



STAR_{sm} Update on ID Theft and ID Fraud

www.STAR.com

Presented to

The Smart Card Alliance

February 12, 2003

Julie Saville

Star Systems[®], (STAR_{sm})

a Concord EFS, Inc. Company



STAR White Paper Series

- ◆ **Developed to educate 6,200 STAR financial institution members on the issues of identity theft and identity fraud**
- ◆ **“Heightened Security: Can Financial Institutions Really Know Their Customers?”**
 - Topic focused on era of heightened security, highlighted by creation of USA Patriot Act
 - Paper surveys identity documents and national ID card debate
- ◆ **“Identity Theft in the United States: An Update”**
 - Compiles the most recent data available from studies by the GAO, FTC, ABA and STAR



Current Identity Fraud Prevention

- ◆ **Financial industry already utilizes fraud protection as matter of course**
 - “Know thy Customer” verifications for new accounts
 - PIN to get cash at ATM
 - Cardholder’s photo on credit card
 - Participating in databases that prevent check fraud
 - Neural scoring of card use patterns
 - To a limited extent smart cards, digital signatures and other technology
- ◆ **Unfortunately growing identity theft, deposit account exposure through e-commerce, acts of terrorism:**
 - Place additional layer of burden on FIs to police crime
 - Suggest that just being in compliance with regulations isn’t enough
 - Multiple tools in arsenal help prevent exposure to money laundering liability, use by identity thieves, costly consumer fraud

Identity Fraud Defined

◆ **Creating a new identity**

- From scratch or
- Cobbling together a name, address, DOB, SS number from several sources
- To evade detection and commit crimes

◆ **Enables**

- Obtaining drivers licenses
- Credit cards, bank accounts
- Housing, transportation, flight training

◆ **Combating Identity Fraud a major goal of USA Patriot Act**

- Not a sea change from current FI activities, but raises awareness about need to redouble efforts

Identity Theft Defined

- ◆ **Criminal's wholesale takeover of someone's identity ("True Name Fraud")**
 - Including Name, birth date, social security number, and financial accounts
- ◆ **Enables**
 - Obtaining drivers licenses
 - Takeover of existing bank accounts or opening new accounts
 - Takeover of existing credits cards or obtaining new cards
 - Obtaining loans
 - Diverting government benefits such as social security
- ◆ **Combating Identity Theft a goal of 13 current pieces of federal legislation**
 - No federal legislation was passed in 2002 despite similar efforts

Industry Impact

- ◆ Losses to FIs projected to exceed \$8 billion by 2004 (Celent)
- ◆ 34% of check fraud at community banks due to identity theft (ABA 2002)
- ◆ Credit card losses from identity theft up
 - Associations report losses +43% to \$114.3M in 2000
 - Law enforcement reports the associations lost \$1B (GAO 2/02)
- ◆ Nearly 300,000 fraud alerts placed on consumer credit files in 2000 (GAO)

Consumer Impact

- ◆ ID theft crime has reached epidemic level
- ◆ 5.5% of U.S. adults have been the victim of identity theft
 - 11.8 million victims
- ◆ 19.2% *personally* know someone who has been the victim

Source: STAR/Market Facts 2002

- ◆ Victims reporting to the FTC increasing

2000	2001	2002
31,117	86,198	161,819

Consumer Impact

- ◆ Victims often experience multiple types of fraud (FTC 2002)
 - 42% Credit Card (new or account takeover)
 - 22% Utility (new wireless, phone or other)
 - 17% Bank Fraud (new or account takeover, wire transfers)
 - 9% Employment-related
 - 8% Government document or benefits
 - 6% Loan (personal, business, auto or home)
 - 16% Other (conducted crime, investments, medical)
- ◆ Between 1-4 credit card accounts are opened on the identity of the average victim

Consumer & Industry Impact

- ◆ Average fraud loss = \$11,100
 - 67% said they were ultimately had to pay \$0 (not incl. lawyers fees, time away from work)
 - 33% had to pay from <\$500-\$10,000
 - Net, the majority of quantifiable losses absorbed by financial industry
- ◆ Conservatively, a median loss of \$2,000 reflects a total impact of \$23.6 billion to date nationwide

Barriers to Prevention

- ◆ Despite epidemic losses, barriers to resolving identity verification issues remain
 - Privacy concerns
 - ID document weakness
 - Law enforcement participation
 - Consistent use of available tools

