other states have laws that address related activities. Identity theft can be prosecuted as a felony in 45 states. One of the difficulties in prosecuting identity theft under state law is that most laws do not address intrastate conflicts that arise among differing jurisdictions, such as when an identity is stolen in one jurisdiction and used in another. In addition to jurisdictional issues, there is also a lack of resources at the state level. Because of a lack of personnel available to research cases, thresholds are set for the number of cases investigated.

At this time, there are not sufficient data with which to direct proposed legislation. However, great care should be taken in proposing legislative solutions, since laws designed to combat one of these elements may lead to higher losses through other methods. New legislation can also lead to a loss of convenience and negatively impact other consumer benefits.

A list of current state identity theft laws can be found through the FTC's Web site at [www.consumer.gov/idtheft/statelaw.htm](http://www.consumer.gov/idtheft/statelaw.htm).

## **VI. CURRENT PRACTICES AND RECOMMENDED STRATEGIES**

### **A. Current Industry Countermeasures and Mitigation Processes**

The financial services industry employs a wide variety of tools and strategies for preventing identity theft. The industry also devotes a substantial amount of effort to helping customers resolve suspected cases of identity theft. Each institution maintains a staff of specialists devoted to helping customers identify and resolve these cases, and many use multiple units to address the nuances of identity fraud in credit card, checking accounts and installment loans. While these specialists provide the core resolution services, customer service professionals, who often field the initial inquiries, are also trained in identity theft issues. The fraud risk team may draw on the expertise of an institution's corporate security staff if an extensive investigation appears warranted.

Fraud-risk teams generally follow a common pattern when providing customer assistance:

- First, the specialist works with the customer to develop a shared understanding of the situation. The customer describes what prompted the call and may offer a theory about how his or her identity was compromised. The specialist offers general information on identity theft and works with the customer to better understand the facts of this specific situation. Many institutions and advocates see the awareness and education component of this initial conversation as one of the most important services that financial institutions can provide.
- The specialist and the customer then work together to identify compromised accounts and fraudulent transactions. This process involves a review of the institution's own systems and may involve a joint review of information obtained from one or more credit bureaus. The specialist will block or close affected accounts, working with the customer to ensure that legitimate charges are honored. The customer may be asked to sign an affidavit, and the specialist will start the process of reversing fraudulent transactions and attempting to recoup some of the costs from merchants or other institutions.
- After the case is mostly resolved, the specialist will have a number of follow-up responsibilities. He or she will continue to work with the customer to provide referrals to the credit bureaus if necessary, provide letters to affected merchants if applicable, and to monitor for subsequent intrusions. If a formal investigation is warranted, the specialist may refer the case to corporate security. If a federal suspicious activity report is required, the specialist may prepare it, or he or she may notify corporate compliance.

Throughout this process the fraud risk team typically relies heavily on the financial institution's core systems and a number of specialized systems. The team will use a variety of transaction systems, and many institutions have developed overnight imaging capability to give fraud investigators immediate access to checks, signatures and other records. Each financial institution relies on a combination of its own authorization, risk scoring and fraud-alert systems, as well as systems that it shares with the card associations, credit bureaus and other vendors. Most institutions have developed case-management systems to track the progress of individual incidents and provide consistent information to customers.

Financial institutions invest substantial resources in helping fraud victims, and they also accept significant risk. Staffing these functions with highly trained professionals is costly.

While continuous technology investments enhance the effectiveness of these efforts and help to moderate the labor-intensive nature of the work, many institutions invest disproportionately in this area in order to preserve or enhance the loyalty of their customers. Institutions accept the majority of the economic risk for fraudulent transactions and, despite their best efforts, still risk damaging their relationship with the customer.

## **B. Financial Institution Centralized Approach to Identity Theft Assistance**

One of the most time-consuming and frustrating aspects of being a victim of identity theft is calling a financial institution to report the fraud and being transferred from individual to individual and from department to department, all the while recounting the details of the victimization over and over again. A "single point of contact" model within every financial institution can help to remove some of the burden from the victim. This model works equally well whether the customer has become aware of suspicious activity and contacts a financial institution, or whether the financial institution first detects suspicious activity and contacts the customer.

For a "single point of contact" model to work, all employees, including branch and telephone banking staff, must be uniformly trained to listen for words and phrases from customers such as "identity theft", "fraud" or "unauthorized activity." When this occurs the customer should be referred to the "single point of contact" area for assistance. The victim is appointed a contact and that contact is responsible for assisting the victim until all issues are fully addressed. The customer now has only one name and a direct telephone number to call for any ongoing issues, i.e., pay/no pay decisions on outstanding checks in the case of a questionable DDA transaction, questions regarding reimbursement, etc. In the event of illness or other absence for the contact, a backup person will have access to all the information concerning the customer's situation.

During initial communication the contact gathers the customer's information and details concerning the suspicious activity, and authenticates that the person they are dealing with is in fact the victim. The facts in the situation must be clearly established, and all steps to fully resolve the fraud are taken. For example, if affidavits are necessary, they are completed by the contact and sent to the victim for signature. After completing the review of the initial suspicious activity, the contact reviews all internal systems for any additional fraud which may have occurred on other accounts/relationships held by the victim within that financial institution, regardless of type. This may include deposit accounts, consumer loans, credit cards, brokerage services, etc. All of the victim's accounts and/or transactions within that institution are reviewed to ensure that all the fraud is identified. Further the contact takes the necessary steps to assist the victim as appropriate. This would include closing accounts, opening new replacement accounts, ordering new checks, debit cards, ATM cards, credit cards, etc. Internal steps are also taken to mitigate additional fraud, such as linking the new accounts to cards and overdraft lines so that the victim's relationship is fully restored. If subsequent calls are necessary an agreement is reached concerning the best time to contact the victim and the best methodology to do so.

The "single point of contact" within a financial institution may be most effective in terms of customer service and cost efficiencies if it is achieved organizationally; however, other

options exist. Options within a financial institution to achieve a "single point of contact" service for recovery from identity theft include:

- An organizational structure with a centralized risk management function that is responsible for all activities as described above.
- Customer/victim support area responsible for customer service with systems access for all products (for query purposes). Contacts are responsible for facilitating all required actions, but they are performed by decentralized product or transaction areas - DDA (debit card, ATM card, ACH, paper check), consumer loans (installment, unsecured, PEL, etc.), credit cards, brokerage, etc.
- The contact functions include facilitating actions in a liaison capacity.

Ideally, each institution would test its response and processes to complaints of identity theft by establishing a means to replicate the customer/victim experience. Additionally, if the results demonstrate that the process is cumbersome and frustrating, then re-engineering the processes to be less problematic is advisable. The above described centralized model within a financial institution is one solution, however, others may exist. Like most business processes that are customer focused, this too deserves testing and our full attention.

### **C. Financial Institution Voluntary Guidelines**

Given the importance of this issue, the BITS Fraud Reduction Steering Committee, in cooperation with BITS and The Financial Services Roundtable, has developed the following voluntary guidelines for both preventing identity theft and assisting victims when it does occur. BITS and the Roundtable launched an effort in May 2003 to encourage financial institutions to commit to implementation of these Guidelines. Implementation of these successful strategies on a voluntary basis will go a long way to deter those who would commit such crimes, and assist those who suffer falling victim to such criminals.

## **FRAUD REDUCTION GUIDELINES**

### **STRATEGIES FOR IDENTITY THEFT PREVENTION AND VICTIM ASSISTANCE**

#### **MISSION**

Members of The Financial Services Roundtable and BITS are committed to creating and implementing a set of efficient, effective and consistent procedures to restore a victim's financial identity and to prevent ongoing incidences of identity theft. To that end we, the participating financial institutions, agree to share and implement the following successful strategies.

#### **PREVENTION**

##### **Participating financial institutions agree to:**

- Share on an ongoing basis successful fraud prevention strategies in areas that include:
  - Account opening and online transactions
  - Authentication
  - Monitoring Controls
  - Loss tracking and reporting
  - Personnel training to detect suspicious activity
- Provide educational materials to our customers to assist them in protecting their financial identities.
- Provide data relating to identity theft to appropriate law enforcement agencies for trending and analysis of patterns of fraudulent activities and prosecution of fraud rings.
- Join with industry associations and organizations, and consider joining the Identity Theft Assistance Center (ITAC), if such a Center is established, to analyze and pool identity theft data for law enforcement purposes.

