What every infosec professional should know about identity theft

Branko S. Bokan, CISSP
Infosec4all.com

Background

- Based on a academic research
- The aim was to show flaws in statistics
- Discovered that there is no national statistics
- Virtually no longitudinal data exist
- No single/commonly accepted definition
- Impossible to estimate magnitude/real cost

What is identity theft

When?

Where does it happen

Who benefits from it?

How much does it cost?

Who commits it?

Can it happen to me?

How often?

Who are the victims?

Is there help?

How serious it is?

Can it happen to anyone?

What is the real magnitude?

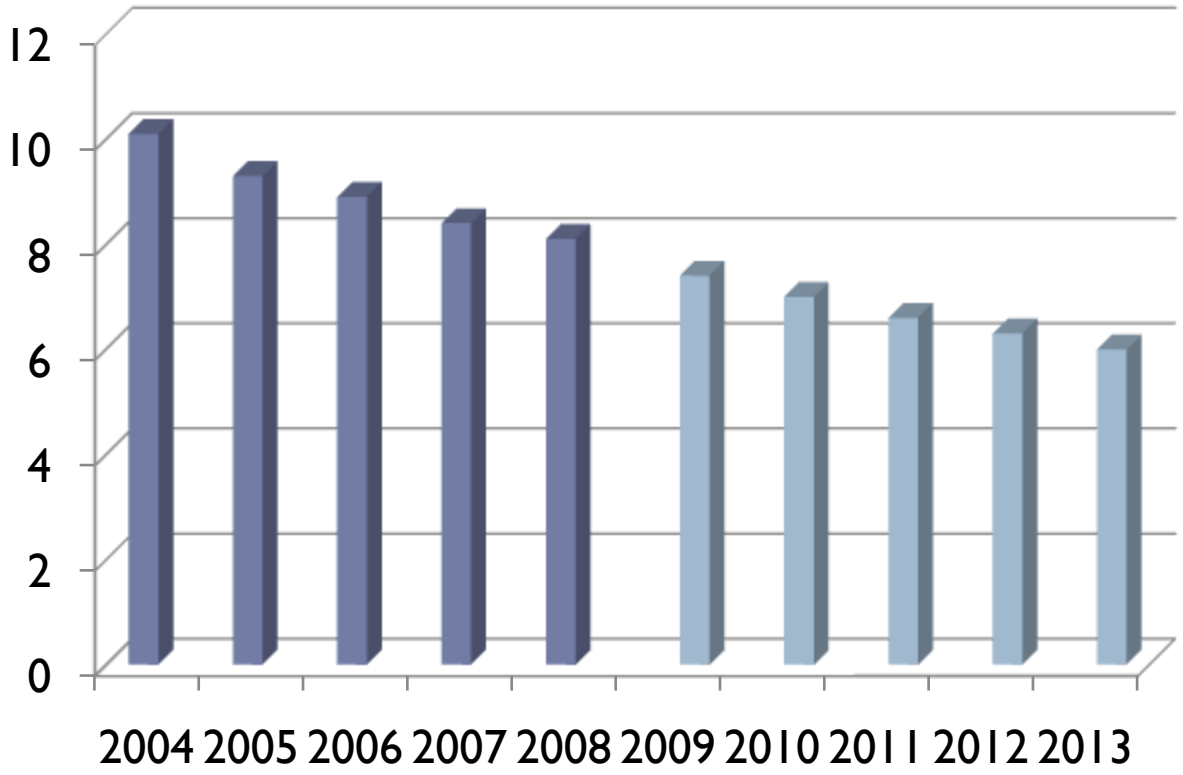
What is government doing to help?

Why most of it takes place in the United States?

Introduction

- Not a modern crime
- Declining trend
- Expansion does not correlate to development of Internet
- No common definition
- Frequently misunderstood
- Often confused with credit card fraud
- Enablers

Declining trend



History

- Existed for centuries
- For long times was only means for committing other crimes and perpetrators prosecuted for ultimate crimes.

History

- People living in organized groups, invented postal services they started using names and numbers to identify themselves. Most of private information was publicly available. Decisions based on reputation in the local community.

- The rise of information-based credentials gave identity theft a modern spin.

- Identity theft with an aim of not only evading the justice but gaining a direct financial benefit emerged in 1980s become epidemic in 1990s.