Barriers to Verification: Privacy concerns

- ◆ **Concerns about privacy reflected in polls**
 - Polls conducted just after 9/11 found support for national ID
 - Harris 68%, Pew 70%
 - Support slipped by 11/01
 - Washington Post 44%
 - And further by 3/02
 - Gartner Group 26%
 - 3/02 Harris Poll found support still high (59%)
 - But only 12% confident U.S. would use expanded surveillance in a proper way (down from 34%)

Barriers to Verification: Privacy concerns

- ◆ **Concerns about privacy remain high, even as concern about personal security/safety decreases**

How concerned were/are you about your personal safety:		
Before 9/11	Right after 9/11	Today
10%	37%	24%

How concerned were/are you about your financial privacy:		
Before 9/11	Right after 9/11	Today
21%	32%	30%

Source: STAR/Market Facts 11/02

Barriers to Verification: ID documents

- ◆ **Current ID documents unreliable**
- ◆ **Issued by multiple government sources**
 - Local, state, national, foreign
- ◆ **Major safeguards lacking**
 - Uniform procedures for official state IDs
 - Governmental verification processes
 - Meaningful biometric identifiers
 - Real-time commercial verification products
- ◆ **Used for purposes beyond original scope**
 - Drivers' Licenses: License to drive
 - Birth Certificates: Public health document
 - SS Numbers: Facilitate payment of retirement and disability benefits
 - Student and tourist visas: Time-limited visitation

Barriers to Verification: ID documents

◆ Drivers Licenses

- Roughly 270 different state formats
- 6 states do not have even have minimum security standards of magnetic stripe or 2-D barcode
- One state has encryption method that can't be read by third parties to verify validity of data
- States store information differently – digital photo images and driver data which prevents sharing state-to-state

◆ Birth Certificates

- 14,000 different certificate formats
- Issued by approximately 6,000 agencies nationwide

Law Enforcement

- ◆ Federal crime: Identity Theft and Assumption Deterrence Act of 1998
- ◆ State crime: 44 states have ID theft statutes
 - No clear rules determining what agency handles what cases
 - Willingness to handle varies by loss level
 - Tampa >\$10,000; LA, Miami, New York >\$50,000
 - In 2,000 limited cases prosecuted:
 - US Attorneys' offices 2,172; FBI 922 arrests; Secret Service closed 7,100 cases averaging \$217,700 fraud each
 - FTC Sentinel Network provides database to generate leads for investigators
 - Only 408 of >18,000 state & local agencies access
 - Of 161,100 victims filing with the FTC (2002), only 9% got a police report

FI investment in ID fraud prevention tools

Bank size	% regarding ID fraud as major threat	% investing X \$ ranges annually in loss avoidance	% of check-fraud losses attributable to ID fraud
Community (Assets <\$500M)	38%	59.2% invest <\$5K	34%
Mid-size (Assets \$500M - \$5B)	40%	24.4%: <\$10K 27.0%: \$10-50K 28.4%: \$50-250K	19%
Regional (Assets \$5B - \$50B)	40%	25.7%: \$50-250K 25.7%: \$250K-1M 31.4%: \$1-5M	13%
Super-regional (Assets \$50B+)	60%	31.3%: \$1-5M 18.8%: \$10-20M 18.8%: >\$20M	4%

Source: 2002 ABA Deposit Account Fraud Survey



Barrier to Verification: Use of Tools

- ◆ **Some tools require time rather than technology:**
 - SARs (Suspicious Activity Report)
 - Subjective, based on individual FI judgment -- making use inconsistent
 - FinCEN (Financial Crimes Enforcement Network) recently provided electronic filing process to improve
 - Recent crackdown on inconsistent filing—Western Union
 - Treasury Department OFAC: List of terrorism-sponsoring organizations and drug traffickers

Barriers to Verification: Use of Tools

- ◆ **A variety of technology-based verification tools available include:**
 - International negative-file database
 - Neural-net models that analyze applicants' info
 - Desktop/handheld scanner that reads mag stripe and 2-D barcode
 - National repository of data for comparison to detect duplicate or inconsistent info

Summary

- ◆ FIs long involved in fraud prevention
- ◆ Stakes are now higher:
 - Increasing fraud losses
 - New regulations heighten expectations
 - Non-enforcement liability
- ◆ Official tools/documents weak, inconsistent
- ◆ Industry-created tools on the forefront, but:
 - Need to be used to be effective
 - Should be part of an arsenal -- multiple fronts and types of fraud