#### **VICTIM ASSISTANCE**

##### **Participating financial institutions agree to:**

- Establish an internal system that provides victims a single point of contact within the financial institution.
- Provide each victim with educational materials to assist in preventing further instances.
- Utilize an industry-wide Uniform Affidavit.
- Establish a system for disseminating the Uniform Affidavit, as appropriate, to law enforcement, industry organizations, and others, including an ITAC, if such a Center is established and participation is elected.
- While reserving the right to receive additional information from the victim, receive and use a completed Uniform Affidavit from other financial institutions.
- Upon receipt of a completed Uniform Affidavit, contact the victim to seek resolution of affected accounts within their own institutions.

#### **D. Financial Institutions' Control Systems and Identity Theft Prevention Tools**

Financial institutions use various control systems to detect and prevent identity theft when opening accounts or as part of their identity theft monitoring programs. The controls used vary considerably by the size of the institution, geography, and the institution's overall exposure to fraud. Each financial institution must weigh its exposure and determine its business case for mitigating risk.

Below are some of the tools available to help prevent identity theft. A financial institution may use one or more of these tools, depending on the level of risk the institution's management is willing to accept.

##### **New Accounts/Application Tools**

- Review negative files for name, address, Social Security data or other element matching.
  - Shared databases of negative information
  - National databases of shared known and verified fraud records
  - “Homegrown” internal negative databases
  - Scan of credit bureau information
- Risk score new accounts application data for fraud.
  - Shared databases of negative information
  - Credit bureau fraud risk scores
- Review fraud alerts when processing loan applications.
- Attempt to validate identity with “out of wallet” information.
  - Credit bureaus and vendors provide simple name, address and phone number verification; also provides a score and can be run independent of a credit report.
  - Authentication for Internet and call centers
    - Level 1 – Name and address verification
    - Level 2 – Fraud identity score
    - Level 3 – Out-of-wallet questions
- Fingerprint or other biometrics at new accounts.
- Check Social Security Master File.
  - The National Technical Information Service (NTIS) and the Social Security Administration together offer the SSA Death Master File on a weekly and monthly basis.<sup>16</sup> The list can be used to check applications against Social Security numbers of recently deceased persons. NTIS is considering making the file searchable online, so that smaller institutions can make queries about Social Security numbers and the names of new depositors, loan applicants, etc., at a reduced price. (A larger institution would purchase the whole file.)

---

<sup>16</sup> For more information, go to [www.ntis.gov/products/pages/ssa-death-master.asp](http://www.ntis.gov/products/pages/ssa-death-master.asp).

### **Ongoing Account Monitoring Tools**

- Secure access to accounts with PINs or other customer-selected codes.
- Assign a greater number of “tokens” or a higher degree of security to higher-value customer relationships. This helps deter pretext callers.<sup>17</sup>
- Monitor accounts for radical changes in activity in order to detect deposit fraud and check fraud.
- Inspect or refuse check orders with address changes.
- Standardize or centralize address-change verification with letters, phone calls, etc.
- Use software to detect data manipulation, e.g., changing one or two digits in a Social Security number, changing part of the name, etc. This type of software routine may be part of reviewing negative files, risk scores or fraud alerts.
- Use biometrics on an ongoing basis.

### **Branch Transaction Tools**

- Use signature verification in back-office environments and at the teller counter.
- Use tools to detect counterfeit identification, such as ultraviolet lights, or the *ID Checking Guide* published by Driver’s License Guide Co.
- Place the customer’s photo on ATM, debit and credit cards.

### **Training**

- Provide fraud-awareness training for all customer-contact personnel (especially branch and call-center employees).

## **E. Credit Bureaus’ ID Theft Prevention Tools and Consumer Assistance Practices**

The nation’s leading credit agencies, Experian, Equifax and Trans Union, have voluntarily implemented a comprehensive series of initiatives to assist victims of identity theft in a timely and effective manner and to provide a more uniform experience for victims who may be working with personnel in multiple fraud units. Credit Bureaus also have implemented tools and practices to assist the financial services industry in preventing Fraud.

Outlined below are the credit bureau industry’s victim assistance processes to aid consumers recovering from identity theft:

### **Consumer Contacts Credit Agencies to Report Possible Fraud**

- Consumers can call the automated telephone system of each credit reporting agency 24 hours a day.
- When a consumer calls a bureau’s automated phone systems to report fraud, a security alert can be added to the consumer’s credit file. This alert warns creditors to verify the consumer’s identity before extending credit to avoid additional fraudulent account openings.
- The consumer’s name and address are immediately opted out of prescreened credit offers.

---

<sup>17</sup> “Pretext callers” gain personal information by calling an unsuspecting person and, posing as a legitimate business, asking him or her to supply certain information.

- When a consumer calls the respective automated phone systems, he or she is asked to enter information such as Social Security number, 2-digit year of birth, and the numeric portion of his or her address and zip code. If the information entered matches what is on the credit file, the credit agency sends the consumer a complimentary credit report within three business days. If the information reported does not match, the report is not mailed until the consumer has completed an alternative manual process in which specific documentation, such as Social Security card, pay stubs, W-2 forms, and a drivers license, is mailed to the respective bureaus verifying the Social Security number and address information.
- It is also common practice to provide the telephone numbers of other credit bureaus and recommend that they be called as well. In September 2002, the bureaus' national trade association, the Consumer Data Industry Association (CDIA), advised the FTC that Equifax, Experian and TransUnion had agreed to pilot test a voluntary initiative. As part of the initiative, when an identity-theft victim calls any one of the participating credit reporting agencies, the victim will be notified that the agency will share his or her identifying information with the other two credit reporting agencies, and that the above three steps (posting a security alert, opting out of marketing lists, and providing a complimentary copy of the credit report) will be taken by each of the three agencies. The pilot was considered successful and the bureaus announced this new practice officially in April 2003.
- Consumers should be advised to contact their credit grantors and any relevant government agencies.

### **Consumer Receives Personal Credit Report by Mail**

- The consumer may dispute fraudulent items in writing, by phone, online, or, in some cases, in person. A toll-free telephone number listed on the credit report enables consumers to speak directly to a specially trained customer service representative.
- The customer service representative helps remove, investigate and verify fraudulent items on the report.
- If the consumer has not filed a police report, the agency recommends he or she do so, provided that there has been an actual occurrence of identity theft. (A police report should only be filed if a crime has been committed; many of the consumer contacts the three credit bureaus receive are precautionary.)

### **Investigation of Fraudulent Items on Credit Report**

- The credit agency notifies the creditors and/or data furnishers of alleged fraudulent items.
- The data furnisher is asked to compare the consumer's identification information with the original application or contract data and to confirm all of the information provided.

### **Fraudulent Data Are Removed**

- The credit agency completes investigations of fraudulent data within 30 days. If the data contributor cannot verify information as accurate within that timeframe, the fraudulent information will be deleted.
- When a police report is provided as part of the process of disputing fraudulent data, Equifax, Experian and TransUnion will promptly block these disputed items from appearing on subsequent consumer reports on that individual. (Data furnishers are

notified that their information has been blocked from appearing.) This voluntary step goes beyond the requirements of the federal FCRA.

### **Consumer Notification**

- Within five days of completing the investigation, the credit agency notifies the consumer of the results. The notice includes a statement that the investigation is complete and a revised credit report.
- A consumer can add a fraud alert to his or her file by contacting any one of the credit bureaus. The information will be relayed to the other bureaus. The alert will notify creditors that the consumer suspects fraud, has a time-sensitive concern about identity theft, or is a victim of fraud.
- Credit reporting agencies educate consumers on how to prevent identity theft and recover from victimization by providing educational materials on fraud and identity theft. Credit agencies also work closely with financial institutions, consumer organizations, government agencies and others to educate consumers about information use and how to protect themselves from fraud.

### **Bureau Practices to Assist Financial Services Companies**

The major credit bureaus have leveraged their extensive data resources and technology to provide fraud prevention tools that can detect the simplest forms of fraud to the most complex criminal activity against either FCRA-regulated or non-FCRA-regulated information. Some of the tools are used by financial institutions as a standard business practice. Others, just now being implemented, provide a more powerful means to authenticate and validate customer information and prevent fraud. The common link among all of the tools is their reliance on the responsible use of data to stop fraud before it starts.

The following bureau practices are available to assist the industry in preventing identity theft:

- **Name, Address and Phone Verification**

- This preliminary verification step ensures the accuracy of consumer information submitted in the application and checks for indicators of fraud by verifying the consumer's name, address and telephone number against non-FCRA-regulated information. This service identifies inconsistent information as well as high-risk addresses and telephone numbers. There are two ways of validating this information:
- **Consistency validation** – The consumer-provided name, address, telephone number and Social Security number are in appropriate formats and are matched to third-party repositories. (A match to individual or household surname may constitute a match.) Two-source validated repositories are recommended to minimize consumer validation against compromised third-party data.
  - **Sensibility verification** – Consumer-provided information and on-file information are checked for synchronous sensibilities. Data points are examined for sensible consistency, such as phone area code and the exchange with the physical address. Other sensibility verifications include the distance between phone or address points to determine viable commute distances.