History

- Postal Inspection Service began tracking mail theft cases that involved fraudulent credit card applications and change of addresses in 1995
- Secret Service began tracking cases that involved identity takeover in 1997
- Arizona that first recognized the crime in 1996.
- US Government introduced the Identity Theft and Assumption Deterrence Act in 1998
- Identity Theft Data Clearinghouse by the Federal Trade Commission established in 1999.
- 2001 society realized the extent to which this crime is involved in commitment of other crimes and even terrorism.

Statistics

- There is no national system in place for collecting statistical data on identity fraud and no federal government entity collects such data.
- Only two major sources of statistics: clearinghouse reports on identity theft complaints produced by the Federal Trade Commission and several surveys and research studies commissioned by the same agency.
- Since the adoption of Identity Theft Assumption and Deterrence Act in 1998, only four major studies released.
- FTC's Identity Theft Data Clearinghouse only source of statistics on identity theft complaints submitted through Sentinel database. Its primarily purpose was not to provide statistical information on identity theft but to help law enforcement fight the crime and help victims share their complaints.
- There is no national database maintained by any criminal justice agency on the number of actual identity theft cases

Common misconceptions

- Internet only impacted the visibility.
- There is no correlation between development of modern technologies (including the Internet) and growth of identity theft.
- Technologies do not increase the risk of identity fraud, but rather present the best way to detect fraud.
- Numbers that show increase actually increase in awareness.

What is identity theft

- Theft - appropriation of property belonging to other with intention of permanently depriving the other
- Identity is information, combination of things we are, we know, and we have - one cannot be deprived of it once it is 'assigned' to her at birth.
- Experts suggest use of more appropriate term – identity fraud

- Javelin:
  Identity theft - someone gains access to personal data without permission.

  Identity fraud –criminal takes personal information and misuses it for financial gain.

- More appropriate definition: information theft as use of false identifiers, fraudulent documents, or a stolen identity in the commission of the crime - identity fraud includes both the identity theft and cases of creating fictitious identity.

Types of fraud

- Financial
- Non-financial
- Criminal record identity theft

Misuse of existing credit card (number)

- Stolen plastic used to make a purchase. Most frequently CNP (card not present transactions). Easily detected by victims by simply monitoring financial statements.
- Banks successfully employ specialized software that looks for anomalies and prevent transactions before they take place.
- The most important characteristic of this type of fraud is that once discovered it is easily to prevent it from taking place again simply by blocking the existing card and issuing a new one.

