Information-Based Identity Authentication

Gary R. Gordon, Ed.D.
Economic Crime Institute at Utica College

Knowledge Based Authentication Symposium
Gaithersburg, MD
February, 2004

Identity Fraud: A Critical National and Global Threat

- A White Paper released Oct 28, 2003
- A Joint Project of the Economic Crime Institute at Utica College and LexisNexis
- Team
  - Gary R. Gordon, Ed.D., Utica College
  - Norman A. Willox, Jr., LexisNexis
  - Thomas Regan, JD., LexisNexis
  - Donald Rebovich, Ph.D., Utica College
  - Judy Gordon, MLS, Utica College

The Identity Problem / Threat

- A government problem
- A commerce problem
- A law enforcement problem
- A national security problem
- A domestic problem
- A global problem

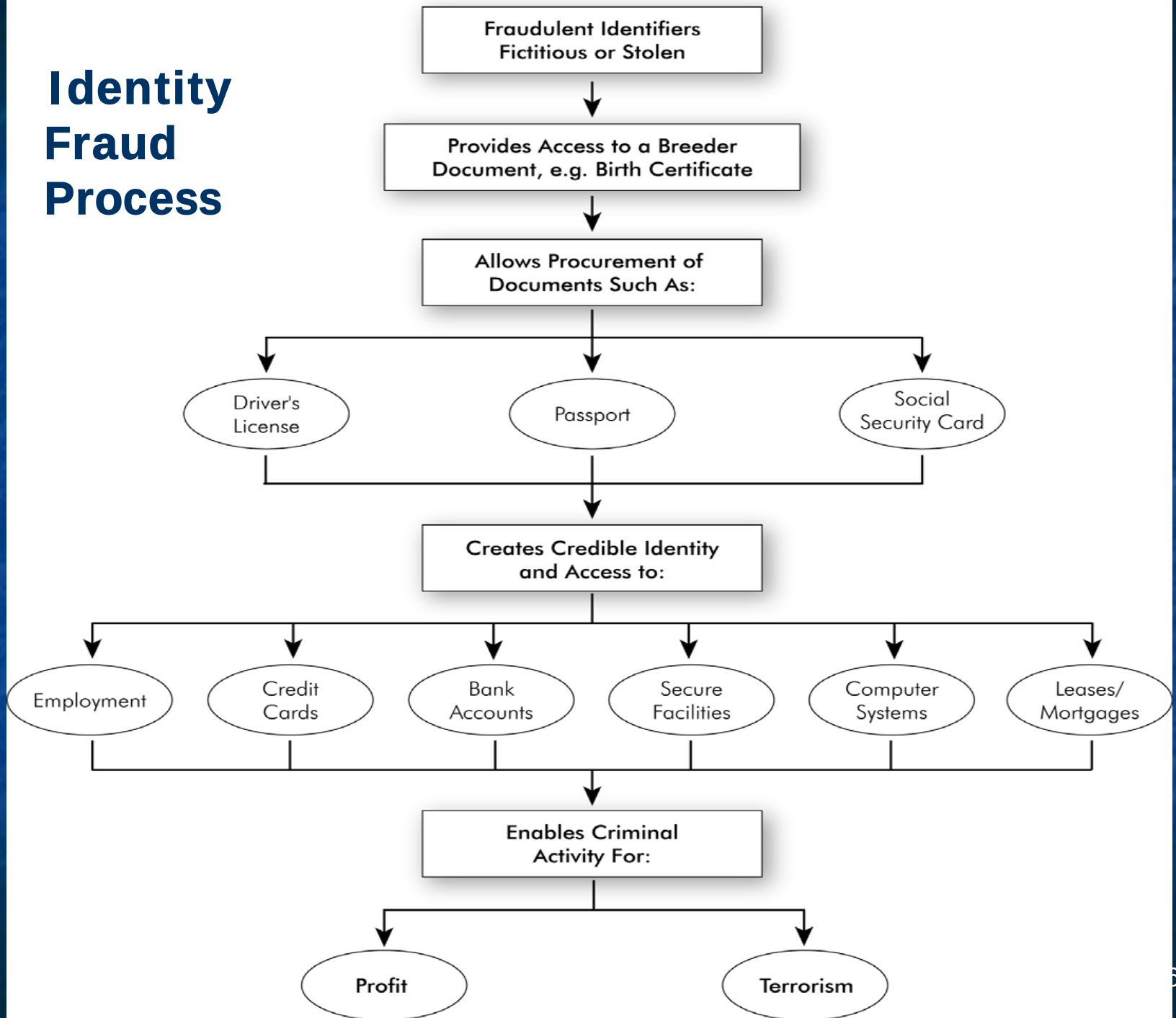
Defining Identity Fraud

Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime.

Facilitator of Criminal and Terrorist Activity

Identity fraud provides criminals and terrorists with the tools they need to remain anonymous, gain access, avoid detection, and transfer resources, all of which can be used to facilitate criminal and terrorist activities.

Identity Fraud Process



Information-Based Identity Authentication

- Strengthens the initial enrollment process
- Uses risk assessment methodologies to determine the likelihood that the person is who they claim to be
- Relies on multiple data sources
- Requires significant amounts of data to make predictions of the goods and bads

Information-Based Identity Authentication

- Focuses on determining the validity of personal identifiers
- Provides an independent assessment of what a person represents about his identity, based on analysis of available information

Sources of Information

- Vary depending on the application and level of risk
- Potential sources: Government, Commercial, Intelligence, and Private
- Need for Global data
- Challenges:
  - Information sharing
  - Information networks
  - Privacy

Information Based Identity Authentication

Applies three levels of risk Assessment

- Validation
- Verification
- Authentication

Validation

- Lowest level, examines identifiers in isolation to determine if the personal information presented by an individual is:
  - Not fictitious
  - Conforms to a proper format
- Limitations: well constructed false identities are not revealed in this stage.

Verification

- Determines if the identifiers presented by an individual belong together
- Analyst can search to determine if the same combination of identifiers match in multiple databases