- **Bureau Fraud Indicator Service**

All three major credit bureaus offer a fraud indicator service with credit report inquiries. The service compares application data to credit file data to help lenders recognize fraudulent Social Security numbers, addresses and phone numbers.

- **Scoring Models**

Scoring models, the next generation of fraud-prevention methods offered by some credit agencies, are quantitative tools used to predict and control fraud risk. Scoring models combine fraud indicators, such as Social Security number information, address validations, telephone validations and application data inconsistencies (such as a phone number that is inconsistent with an address or the establishment of credit prior to the age of 18), into one highly predictive number or score. The score helps identify which applications are most likely to be fraudulent and therefore require further manual review. The score threshold by which an application “passes” or is sent on for further internal review is set by the lender and is based on the lender’s business objectives and defined threshold for manual reviews.

- **Data-sharing Initiatives**

Data sharing can be the industry’s first line of defense against identity theft. Current data-sharing practices in use by some of the credit bureaus include:

- **Industry data exchanges** – This practice prevents fraud by providing positive and negative defaulted or fraudulent account information for the small business lending, telecommunications and utility industries. Many of these exchanges are owned by the members that contribute data to them. The members determine the operating principles, often prohibiting the use of the data for either cross-selling or marketing purposes. Leveraging such sources allows participating members to instantly identify potentially risky applications, indicative of either possible identity theft or payment-fraud characteristics. When such indicators are present, alternative cautionary processes, such as a manual review of the application or deposit guarantees, are often the result.
- **Shared cross-industry known fraud data** – This refers to practices of sharing known fraud records from various business sectors and across industry boundaries to provide an immediate indication of an applicant’s prior fraud activity at the point of application. The concept of sharing verified fraudulent data across industry boundaries has been standard business practice in the UK for almost a decade. The success of data sharing to prevent fraud can be measured in the fraud saving results reported by members of the UK’s fraud database:
  - UK fraud database members reported a total fraud savings of \$295 million in 2000, up from \$50 million in 1995. The increase in savings each year was a result of an increase in businesses contributing to the fraud database. As more businesses began to share fraud data, fraud savings increased.
  - One organization reduced the number of booked fraudulent accounts from 730 in 1996 to 48 in 2000.
  - One organization increased the number of fraudulent applications refused from 30 percent in 1996 to 97 percent in 2000 and reduced the number of fraudulent applications accepted from 35 percent in 1996 to only 1 percent accepted in 2000.

- **Shared full application data** – In this method, a variety of policy rules are applied to the current application, comparing it to past applications, fraud records and credit data to achieve a 360-degree view of an applicant and verify applications beyond the traditional name, address and Social Security number checks. This view reveals inconsistencies, anomalies and known fraudulent information in applications that can indicate identity theft, as well as other types of fraud.

- **Online Authentication Tools**

Online authentication tools help to instantly verify customer identity for online, call-center, or other card-not-present transactions, as well as for online bureau access. Authentication tools use consumer credit file data to verify application information in conjunction with internal and external data resources, and draw upon criteria determined by each client to deliver a fraud risk score. The most powerful level of online authentication draws detailed information from various databases to provide an interactive session in which customized out-of-wallet questions are designed so that only the consumer can answer them. For example, a consumer might be asked to identify his or her previous address, mortgage lender or car loan information. The consumer's ability to answer these out-of-wallet questions provides a "level of certainty" value and a group of associated "reason codes" that indicate either potential fraudulent characteristics of the transaction, or match quality assessments that verify the individual's identity. Each firm using such a solution will generally set a threshold for the level of certainty value in combination with the various reason codes by which a transaction either "passes" or is potentially directed to an alternative manual process for further review.

One drawback to the credit bureaus' systems is the lack of feedback loops in place to allow lenders to know at the time an application is being processed if the applicant's fraud score has prompted previous lenders to manually review his or her application. This may not always be within the credit bureaus' control, however, since they do not always have access to that information.

## VII. FRAUD PREVENTION TECHNOLOGIES

### A. Authentication Technologies and Processes

Identity authentication is essential to grant an individual access to confidential services of value. Authentication is the “gatekeeper” to other security tasks, such as confidentiality, non-repudiation, authorization and access control. It is necessary in order to verify a customer’s name, email address, mailing address and account number, as well as to validate the customer him or herself and the information he or she supplies.

Varying technologies are available for authenticating individuals, the most common of which are:

- **Shared secrets**
  - **Static secrets**, such as user IDs with passwords, are easy to implement because the underlying technology is widely deployed, used and understood. When shared secrets are used, no special hardware or software is needed. The strength of this technology is low-to-medium security if implemented correctly (keeping the password sufficiently long, not sharing it with third parties or writing it down somewhere, and changing the password frequently) because the password can be guessed or stolen. Some secrets are really secrets, such as passwords. Other forms of information used to authenticate the identity of an individual are not really secrets—they are just not easily known, but are facts not likely to be known by anyone but the real person, such as mother’s maiden name, Social Security number, or pet’s name.
  - **Dynamically changing shared knowledge** refers to a shared secret, such as details from the last transaction (e.g., amount, merchant, and/or date), that changes frequently. These systems are also relatively easy to implement. This type of authentication is used less often and therefore is less familiar to users. However, it is more secure (medium to high security) than static secrets because the secret information is constantly changing.

The problem with shared-secret authentication is that secrets can be guessed or stolen. The more they are used, the less secret they become and the more likely they are to be compromised.

- **Tokens**
  - **Proprietary random PIN tokens**, such as RSA, Vasco, and Rainbow cards, have the characters displayed on the card (typically six or more alphanumeric characters) continuously change. The algorithm used to update the continuously changing sequence is generally known only to the authentication service provider and is proprietary. The sequence appears random to the observer, but actually can be deterministically linked to a unique hardware token by the authentication service provider. Thus, the service is actually authenticating the token, and indirectly the user, by association with his or her possession of the token/card. For this reason, proprietary random PIN tokens are generally used with a secondary identifier, e.g., they are secured from operation unless the holder of the token enters in a correct user ID and password or passes a biometric test (see below for a discussion of biometrics), making this a medium-high authentication security. It is relatively easy to implement because the underlying technology is in generally widespread use for intra-company remote access. It is costly, however, with hardware tokens costing \$20

or more per card/token. Token issuance and administration are also more costly than password maintenance, although password administration and maintenance are costly as well.

- **Smart cards**, such as Sun, ActivCard, GemPlus and RSA, typically store secret keys that are used to cryptographically identify the user by “digitally signing.” Digital signing involves encrypting a message digest with a secret private key stored on the smart card, where the digital signature can be verified as having been encrypted with the secret private key. This is also relatively easy to implement internally because the underlying technology is relatively widely deployed. (It is in widespread use for intra-company remote access.) The security of the smart card/token generally comes in one of the following three classes, listed in order of increasing security:
  - Smart card stores keys and certificates only;
  - Smart card stores keys and certificates and actual signing takes place on smart card reader; and
  - Smart card stores keys and certificates and signing, display and data entry (keyboard) on combination of smart card and smart card reader

Because digital signature technology is difficult for users to understand, complex to use, and fairly expensive to implement, this technology will most likely be deployed on more portable and personal hardware tokens/cards. Additionally, many smart card systems are not interoperable across institutions. Further, though the whole system could be implemented as a software module on an individual’s PC, the computer (where the private key is stored) would be authenticated, rather than the user.

As is the case with the proprietary random PIN token, the authentication here is actually authenticating the token (smart card), and only indirectly the user, by association with his or her possession of the token/card. For this reason, smart cards are generally used with a secondary identifier, such as a user ID and password or biometric test.

If symmetric encryption (when the same key used to encrypt is also used to decrypt the message digest) is employed, the verifier must know the secret private key. This works if the secret key is known only to a very limited number of parties, normally two—the user and the trusted third-party authenticator—as the technology can be compromised if the trusted third party is criminal or negligent. Thus this technology provides only a medium-to-high level of security.

If non-symmetric encryption is used, the verifier only needs to know a public key that is uniquely paired with the private key to decrypt and verify the digital signature. Furthermore, the private key cannot be determined from knowledge of the public key. In this case, many parties may verify without fear of compromise, and thus this approach can be considered to provide high security when integrated with a secondary authentication technology, such as passwords or biometrics.