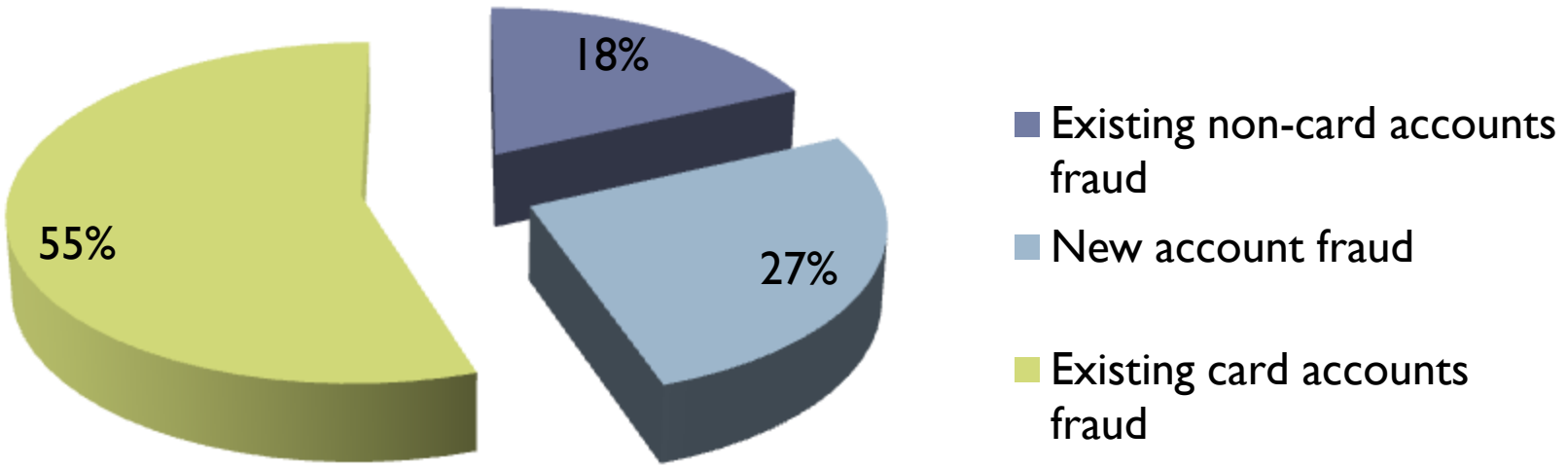
Misuse of existing non card or account

- Criminals get access to existing accounts and either make money transfers to their own account or change the ownership of the account to their name.
- Characteristics: low dollar loss and out of pocket cost, short detection time, most frequently detected by companies, victims first find out of the crime through company notification and statements monitoring.
- Victim released from any liability and reimbursed for possible financial damage.

New accounts and other fraud

- Low occurrence. Pure identity theft. Most serious. High dollar amount and out of pocket cost, longer detection time, lower discovery by financial institutions and victims' discovery when contacted by debt collector or law enforcement.
- Criminals use identifiers such as name, social security number, address, date of birth, and other identifying information to establish a new identity.
- It is possible for this type of crime to stay completely undetected since the criminals might try to keep a clean record on their 'new identity'.
- New accounts are opened using criminal's address and paid regularly in order to avoid any unnecessary attention.
- Criminals use this type of fraud to obtain jobs that would otherwise not be available due to their criminal history, escape criminal prosecution, and engage in illegal immigration.

Incidence of fraud



Credit card fraud

- Credit and debit card related frauds make up to 50% of identity theft crime

Three types of credit card fraud:

- Lost or stolen card (most common, criminal does not assume victim's identity in any way, short life).
- Counterfeit cards (typically occurs through 'card-not-present' transactions).
- Application fraud (more serious fraud, more time to detect and recover),
-
- Characteristic of credit card fraud or at least lost or stolen type is that there is no cost borne by the consumers ($50 limit usually waived)

Credit card fraud vs. identity theft

- The credit card industry does not lose money from credit card fraud - merchants foot the bill in the end, topped with fines
- Dos not publish information on the cost of lost or stolen cards and card not present fraud but consider the loss as a cost of operating the business.
- Only when criminals use stolen identity to open credit card accounts in someone else's name identity theft occurs since it requires use of victim's personal identifying information..
- In most reports' credit card fraud makes more than 50% of identity theft cases.

Characteristics of credit card fraud

- Does not cost the victim any money
- Execution and recovery time is insignificant compared real identity theft
- Easily detectable while real identity theft sometimes remains undetected
- Does not leave any record in the victim's criminal or financial history
- Once reported the card is blocked and it is not possible to continue exploiting the same card
- Process significantly differs from the real identity theft
- Remediation significantly differs from the one of real identity theft
- Credit card fraud distorts statistics on identity theft

Federal legislation

- Situation in the United States more complicated due to overlapping jurisdictions
- The federal penalty code was amended in 1998 to introduce the Identity Theft Assumption and Deterrence Act (U.S. Public Law, 1998). This act was again amended in 2004, and the amendments are still in force.
- Separate law (Title 18, Chapter 1029 Fraud and Related Activity in Connection with Access Devices) addresses credit card fraud

[One is guilty of identity theft if...] knowingly and without lawful authority ***produces an identification document****, authentication feature, or a false identification document (hereafter identification document); [...]* ***transfers an identification document****,[...] knowing that such document [...] was stolen or produced without lawful authority;[...]* ***possesses with intent to use unlawfully*** *or transfer unlawfully five or more identification documents[...]* ***possesses an identification document****, [...] with the intent such document [...] be used to defraud the United States;[...]* ***produces, transfers, or possesses a document-making implement*** *[...] with the intent such document-making [...] will be used in the production of a false identification document or another document-making implement [...] which will be so used; [...]* ***possesses an identification .. that is or appears to be an identification document*** *[...] of the United States which is stolen or produced without lawful authority knowing that such document [...] was stolen or produced without such authority;[...] transfers, possesses, or uses, without lawful authority, a* ***means of identification of another person*** *with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or [...]* ***traffics in false authentication features*** *for use in false identification documents, document-making implements, or means of identification[...]*

Identification

- Definition of identity vague.

