

Identity Theft

...Building Your Customer's Trust

Biometric Consortium Conference 2004

Joel S. Lisker, Dudinsky Lisker &
Associates, LLC

Evolution of Payment Card Fraud

1983 re-embossed counterfeit fraud

1988 Re-encoded counterfeit fraud

1989 Card not present fraud

fraud applications

1991 Never received issued fraud

1992 Merchant fraud

1994 Identity Theft

2000 Hack & Attack

Web-based account compromise

2001 Skimmed counterfeit

2002 Server Hacking

2003 Communications interception

2004 Phishing Attacks/Schemes

- As difficulty to perpetrate fraud increases financial incentives decrease...but, in the case of identity theft, the horrific impacts to the lives of the victims do not abate, they only intensify

Identity Theft - An Overview

- Dubbed by the Department of Justice as the “crime of the century”, Identity Theft refers to all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain.
- The following are some of the most common types of identity theft complaints:
 - Payments Card Fraud
 - Unauthorized Phone or Utility Services
 - Bank Fraud
 - Fraudulent Loans
 - Unauthorized Access to Government Documents or Benefits

Identity Theft - Issues

- Approximately 50% of all identity theft victims reported that a Credit Card was opened in their name or unauthorized charges were placed on existing cards. Amongst the major sub-categories of Credit Card related fraud are:
 - Account Takeover
 - Fraudulent Applications
- Approximately 16% of all Identity Theft victims reported that a new bank account had been opened in their name, checks written, or unauthorized withdraws made.
- In the U.S. alone, more than 900,000 consumers became victims of identity theft during 2003.

Identity Theft - Issues

- One major global consumer bank reported that 30% of fraud - unrelated to payments cards, involved identity theft.
- Not easily recognizable by financial institutions - often times mistaken as an individual's credit problem
- Lack of familiarity on part of law enforcement in this burgeoning category of fraud, thereby limiting effective investigative capability
- Requires concerted education effort for:
 - Consumers
 - Financial Institutions
 - Law Enforcement Agencies
 - Government Regulators

Criminal Investigative Difficulties

- Delayed reporting/no reporting months/years
- Multiple jurisdiction investigations required
 - Criminal and victim rarely in same jurisdiction
 - Nearly impossible for state and local investigators
- Venue issues involving opening investigations -- where/when
- Multiple Subpoenas required, even for fraudulent accounts
 - Law enforcement is charged with subpoenaing fraudulent accounts
 - Delayed investigative results
- Result: State/local investigator/small police forces are helpless and overwhelmed

Biometrics – Applications for the Payment Card Industry

Given the focus on identity compromise and account takeover it appears that a biometric CVM may offer a secure solution to these burgeoning threats:

- Because, above all anonymity is a critical factor in the enabling of fraud, the elimination of anonymity with protection for privacy will, in and of itself, impact fraud significantly
- Biometric template should reside on off-line IC platform to ensure privacy

Today-

- Overview, based on FBI's leadership and work by private sector in dealing with the crime of ID theft and the aftermath
- A presentation on the impact to ID theft through a biometric solution
- Potential platforms for biometric augmentation leading to authentication