At present, this technology is not in widespread use and has been used only on a pilot or limited basis. It is still costly to deploy and complex for the user to install, use and understand. Smart card costs vary by class (the strength of the security),

typically ranging from \$10 to \$100. There are also interoperability problems between vendors and implementations.

A major problem with token authentication like proprietary random PIN tokens and smart cards is that they become insecure if lost.

- **Biometrics**

Biometrics technologies, which are usually used with digital certificates or smart cards, identify individuals by some unique physical or behavioral characteristic or characteristics, such as facial features, speech patterns, fingerprints, iris, handwriting or typing. As such these technologies represent the highest form of security because these characteristics are extremely difficult (though not impossible) to forge when the technology is implemented properly. On the other hand, because biometric technologies do uniquely and universally identify an individual, privacy concerns can inhibit consumer acceptance. Biometrics often use digital certificates to describe what “permissions” the holder has.

Because they are in an early stage of development, biometrics technologies are still complex to implement and use, and costly to deploy. There are false rejects that may impact customer service. Thus they are not yet in widespread use. They have been used to date primarily as a means of physical access; other uses have occurred only on a pilot or limited basis. In the future, however, smart cards or tokens could store biometric information for remote verification.

Aside from those already mentioned, another problem with biometrics is that, if compromised, these technologies are difficult to correct. Another drawback to biometrics technology is that its performance is not exact. There is always a possibility of false reject of the right person, and false accept of the wrong person. Further, biometrics, especially if not properly implemented, can be spoofed (for example, by using voice recordings, photos and play-back).

**Authentication Technologies: Key Points**

Key points about these authentication technologies are summarized in the table below. It is important to note that many systems actually employ one or more of these authentication technologies.

**Authentication Technologies**

Authentication Technology	Security of Authentication	Complexity of Implementation	Cost	User Acceptance
Shared secrets	Low-medium	Low	Low	Widespread
Proprietary random PIN tokens	Medium-high	Medium	High	Relatively widespread for intra-company remote access
Smart cards	Medium-high	High	High	Limited
Biometrics	High	High	High	Very limited

It is equally important to note that an online authentication method is only as good as its implementation, including the offline processes used for verifying identities during enrollment, registration and customer service involving changing information, revoking or updating authentication secrets or tokens, biometric registrations and bindings. This includes collecting and maintaining identifying information and providing confirmation and acknowledgements via diverse channels, such as email or U.S. mail. Therefore, the actual security of an authentication system can only be properly evaluated through analysis of the complete system implementation and associated offline processes. An implementation using a weaker authentication technology might actually result in a stronger authentication system than one based on a stronger authentication technology.

### **Limiting Risk Exposure and Liability for Very Sensitive Applications**

Many services and applications are sufficiently sensitive that the service providers are rightfully reluctant to rely on another third-party service. For example, most financial institutions find outsourcing authentication and authorization of consumer banking and brokerage services to be too risky. Some of the motivations for keeping this function in-house are:

- Reluctance to accept risks outside of the institution's control for which it could be held liable.
- Potential loss of control over the security of customer account information.
- Reluctance to lose the use of confidential customer data known only to the bank or brokerage and its customer or to share that information with a third party.
- Fear of data compromise when more broadly confidential data are shared among third parties.
- Fear of loss of control over the means of authentication and the strength of the authentication technology employed.
- Potential denial of many of the tools the institution uses for fraud management.
- Potential weakening of the customer's confidence in the institution's security, and/or erosion of the "trusted" relationship between the customer and institution by placing a third party in direct contact with customers.

### **Findings and Recommendations**

Companies can choose from a wide range of authentication technologies, including user IDs with passwords, proprietary PIN tokens, smart cards and biometrics. Each has its strengths and weaknesses, and no one technique is right for all circumstances and applications. Techniques can be combined to get better results, but often at higher cost and complexity. Such a combination is referred to as a "multi-factor system." For example, a hardware token unlocked by a user password would be a two-factor system.

User IDs and passwords are generally the most widespread authentication technologies in use today. Whether or not they will be displaced by stronger authentication technologies remains to be seen. The likely successor technology (or technologies) are uncertain and subject to a number of factors. For example, the use of user IDs and passwords, augmented by other shared secrets, could continue into the foreseeable future, particularly if incremental improvements are made that strengthen overall system security and further reduce cost and complexity. On the other hand, this system's continued use could decline dramatically if

some major and highly publicized security violations occur, and/or dramatic advances are made that reduce the cost, complexity of use, and adoption rate of one or more of the other authentication technologies. See the BITS Web site at [www.bitsinfo.org](http://www.bitsinfo.org) for additional information about BITS' Authentication initiative.

## **B. Information Management Technology**

Today financial institutions are collecting, examining, storing, securing and moving information at unprecedented levels. New technologies are allowing them to significantly enhance their ability to use that information. Along with this shift comes a new responsibility for ensuring that the information is kept secure and private, and that any sharing or destruction is carried out appropriately. Operating in a need-to-know environment, financial institutions have learned to not share information unless there are clear and compelling reasons to do so. Though generally a positive trend, this results in the isolation of information. While secure and protected, the data serve no practical purpose in the larger community.

Collected information is usually catalogued and stored in meaningful groups by the data owners, with classification often based on business or legal guidelines. The data are often classified into categories: public, sensitive, or restricted. Regardless of the classifications, there are clear benefits for the broader use of information. Criminals have no restrictions and will use any and all information that they come in contact with during the course of their activities. Criminals realize that financial institutions, government agencies, and others do not fully share information because they are either reluctant to do so or are restricted by legal guidelines. But financial institutions now face growing challenges, including identity theft, sophisticated and organized fraud schemes, money laundering, and the threat of terrorism, that may reshape the controls on data sharing. How financial institutions engage in the sharing of data and remove the blind spots will determine their success in meeting these challenges. However, before we can address sharing of information, we first must examine how information is managed.

While many institutions recognize the need to collect information and store it securely, far fewer recognize the challenge of efficient use and manipulation to mitigate fraud and identity theft. Institutions must begin to identify and use tools that enhance the use of information once it is collected. The collection and storing of data into databases and data warehouses are essential elements for manipulating information. These are the platforms from which data can be selected to perform analytical reviews and to link information to other events to portray a full picture of activity. Manipulating both internal and external data with analytical tools reveals data relationships that would otherwise be hidden.

While it is important to have access to information stored in one database or data warehouse, it is far better to have access to information contained in several databases or warehouses. The first step is to identify internal databases that are available and aligned to the institution's anti-fraud strategy, and that contain relevant information, e.g., customer/account databases, negative employee/entity databases, case-management systems. One challenge of efficiently using information is that of identifying which external databases would benefit from an anti-fraud strategy, as well as which data are actually available and/or able to be shared with others.

Once information is available and retrievable, it can be analyzed and linked with electronic tools, which create electronic visual reports that capture the links and relationships of data. The data range from names, addresses, telephone numbers, Social Security numbers, transactions, applications, and accounts, to photographs and external documents. The link and analytical tool lend themselves to non-complex fraud cases, but are most effective for complex cases involving many people, accounts, addresses and events.

Data input and structures are a different challenge. Information takes many forms and often one structure can take on different views. For example, the entry “John Smith” can be captured as “J. Smith,” “Mr. Smith.” It may also have slight alterations (keystroke errors), such as “Jon Smith,” or “John Smyth.” Information-management technology therefore must be able to query using “fuzzy” search tools. This applies not only to names, but also to addresses, dates of birth, and other key pieces of information.

So while it is important to recognize the value of technology as it applies to information management, it is equally important to recognize the need to employ technology to gather, manipulate, and analyze information, and generate reports that allow for the articulation of complex cases. Listed below are examples of technology that can be used to efficiently manage information. While they have broad uses and application to various management groups, they certainly play key roles in identifying and managing identity theft and fraud.

- **Database** – A database is a collection of information organized so that a computer program can quickly select desired pieces of data; in other words, it is an electronic filing system. Traditional databases are organized by fields, records, and files. A field is a single piece of information, a record is one complete set of fields, and a file is a collection of records. For example, a telephone book is analogous to a file. It contains a list of records, each of which consists of three fields: name, address, and telephone number.

An alternative concept in database design is hypertext. In a hypertext database, any object, whether it is a piece of text, a picture, or a film, can be linked to any other object. Hypertext databases are particularly useful for organizing large amounts of disparate information, but they are not designed for numerical analysis.