State legislation

- States laws define identity theft in very similar way, except for two differences – the penalty for the crime, and treatment of credit card fraud.

- Most state laws use the term identity theft to describe the crime, others call it criminal impersonation, taking identity of another person, false personation, identity deception, misuse of identification, unauthorized or fraudulent use of personal identifying information, and identity crime.

- Only the state of Nebraska clearly differentiates between identity theft and credit card fraud

Related legislation

- U.S. Public Law, Title 42, Chapter 408 – Fraud in Connection with the Misuse of Social Security Numbers

- **The Fair Credit Reporting Act (FCRA)**
  Originally passed in 1970 and last amended in 2003. One of the most significant provisions of this law related to identity theft prevents states from passing more stringent financial privacy rules than federal government.

- **The Fair and Accurate Credit Transactions Act**
  Passed in 2003 with sections specifically designed to combat identity theft, it protects consumers' credits and calls for enhancements in identity authentication.

- **Gramm-Leach-Bliley Act (GLBA)**
  Enacted in 1999 it instructs financial institutions to have policies, procedures, and controls to prevent unauthorized disclosure of financial information, and allows consumers to opt-out from having financial institutions disclose their private financial information.

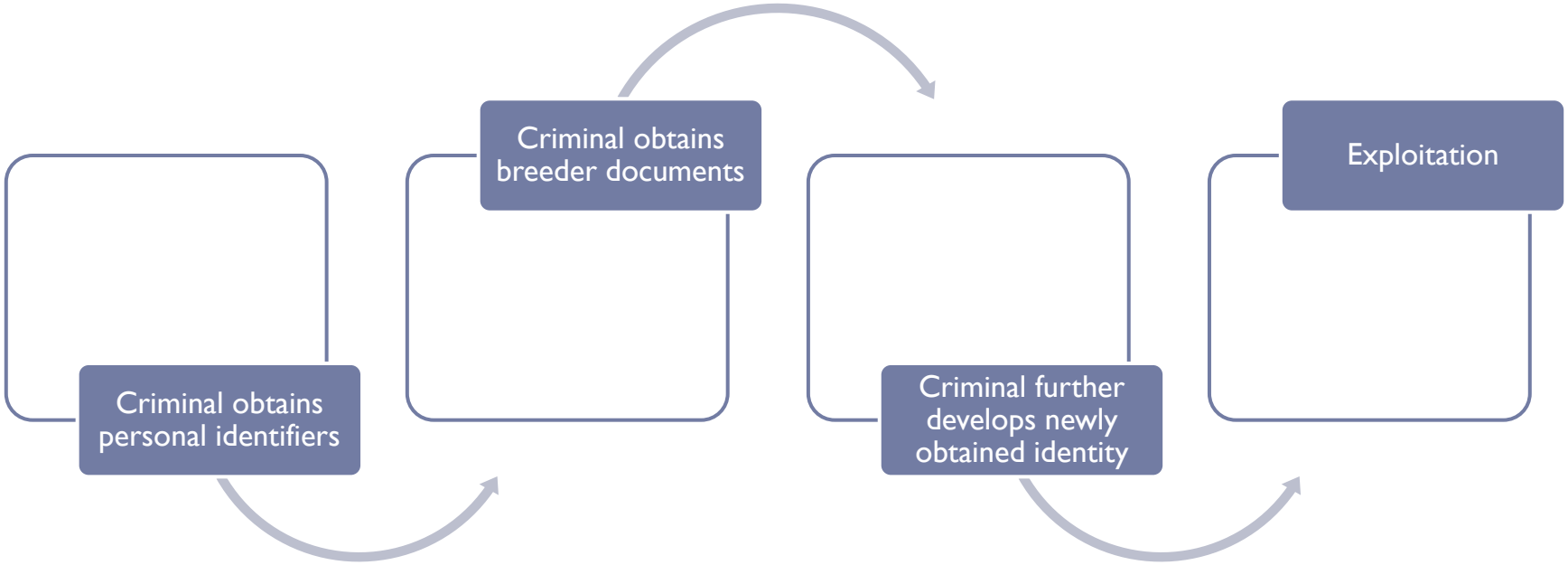
The process

- **Why does someone steal an identity?**
  Hot items are **CRAVED**:
  (Concealable, Removable, Available, Valuable, and Enjoyable - IDT not removable but multipliable)

