# The Use of Data in the Judicial System – Identity Theft

# The Use of Data

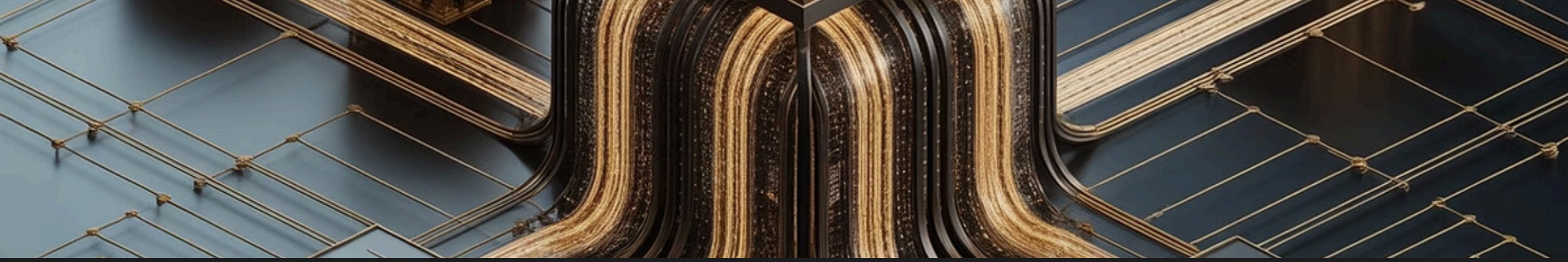
## Tackling Identity Theft

Understanding Laws, Data Practices, and Impacts

# Introduction

## What is Identity Theft?

The fraudulent use of another person's personal identifying information for financial gain or criminal intent.



# Role of Data in the Judicial System

### Case Profiling

using digital footprints

### Biometric Verification

for accurate identity tracking

### Database Matching

(e.g., SSN, credit records)

### Cross-jurisdictional Tracking

via shared federal and state databases


# Federal Laws That Punish Identity Theft

## Identity Theft and Assumption Deterrence Act (ITADA) – 1998

- Codified in 18 U.S. Code § 1028
- Criminalizes unauthorized use of identity data
- Penalty: Up to 15 years in prison, fines, property seizure


# Aggravated Identity Theft Law – 2004

## Mandatory Sentencing

Mandatory 2-year sentence for identity theft tied to other crimes

## Application Areas

Applies to immigration, wire fraud, and bank fraud cases

# Computer Fraud and Abuse Act (CFAA)

- **Target**

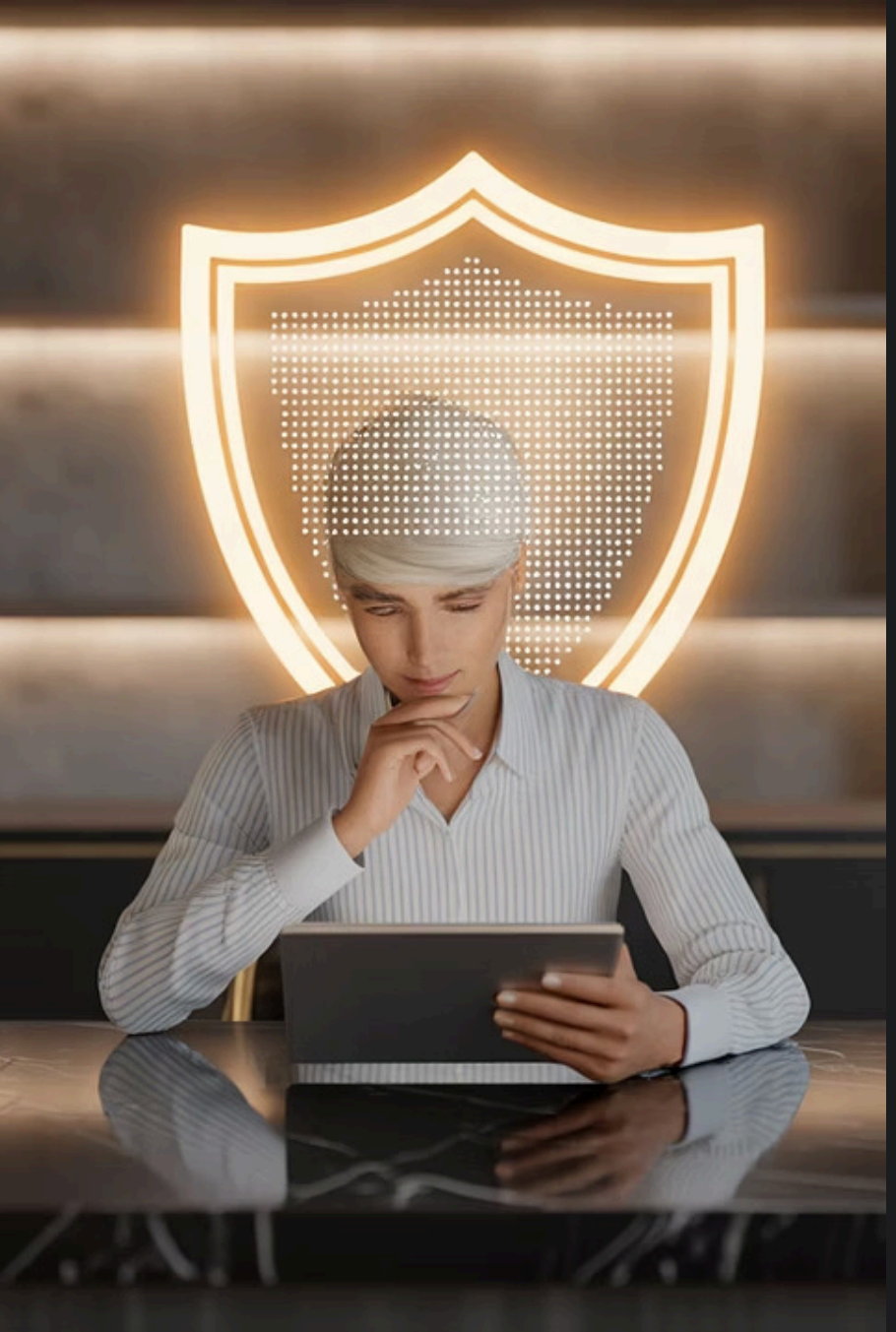
  Targets unauthorized computer/network access