- **Data warehouse** – A data warehouse is a collection of data designed to support management decision-making. Data warehouses contain a wide variety of data that present a coherent picture of business conditions at a single point in time. Development of a data warehouse includes development of systems to extract data from operating systems and installation of a warehouse database system that provides managers with flexible access to the data. The term “data warehousing” generally refers to combining many different databases across an enterprise.
- **Link analysis tools** – Link analysis is a technique that reveals the structure and content of a body of information by representing it as a set of interconnected linked objects or entities. By visualizing the entities and links, one can identify what is missing. The resulting charts efficiently demonstrate the relationship of the data to management, law enforcement and legal issues.

- **Query/fuzzy search tools** – These tools are typically used for searching, matching and duplicate discovery on the following data structures:
  - Names
  - Addresses
  - Telephone numbers
  - Social Security numbers
  - Dates of birth
  - Drivers license numbers
  - Identification numbers
  - Gender
  - Eye color
  - Employer names and addresses
  - Titles
  - Company names
  - Organization
  - Free text descriptions
  - Account codes
  - Dates
  - Region

These search capabilities include querying multiple fields simultaneously and in multiple languages. Additionally, since typographical errors do occur and data entry methods vary by input structure, the query tool allows for fuzzy hits rather than rejecting near or close hits.

- **Case management systems** – Case management systems (CMSs) track incoming calls and other inputs (Web-based data entries) that result in a referral, assist, or investigation. These systems track referrals, assists, and investigations so that the current status of any activity performed on a case is readily available. CMSs also serve as a central source for investigation notes and actions, and have the capability to create immediate statistical reports.
- CMSs also serve as management tools by allowing supervisory staff to track an investigator's progress on a case, check the current status of cases, and close cases. CMSs help to ensure the efficient, effective progression of investigations and the efficient use of information for management reports, trend analysis, and archiving of historical data. This technology serves as a comprehensive data system when addressing issues of fraud and identity theft. It also eliminates or reduces manual and duplicate procedures by automating many tasks.
- A state-of-the-art CMS allows management to track specific types of cases and to cross-reference them with similar cases. The system allows tracking of fraud trends by fraud category, product, business unit, and geographic location, and facilitates the allocation of resources to counter the identified trends and threats.
- **Data mining**<sup>18</sup> – This is a buzzword for a class of database applications that look for hidden patterns in a group of data. Data-mining software has been used by marketing groups to help identify customers with common interests. However, it can also be used to ferret out criminals who have successfully opened accounts. Once a bogus application has been identified, the data from that application can be used to “mine” the account database to determine if similar information has been used to open other accounts.

---

<sup>18</sup> The term “data mining” is commonly misused to describe software that presents data in new ways. True data-mining software doesn't just change the presentation, but actually discovers previously unknown relationships among the data.

### **C. Information Security**

The information financial institutions gather, create, process, and use is one of their most valuable assets. Given the competitive nature of financial institutions, along with the significant value of the resources they manage, they must take all steps necessary to protect these assets. A compromise of this information could severely impact customers, constitute a breach of laws and regulations, and damage the institution's reputation and revenues. In addition, effectively securing information is essential to ensuring the privacy of customer information in accordance with internal and external privacy requirements.

Most institutions have refined their information-security services over the years, deploying new technologies to protect both internal and customer information. Information-security programs address information theft, thereby directly or indirectly deterring identity theft. Most financial institutions have continuously provided awareness education about information security to their employees, contract workers, and customers. Also, most have deployed state-of-the-art access controls, authentication and encryption systems, as well as stringent policies to protect against external attacks and internal fraud or abuse. So, while information security is a separate discipline strongly bent towards protecting and controlling all information with which institutions are entrusted, it is also a first line of defense against identity theft. Refer to the BITS Web site at [www.bitsinfo.org](http://www.bitsinfo.org) for additional information about BITS' Security and Risk Assessment Initiative, including the BITS Product Certification Program.

## **VIII. STRATEGIC PARTNERSHIPS**

Strategic partnerships can help significantly to combat identity theft. Most financial institutions participate in several associations that work to identify common problems and develop solutions. Organizations like BITS allow institutions to share information and experiences in controlled environments in which high levels of trust have been established.

It is clear that problems with the widespread, industry-level impact of identity theft must be addressed collectively. This white paper is evidence that strategic partnerships can play a major role in focusing the industry's attention and fostering productive communication between institutions. The challenge, though, is to not only prepare a white paper and recommend possible solutions, but to promote continued cooperation and information sharing among financial services companies to implement these solutions on a voluntary basis.

### **A. Financial Institutions**

Though BITS and other industry associations offer programs that allow financial institutions to discuss identity theft issues and solutions, more can be done on the industry level. Today many financial institutions use vendor services to vet account opening information in order to ensure that they have met the Know Your Customer requirements and are discouraging criminal activity to the extent possible.

With certain vendor services, the amount and accuracy of the vendor's information depends on who is supplying it. Financial institutions using such services are encouraged to participate, reporting events to the vendor in a cost-effective manner. Additionally, institutions that use vendor resources must work together to help ensure that the vendor manages the information properly, that the service is usable and reliable, and that its purpose is limited to helping participating organizations.

Financial institutions must continue to work together and, when appropriate, with vendors, to develop new methodologies to validate customer information. They should also seek out new technologies to help reduce the risk of fraudulent accounts being opened and prevent other forms of fraud from occurring.

### **B. Financial Institutions, Credit Bureaus, and Law Enforcement**

Another dimension of information sharing is the growth of strategic partnerships with other key stakeholders. With identity theft, this includes credit bureaus and law enforcement (federal and state) as partners. Each of these entities possesses information that, when used in concert with financial institution data, can help to intercept and prevent identity theft. A cooperative relationship between credit bureaus and financial institutions will help to address the inclusion of relevant information in a credit report. However, currently the most useful information is that collected and maintained by law enforcement agencies and other government entities such as the FBI, state police and the FTC.

Understandably, these entities cannot share the details of the information they collect. However, financial institutions could potentially use the information without the entity having to disclose any information directly; instead, an inquiry could be responded to with a

cautionary note back to the institution. For example, the FTC collects complaints from victims of identity theft. During account opening, financial institutions could provide information to the FTC database to determine if the potential customer has registered a complaint of identity theft with the FTC. The institution would not have access to any details of the report, but if the reporting party is required to include a police agency name and case number, that information is public and could potentially be shared with the inquiring institution. This is just one example of how strategic partnerships and leveraging information can benefit the industry and the customer while also addressing government concern about identity theft.

There are likely to be other potential partnerships and means of sharing information—even limited amounts of information—that will help mitigate identity theft. However, in order to accomplish this, key players must develop processes for working together.

### **C. Technology Developers**

In addition to the strategic partners already identified, financial services industry requirements for authenticating customers should also be communicated and positioned as industry standards that technology developers must meet. The financial services industry would be best served by collectively and mutually agreeing on what technology solutions are needed or need strengthening, and then communicating those needs to the technology vendors clearly. Today this does happen on a one-on-one basis, with some institutions developing their own technology solutions. However, this process could be improved to create solutions usable throughout the industry.

## IX. CONSUMER AWARENESS AND EDUCATION

### A. Resources

A number of organizations have established programs to educate consumers about identity theft, including how to prevent it and provide advocacy for victims. The following organizations offer resources for consumers:

- **BITS, The Technology Group for The Financial Services Roundtable** ([www.bitsinfo.org](http://www.bitsinfo.org)) maintains tips for consumers to protect their security, especially in an online environment.
- The **Federal Trade Commission (FTC)** maintains [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) and 877-IDTHEFT, both of which allow consumers to register incidents of identity theft.
- The **Social Security Administration** ([www.ssa.gov/pugs/idtheft.htm](http://www.ssa.gov/pugs/idtheft.htm)) provides resources and articles.
- The **U.S. Department of Justice** provides information on identity theft at [www.usdoj.gov/criminal/fraud/idtheft.html](http://www.usdoj.gov/criminal/fraud/idtheft.html).
- The **FBI's Internet Fraud Complaint Center** ([www.ifccfbi.gov](http://www.ifccfbi.gov)) allows consumers to file a complaint.
- The **Federal Reserve Bank of Boston** ([www.bos.frb.org/consumer/identity/index.htm](http://www.bos.frb.org/consumer/identity/index.htm)) offers educational materials and links to other resources.
- The **Privacy Rights Clearinghouse** ([www.privacyrights.org](http://www.privacyrights.org)) is a nonprofit consumer education, research, and advocacy organization. Its publications provide information for consumers on how to control their personal information.
- **Victim's Assistance of America** ([www.stolen-identity.com](http://www.stolen-identity.com)) was created by an identity theft victim to help other victims clear their names.
- The **National Consumers League** ([www.nclnet.org](http://www.nclnet.org)) provides steps that consumers and businesses can take to secure information. Identity theft scenarios and examples of how thieves use personal information to commit fraud are also provided.
- The **Electronic Privacy Information Center** ([www.epic.org](http://www.epic.org)) is a resource for information on privacy-related topics, including pending identity theft legislation.