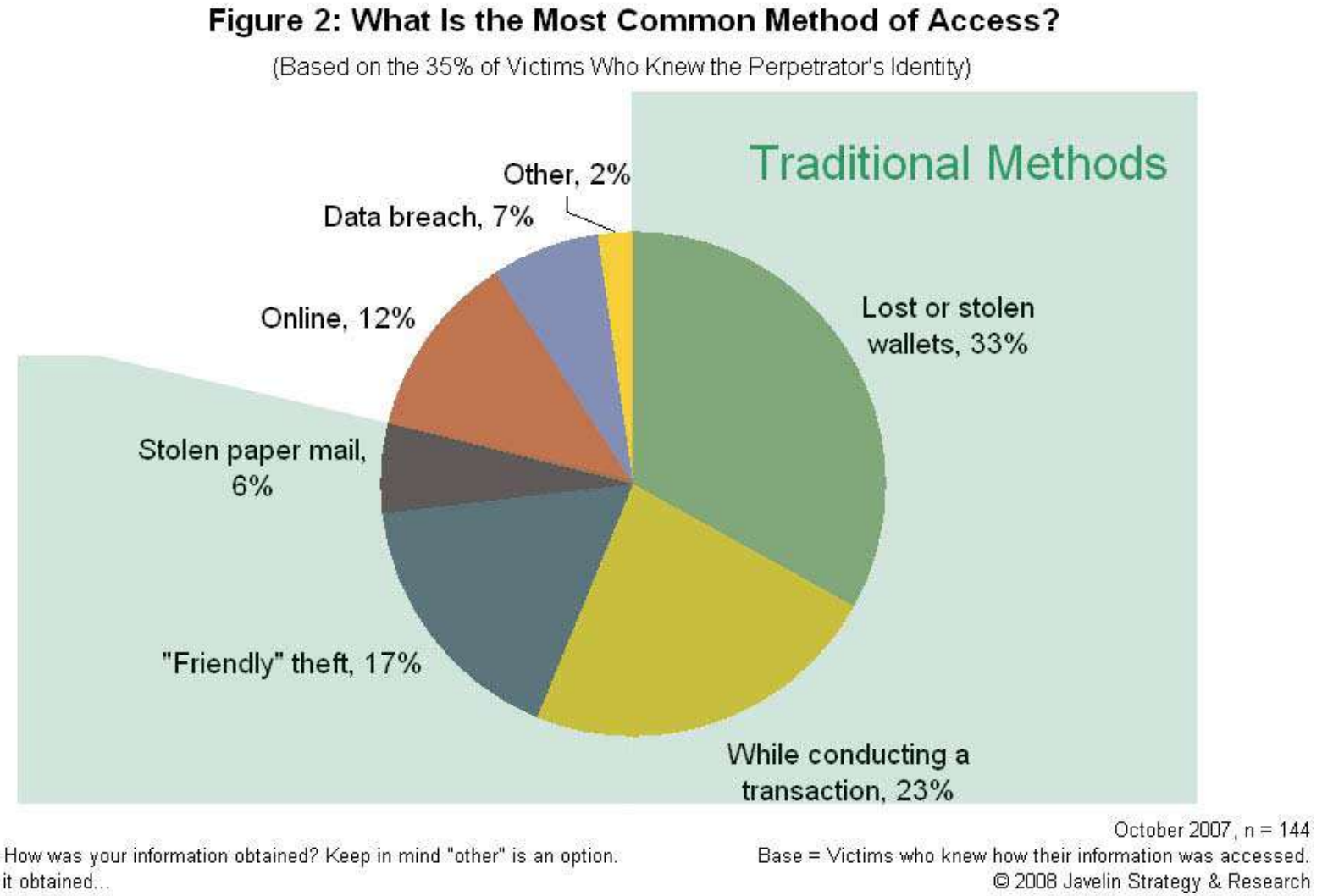
- Benefits: stolen identity can be enjoyed through direct financial benefits, non financial benefits, and misuse of legal records.

- Identity theft is not a tool of a con artist anymore; it is indigenous to any criminal enterprise.

How does it take place?