- **Penalties**

  5–20 years depending on severity

- **Application**

  Often overlaps with cybercrime cases



# FCRA & FACTA Protections

## Consumer Rights

Consumer rights to correct credit records

## Data Security

Emphasis on data security and consumer protection

## Civil Remedies

Non-criminal but integral to civil remedies

# State-Level Identity Theft Laws

## Vary by jurisdiction

### Common traits:

- Felony classification for serious theft
- Restitution mandates
- Enhanced penalties for targeting vulnerable individuals
- Civil lawsuits enabled for victims


# Why Harsh Penalties?

1

## Financial Impact

Financial devastation for victims

2

## Personal Trauma

Emotional and legal trauma

3

## Criminal Networks

Links to terrorism and organized crime

4

## Prevention

Legal deterrence and prevention

# Conclusion: The Data-Justice Nexus

## Investigation & Tracking

Legal systems rely on structured data to investigate, track, and convict identity theft

## Accountability

Data enhances transparency, accountability, and protection of civil liberties

## Enforcement

Identity theft laws are data-driven in design and enforcement

# References

## Academic Sources


📜Romanosky, S., & Acquisti, A. (2009). *Privacy Costs and Personal Data Protection*. Berkeley Tech Law Journal, 24(3), 1061–1101.

📜 Matsueda, R. L., et al. (2006). *Deterring Delinquents: A Rational Choice Model*. Am. Socio. Review, 71(1), 95–122.

📜 Perl, M. W. (2003). *Why State ID Theft Laws Fail to Address Criminal Record Theft*. J. Crim. Law & Criminology, 94(1), 169–208.


## Legal References


📜 **1. 18 U.S. Code § 1028 – Fraud and related activity in connection with identification documents**

🔗 Read the Law on Cornell Law School's Legal Information Institute
**https://www.law.cornell.edu/uscode/text/18/1028**

📜 **2. Identity Theft Penalty Enhancement Act – 2004**

🔗 Congressional Research Summary via GovInfo

**https://www.congress.gov/bill/108th-congress/house-bill/1731**

🔗 Text of the Law (Public Law 108–275)
**https://www.congress.gov/108/plaws/publ275/PLAW-108publ275.pdf**

📜 **3. Computer Fraud and Abuse Act (CFAA)**

🔗 U.S. Code: 18 U.S. Code § 1030 – Fraud and related activity in connection with computers

**https://www.law.cornell.edu/uscode/text/18/1030**

📜 **4. Fair Credit Reporting Act (FCRA) & Fair and Accurate Credit Transactions Act (FACTA)**

🔗 FCRA Full Text (**FTC.gov**)

**https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act**

📜 **5. Data Breach and Violation Laws**

🔗 U.S. State Data Breach Notification Laws – National Conference of State Legislatures (NCSL)

**https://www.ncsl.org/technology-and-communication/security-breach-notification-laws**

🔗 FTC on Data Breach Response & Legal Responsibilities

https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business