### B. Protective Steps for Consumers

#### Identity Theft Prevention

Because financial institutions are targets for fraud and identity theft, each institution must educate customers on how to protect themselves. There are many steps consumers can take

to decrease their identity theft risk. Listed below are some ways individuals can protect themselves from becoming identity theft victims. Financial institutions may choose to change internal practices to accommodate consumers' preferences (subject to the institution's policies).

### **Social Security Cards and Numbers**

- Do not carry your Social Security card.
- Remove your Social Security number from your driver license and bank checks.
- Release your Social Security number only when necessary—for example, on tax forms and employment records, or for banking, stock and property transactions.
- Do not give out your Social Security number without questioning how it will be used. (Be aware that if you refuse to give your Social Security number to a business, that business can refuse service if it feels the information is necessary.)
- Use a unique number as an account identifier instead of a Social Security number. When creating passwords and PINs, don't use any part of your Social Security number, birth date, middle name, spouse's name, child's name, pet's name, mother's maiden name, address, or consecutive numbers, i.e., anything that a thief could easily discover.
- Check your Social Security earnings and benefits statement each year to ensure that someone else is not using your Social Security number. (This statement can be ordered from the Social Security Administration.)

### **Credit Cards**

- Carry only one or two credit cards. When carrying cards, take precautions to prevent their loss.
- Always take credit card, debit card, and ATM receipts. Tear them up or shred them when no longer needed.
- Tear up or shred unused pre-approved credit card solicitations and convenience checks.
- Never provide credit card numbers over the telephone unless you placed the call and have a trusted relationship with the other party.
- Cancel unused credit cards.
- Create a list of credit cards and bank accounts. For each, include the account number, expiration date, credit limit, and telephone numbers for customer service and fraud departments. Keep this list in a safe place (not in a wallet or purse) so each creditor can be contacted quickly if cards are lost or stolen.

### **Internet**

- When making online purchases, be sure you know the entity or person to whom you are giving your personal information. To confirm the legitimacy of a site, click on the solid lock or key symbol on your browser window. The symbol provides information about the merchant from the server certificate. If the certificate was issued by an independent certificate authority, some due diligence has been performed on the business. A cloned site will not have a certificate. If a certificate name does not match the site, do not use it.
- Only do business with Internet companies that use secure technology to capture private information like account or credit card numbers, or place orders by telephone or mail. The key symbol on your browser status bar indicates whether or not a page is secure.
- Check merchant privacy policies and only shop with those whose published privacy policies are acceptable to you.

- Ensure your computer(s) are equipped with antivirus protection and firewalls to help keep trespassers out. Always maintain backup of your original data.

### **Mail**

- Do not leave bill payments in your mailbox. Install a lock on your mailbox if mail theft has occurred in your area.
- Immediately review credit card and utility statements, including cell phone bills, for unauthorized use. If you suspect your account has been used fraudulently, contact the provider's customer service and fraud departments.
- Monitor your bank accounts and monthly statements thoroughly, ensuring that all the activity is accurate. If your account statements are late, immediately contact your bank to find out when they were mailed.
- If credit card statements or new or renewed credit cards are not received in a timely manner:
  - Call the creditor to see if a change-of-address request has been filed, or if additional or replacement cards have been requested. If either has happened, instruct the creditor not to honor the request.
  - Contact the post office to see if a change-of-address request has been filed. If so, immediately notify your local postal inspector.

### **Miscellaneous**

- Never divulge personal information to anyone, including close friends and family members. No matter how good a reason a person might have for needing your information, do not give it away. (Often identities are stolen by skilled “social engineers” who have their stories down, know to what most people will respond, and understand that people are often willing to provide information to others if they perceive that it is needed or that they will benefit.)
- Keep your birth certificate and passport in a safe place.
- Always protect your account information. Memorize passwords and PINs—never keep them in a wallet, purse, or Rolodex. Never write a Social Security or credit card number on a check.
- Shield the keypad when entering a PIN at an ATM, store, or telephone to protect against “shoulder surfers.”
- Consider having your name removed from marketing lists by the following methods:
  - The three major credit reporting agencies develop lists of consumers who meet criteria specified by potential creditors. Limits can be placed on these “pre-approved credit offers” by requesting that information not be used for these purposes. Individuals who would like to have their name and address removed from mailing lists obtained from the main consumer credit reporting agencies should call 888-5OPTOUT (888-567-8688).
  - Request that credit card issuers not disclose to marketers any information based on the purchases you make.
  - The Direct Marketing Association (DMA) maintains lists of people who do not want to receive mail and telephone solicitations from national marketers. Request that your name be added to the DMA's Mail Preference Service and

Telephone Preference Service name-removal lists. For more information go to [www.dmaconsumers.org/offmailinglist.html](http://www.dmaconsumers.org/offmailinglist.html).

- Order a credit report each year from each of the three major credit reporting agencies. Check the reports for accuracy and indications of fraud, such as new accounts, unauthorized credit applications or inquiries, and any unrecognized charges, defaults or delinquencies. Also check the accuracy of your name, address, Social Security number, and other identifying information.

### **Corrective Action for Victims**

It is critical to act quickly upon learning of a possible identity theft. While each case is different, the following tips can help consumers understand how to report the identity theft and begin to rebuild their credit:

- Report the crime to the police immediately and ask for a police report. (Creditors, banks, credit reporting agencies and insurance companies may require a police report to verify the identity theft.) Consumers may also call the FTC at 1-877-IDTHEFT.
- Keep a log of the date, time and substance of telephone conversations regarding the theft. The log should include the name, title, and telephone number of each person with whom the victim spoke. Follow each call with a letter confirming the conversation and any agreed-upon action. Send correspondence by certified mail, return receipt requested, and keep a copy of each letter and return receipt.
- Call the fraud units of one of the three major credit reporting agencies and report the theft. Any one bureau will notify the other two. Be sure to request that each reporting agency take the following actions:
  - Check each credit report carefully for accounts, charges, inquiries, defaults and delinquencies for which you are not responsible. All personal identifying information should be verified.
  - Place a fraud alert in your account file. Ask how long the alert will remain in the file.
  - Add a victim’s statement to the credit report. For example: “My identification has been used to apply for credit fraudulently. Call me at \_\_\_\_\_ to verify any application for credit.”
  - Have a copy of your credit report sent to you. The agency must give a free report to any consumer who has been denied credit or has certified in writing that they believe their file contains inaccurate information due to fraud. (In other circumstances, agencies can charge for credit reports.)
  - Remove information that appears as a result of the theft of personal and credit information. (It may take some time to have all erroneous information removed from each credit report.)
  - Have a copy of the corrected credit reports sent to you. When received, verify that erroneous information has been removed and that the report contains the fraud alert and victim’s statement as requested. It’s a good idea to send a letter to each agency every two to three months explaining the identity theft and requesting a free copy of your credit report. This will enable you to check for new erroneous information and previously deleted erroneous information that may have reappeared.
- Call each of your credit card issuers to report the theft. Each issuer should cancel their card and provide a replacement with a new account number. Confirm the telephone call with a letter. During the call, be sure to:

- Ask about the status of the account and whether the issuer has received a change-of-address request, or a request for additional or replacement credit cards. Instruct the card issuer not to honor unauthorized requests.
- Inquire about waiving all unauthorized charges, including the initial \$50. (A consumer’s liability for unauthorized use of a credit card cannot exceed \$50. The consumer must notify the credit card issuer promptly upon learning of the unauthorized use. Most creditors will waive the \$50 if the consumer notifies the creditor within two days after learning of the problem.)
- Call each credit card issuer or creditor that has opened an unauthorized account. Explain the incident of credit identity theft, and ask each issuer and creditor to close the accounts immediately. These accounts probably will be listed in your credit reports. Ask each issuer and creditor to inform each credit-reporting agency that the fraudulent accounts have been closed.
- If bank account information or checks have been stolen, or if a fraudulent bank account has been opened using personal information, notify the bank and check verification companies listed in Section VIII, A. Be sure to also:
  - Close checking and savings accounts and obtain new account numbers.
  - Call the payees of outstanding checks. Explain the identity theft and note that your checking account has been closed. Ask each payee to waive late-payment or returned-check fees. Send each payee a replacement check drawn on the new account and stop payment on the check that it replaces. Enclose a note explaining why a replacement check is being sent and reminding the payee of any agreement to waive late-payment or returned-check fees.
  - Get a new ATM card, and don’t use your old password or PIN.
  - If a merchant refuses to take a check on the advice of a check verification company because a thief has written bad checks on the account, call the check verification company and explain the situation.
  - Notify utility companies such as gas, electric, water and trash-collection service providers and inform them of the identity theft. Also alert them to the possibility that the thief may try to establish accounts using fraudulent information. Notify local, long-distance and cell phone providers. If calling cards or PINs have been stolen, cancel them and obtain replacements.
  - Ask banks, utilities, and telephone companies to use new, unique identifiers for all accounts. Do not use your mother’s maiden name.
  - If a driver’s license has been lost or it is suspected that someone may be using the driver’s license number, contact the local department of motor vehicles (listed under “state government” in the telephone directory). It is possible to obtain a new driver’s license number under some circumstances.
- If you think someone is using your Social Security number for work or another purpose, or if you receive a notice from the Internal Revenue Service of unreported taxable income that is not accounted for, report the situation to the Social Security Administration. Their representatives will take steps to ensure that earnings records are correct.
- Banks and credit grantors may require that fraud affidavits be notarized. You can ask to have the notary fees waived or reduced.
- If you suspect that an identity thief has stolen your mail or made a change-of-address request, notify the local postal inspector.

## **X. INTERNATIONAL (UK) CASE EXAMPLE: APACS**

In the United Kingdom (UK), a project led by the Association for Payment and Clearing Services (APACS) is helping financial institutions and government to understand the scope of identity theft and define methods to prevent it. With participation from organizations such as major UK banks, credit reference agencies, the British Bankers Association, the Credit Industry Fraud Avoidance Scheme (CIFAS), Metropolitan Police and various government groups, this effort focuses on education, best practices, data reporting, data sharing and technology.

### **Education**

In an effort to help consumers understand how to reduce their susceptibility to identity theft, APACS is developing:

- Consumer messages and educational documents to be communicated to the public through channels such as APACS, credit reference agencies, CIFAS and/or Home Office (possibly through TV advertising); and
- An awareness program, which can be applied by any banking institution and modified for use by other sectors, to help minimize identity theft within the organization.

### **Best Practices**

APACS members are developing an “Identity Theft Fraud Best Practice Guide.” APACS members will be encouraged to review their internal practices and procedures with a view to implementing the best practices covered in the guide. The guide could be promoted to other sectors and/or could encourage similar industry bodies to develop their own best practices.

### **Reporting**

Efforts are underway to develop a methodology for reporting suspected and proven identity theft activity in the credit card industry and beyond. Universal procedures to help facilitate criminal investigation will be developed around the following steps:

- Reporting proven incidents to other organizations for the purposes of limiting further fraudulent activity;
- Reporting suspicious or proven incidents to the police for the purposes of further investigation and/or prosecution; and
- Reporting proven incidents to APACS for the purposes of collating management information for the industry.

### **Data Sharing**

APACS is working to identify effective and feasible means of sharing data to reduce identity theft fraud, and particularly of using data to assist during the containment phase of the identity-theft lifecycle. Historically, the credit card industry has greatly relied on central fraud databases, such as CIFAS and the credit reference agencies, to assist with credit scoring and authenticating the genuine identity of new customers. This data sharing has been operated on a reciprocal basis.

Since identity theft is known to migrate among financial institutions and, in some cases, other sectors, the ideal data-sharing solution would involve a knowledge base of all known identity theft attempts to curtail migration. However, the success of this ideal solution is dependent on:

- The availability of reliable data;
- The inability to always achieve perfect data matches (i.e., the variability of address formats);
- Commercial constraints; and
- Data protection issues.

### **Data Access**

An Experian proposal drafted a system designed to assist financial institutions and credit grantors with identifying the occurrence of identity theft. This system would monitor address changes from multiple sources, in conjunction with other sources of data including:

- Electoral register;
- Address re-directions file;
- Telephone subscriber file; and
- MOSAIC socio-economic classification data.

Another proposal involved the Verification Information System (VIS). The VIS is used in the Netherlands by over 9,000 organizations, primarily in the financial sector but also by other public and private groups. VIS is a database of missing documents taken from more than 180 different countries. It primarily holds missing passport numbers and visas, but also links into the Dutch Driving License and Moped Certificates Register (CRB), allowing organizations to search for lost driver's licenses as well as other documents. VIS is operated by the National Criminal Intelligence (CRI), which is part of the Dutch National Police Service and BKR, the Dutch Credit Reference organization (similar to Experian or Equifax in the U.S. but nonprofit).

This effort is considered to be a practical way of sharing data from multiple sources. The data in the VIS system could possibly be made available to financial organizations through the credit reference agencies or via the Internet.

### **Technology**

Technology is used to combat crime in all sectors of industry and commerce, including law enforcement. Within the card-payment sector the recent introduction of chip cards to reduce counterfeit fraud provides an opportunity to leverage the significant investment in technology infrastructure to achieve further reductions in various types of fraud.

Within the context of identity theft, APACS is largely focused on the use of technology to assist during the prevention and containment phases of the identity theft lifecycle. A number of technologies have been considered, including biometrics, dynamic CV2 including dynamic code generation and random challenge, and finally neural network based scoring systems.

## **XI. RECOMMENDATIONS AND NEXT STEPS**

There are many things financial institutions can do to combat identity theft. At the industry level, institutions can take steps to work with each other and with other organizations to combat identity theft. At the individual institution level, know your customer and know your employee practices are critical tools in preventing identity theft.

### **A. General Recommendations and Next Steps**

In order to successfully decrease the incidence of identity theft, consistency of efforts is needed among financial institution. Also essential are credit bureau efforts to coordinate with financial institutions and share information among other credit bureaus. The following steps are suggested to help create consistency at individual organizations and across the industry:

- Financial institutions should implement a process to isolate identity theft incidents from other reported fraud and report monthly to appropriate levels of management. Sort the incidents by major products, such as credit cards, other consumer products.
- Communication channels between financial institutions and credit bureaus should be established to share information about trends and techniques of for fighting identity theft and to collectively develop countermeasures.
- A methodology for sharing reported incidents of identity theft between defrauded firms and the credit bureaus should be developed.
- All stakeholders should encourage and support prosecution of identity thieves.

BITS will continue in its efforts to combat identity theft through the BITS Fraud Reduction, Authentication, and Security and Risk Assessment Working Groups. Next steps will include:

- In cooperation with The Financial Services Roundtable, promoting the industry-wide adoption of the “Financial Institution Voluntary Guidelines: Identity Theft Prevention and Victim Assistance.”
- Continuing to promote the industry’s adoption of the definition of "identity theft" as identified in this paper.
- Developing a methodology for collecting MIS from participating banks on reported incidents of identity theft and other key components of victim resolution, losses, etc., through the efforts of the BITS Statistics Working Group.
- Working with other industry organizations and government agencies on a campaign to communicate with the public on identity theft issues.
- Researching and sharing financial institutions’ strategies for mitigating identity theft and identifying key consumer identity-theft reporting issues.
- Developing a model for account opening that incorporates identity-theft mitigation technology, processes, and information.

Finally, a government process by which federal agencies, particularly the FTC, safely share reported incidents of identity theft with financial institutions could be a key tool in preventing identity theft.

### **B. Know Your Customer Practices**

The U.S.A. Patriot Act passed in October 2001 states that financial institutions must “implement reasonable procedures” upon opening new accounts to verify potential

customers' identities. Further, the Act states that records of the identification used during the verification process must be maintained and screened for affiliation with terrorist organizations. Know Your Customer (KYC) practices help organizations meet these new requirements and mitigate identity theft.

For account openings, institutions should take the following KYC-related steps:

- Maintain a customer identification program (CIP) with reasonable procedures for identifying any person, including businesses, to open an account.
- Maintain procedures for verifying the identity of customers (i.e., any signer) opening an account.
- Require information used to verify the customer's identity to be retained. This includes the person's name, address, date of birth, tax identification number, and other identifying information.
- Determine whether a customer appears on any lists of known or suspected terrorists issued by the federal government (through internal records and third-party vendors).
- Maintain firm policies for determining the point at which an account should not be opened because the person's identity cannot be verified.

Customers should be properly identified using two acceptable forms of identification.