Sources of identifiers



The other side of exploitation

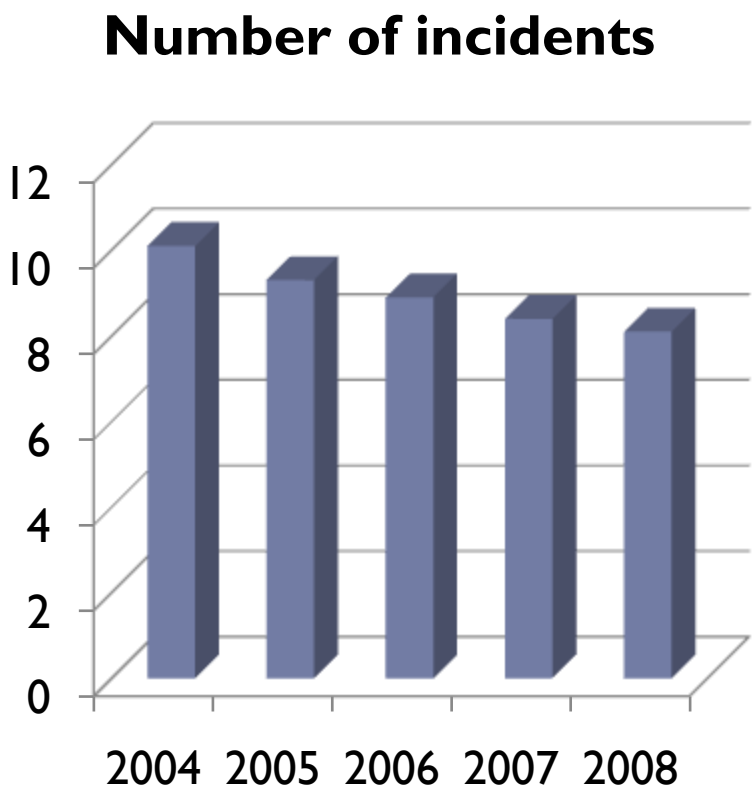
- Financial institutions benefit from various legal requirements by transferring the costs to consumers through disproportional increase in service fees.

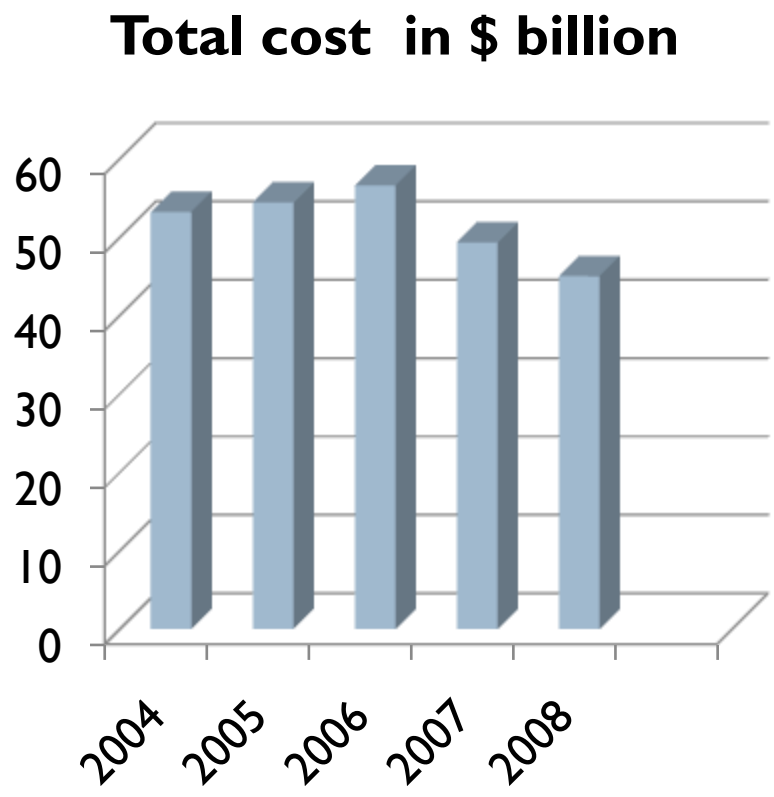
- Fast growing industry that legally profits from selling various services ranging from financial insurance, privacy protection, to credit monitoring.