- Level of risk determines extent of search and use of specific databases

Authentication

- Builds on validation and verification
- Uses modeling and scoring engines to determine the probability of a claimed identity of an individual being real
- Three outcomes: affirmative, negative or an exception
- Predicts the authenticity of the individual's claimed identity.

Key Questions for Information-Based Identity Authentication Systems

- How effective are the predictions?
- How reliable is the information?
- How is trust managed and measured?
- How can individual privacy be protected and enhanced?

Effectiveness and Efficiency

- Standards, metrics, methodologies need to be developed for the evaluation of effectiveness.
- Test to determine how effectiveness is influenced by using specific and multiple identifiers.

Reliability of Data

- Quality of data
- Quantity of data
- Source of data
  - Domestic
  - Global
- Other

Trust

- Oversight
- Audit compliance with policies builds trust.
- Metrics + Audits = Trust
- Technology builds trust.

Enhanced Privacy Protection

Data Sharing Policies and Standards

- Develop comprehensive policies, standards, laws, and regulations to define how and under what circumstances personal information and records can be shared and who can have access to it.

A Trusted System must:

- Protect the digital data.
- Gather data, rather than storing it, when it is required, from domestic and global databases.
- Maintain the privacy of the information.
- Distribute data on a need to know policy-based, technology driven basis.
- Log all activities so that they are auditable in near or real time with proper oversight.
- Adhere to legal and regulatory standards.
- Be technically sound.

Recommendations

- **Recommendation 1:** Gain a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem.
- **Recommendation 2:** Establish a central information database of identity fraud incidents.
- **Recommendation 3:** Establish a national identity fraud research agenda.
- **Recommendation 4:** Establish more sophisticated domestic and global information-sharing networks

Recommendations

- **Recommendation 5**: Conduct a study of existing domestic and global policies, laws, and regulations to determine best practices for combating identity fraud.
- **Recommendation 6**: Enhance the protection of individual privacy and information ownership.
- **Recommendation 7**: Improve information-sharing systems that enhance identity authentication solutions while protecting privacy.