Acceptable forms of identification are:

- Bank-issued ATM card or debit card.
- Driver's license with photo (original, not duplicate). Includes U.S. territories, such as Puerto Rico, as listed in the *ID Checking Guide* published by the Drivers License Guide Company. (These must be accepted with care since many do not contain the same security features as state licenses. Consult the *ID Checking Guide* for a description.)
- New Jersey non-photo driver's license (original, not duplicate).
- State-issued learner's permit with photo.
- State-issued non-driver's ID card with photo.
- State, county, or city-issued senior citizen ID card with photo.
- Military ID card with photo.
- U.S. or foreign passport with photo.
- Mexican consular ID card with photo.
- U.S. Immigration and Naturalization Service (INS) issued Alien Registration Card with photo (includes Resident Alien and Employment Authorization Cards).
- State, county, or city-issued welfare/public assistance card with photo.
- EBT (Electronic Benefits Transfer) card with photo.
- Major credit card (American Express, Visa, MasterCard, Novus).
- New Jersey Casino Commission and Connecticut Casino Commission ID cards.

An exception may be made for a customer verified as a "known customer" with branch manager or designee approval. However, the institution must be able to prove that the person was at some prior time properly identified and verified in a way that meets the requirements of the regulation.

Compare the identification to the presenter. Determine the following:

- Does the picture resemble the customer?
- Is the date of birth reasonable?
- Do the eyes, hair and height of the customer match the description?

- Is the information on the identification (i.e., name, address, etc.) consistent with the information verbally provided by the customer?
- Is the identification provided consistent with the customer's situation? (For example, is a non-resident alien contradictorily presenting an INS-issued alien registration card or "green card"? Is a person born after 1943 presenting a senior citizen ID card?)
- What is the date of issuance? If the ID was issued in the last 60 days, be cautious. Recently issued identification is more likely to be fraudulent.

Examine both forms of identification to determine whether the information is consistent. If there are any discrepancies, ask the customer to explain. Proceed only if he or she provides a reasonable explanation, such as "I colored my hair when that picture was taken," "I've since moved after I obtained my driver's license," or "I changed my name after I married."

### **C. Know Your Employee Practices**

Criminals have been known to use customer information obtained from financial institution employees to advance their identify-theft schemes. Most, if not all institutions are intent upon keeping criminals out of their ranks and identifying criminals within their organizations in order to root them out. This is especially true when the criminal activity has a direct connection to the honesty or trustworthiness of the employee.

Two critical Know Your Employee (KYE) tools are background screening and a code of conduct process. Background screening, especially for criminal records, is essential for keeping unwanted employees out and identifying those that should be removed. A code of conduct process is an important method for communicating the company's values and key rules of behavior to employees and requiring them to comply.

#### **Background Screening**

Most large organizations, particularly large financial institutions, have been performing background screening on prospective employees for quite some time. Some have begun to screen current employees as well.

Financial institutions conduct background screening in a number of different ways. The FDIC does not require a specific type of screening process, but instead expects a reasonable inquiry "which consists of taking steps appropriate under the circumstances." Some institutions use the name and date of birth of the new employee to check with the county clerk to determine whether the person has a criminal record. (This may be appropriate for a small institution hiring a person who has lived all or most of his or her life in that county.) The criminal record search can proceed through higher levels, including statewide and national searches. One method for conducting national searches is by fingerprinting the new hire and sending the prints to the FBI, where they are run against the National Crime Information Center (NCIC) database.

Any level of search—local, state or national—can be conducted by the employer itself or by a vendor. Searches can either be limited to criminal record searches or can involve more extensive background checking, which may include additional features, such as credit checks, and verification of Social Security number, education and employment.

Sharing information about a former employee with his or her prospective new employer is a delicate matter. Employers generally provide only basic information as to tenure, position and compensation. The risk of lawsuits for defamation deters them from providing any further information. This may change as the industry adjusts to new legislation encouraging certain disclosures.

A provision in the USA Patriot Act, Section 355, amends Section 18 of the FDIA by adding a section covering written employment references that contain suspicions of involvement in illegal activity. The amendment provides that, while not an affirmative duty, any insured depository institution may disclose its suspicions of an employee's possible involvement in potentially unlawful activity in any written employment reference provided to another insured depository institution and be shielded from liability to the person identified in the disclosure, unless it is made with malicious intent. An open question is whether this safe harbor will be relied upon. While it is not a guarantee against litigation, it does set a higher standard (malicious intent), for a claimant to prevail.

### **Codes of Conduct**

Another important KYE method is a formal code of conduct process. This consists of drawing up a code of conduct or ethics that sets forth the key, general guidelines and rules of behavior for the company, disseminating it on a regular basis, and requiring some form of disclosure and certification by employees. This way, the employer demonstrates its diligence in promulgating the standards it expects employees to follow, obtains employee compliance with these standards, and requires their continued acknowledgment of the standards.

Methods of communicating a code of conduct and obtaining employee disclosures and certifications vary from organization to organization. Some provide their code in booklet or pamphlet form to all new hires, and to all employees on a periodic basis, or whenever substantive changes are made. Some create training videos that include vignettes depicting employees in situations where ethical issues arise and decisions must be made; a viewing of the video may be followed by a summation by a member of management, or even a short quiz. Others, after distributing the code, poll their employees with a questionnaire. The questionnaire may be lengthy, containing questions that correspond to elements of the code, to which yes or no answers are supplied, or may require disclosure of all outside affiliations or potential conflicts of interest. It may also include both elements.

Codes of conduct often require employees to report violations of the code, making an employee's failure to report a breach of the code a violation itself. This deputizing of all employees underscores the code's importance. Some codes provide a confidential hotline to an ombudsperson or another function in the organization capable of responding to code-related issues, such as human resources, corporate security, audit, legal or compliance.

The existence of a code of conduct sends an important message to employees. A code of conduct and a robust code of conduct process that includes dissemination, training, disclosure and certification, demonstrates that the organization values ethical behavior enough to take significant steps to formally integrate it as a standard in its corporate culture.

### **The Cost of KYE**

All employers must weigh the costs and benefits of implementing or enhancing background screening and a code of conduct process. An assessment of the risks involved and how the implementation or enhancement will address those risks, including whether the risks are significant enough to require the action proposed, is a critical part of this analysis. While some form of background screening is mandatory for financial services companies in order to comply with legal requirements, the nature and extent of the screening will depend on the size of the firm, the nature and geographic reach of its business, and the nature and location of its target labor pool. The type of screening will also be influenced by the company's hiring experience, as well as by industry practice.

## **XII. CONCLUSION**

Identity theft is a major problem that cannot be solved by financial institutions alone. The industry needs the cooperation of other businesses, government, and, perhaps most importantly, the public.

Still, there is much that institutions can do. One basic step is to adopt a common definition of identity theft and be sure key institution employees understand the problem thoroughly. This paper suggests the following definition: “the unlawful capture and/or use of another person’s identifiers to impersonate him or her in the commission of a crime or to gain financial benefit.” When all interested parties agree on what is being talked about when the term is used, discussions can be more effective and solutions arrived at more swiftly.

Institutions should also be aware of existing and proposed legislation—both federal and state—related to identity theft. It is a good idea to keep abreast of privacy laws as well, which can work against identity-theft prevention efforts by limiting information sharing.

Another step institutions should take is to familiarize themselves with the mitigation practices outlined in this paper and keep abreast of new technologies and processes. Though these practices do not reflect an industry standard, they are widely agreed to be among the most effective tools institutions have to mitigate the problem. Smaller institutions that may not have the resources to implement some of these processes should be aware of their existence and should implement prevention tools to the extent reasonable.

Finally, institutions should work with their customers to increase their awareness of identity theft issues. Well-educated customers can be a great asset in preventing identity theft. Informing customers about identity theft issues can also help a customer to be more prepared if he or she does become a victim.

The current environment in which identity theft crimes are thriving took years to develop, and it will likely take years to implement effective means of preventing identity theft. No one single solution or piece of legislation will solve the problem. Instead, a concerted effort by businesses, law enforcement, government and the public is needed to curb its growth and reduce the incidence of identity theft. As noted in this paper, strategic partnerships are essential to truly effectively address the problem. As part of this effort, the BITS Fraud Reduction Steering Committee, through its Identity Theft Working Group, will continue to work not only with member financial institutions of BITS and The Financial Services Roundtable but also with credit bureaus and government agencies to explore solutions and recommend appropriate action.

This white paper seeks to educate the industry and recommend measures that institutions have tested and found to be most effective. However, it is not intended as a conclusive document. Instead, its purpose is to stimulate individual institutions to take action and encourage discussion among all interested parties.