Cost and recovery

- Impossible to determine the extent of the crime and real cost without a proper definition
- Available data just a tip of an ice berg
- According to the United States Treasury Department's own research, cyber criminals made more money than illegal drug traders in 2005

Cost and recovery

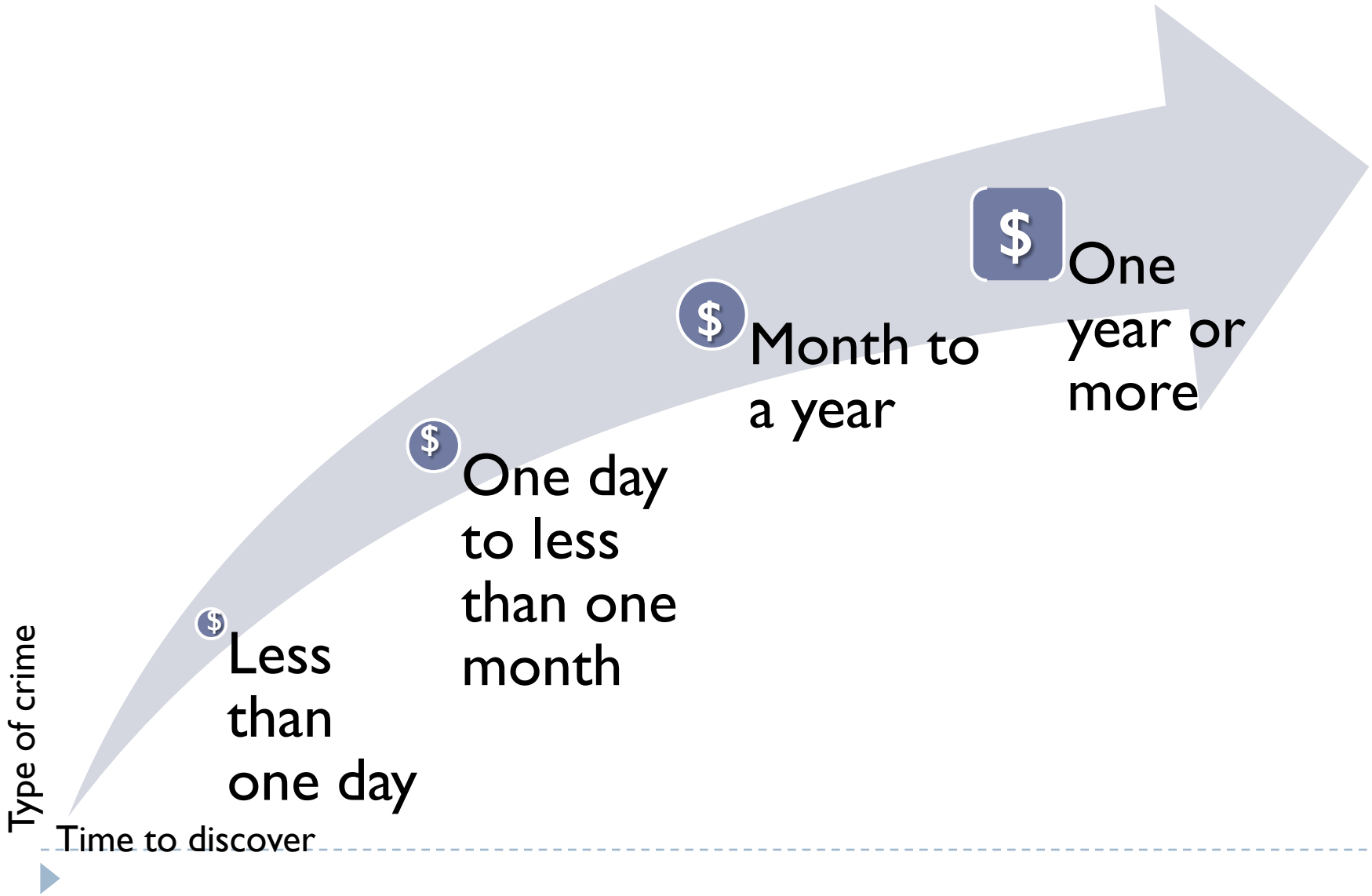




Individuals

- Credit card - consumers responsible for $50 or none. Minimal time and effort to resolve.
- Real identity theft - cost both tangible (money and time) and intangible (reputation, credit worthiness, possible false criminal record, and efforts on clearing name and financial and criminal history.)
- In spite of decline in number cost increases. Currently around $1000 per individual, totaling $5 bn.
- Recovery takes many months, years.
- Other costs include: harassment from debt collectors, banking problems, loan rejections, utility cutoffs and even arrest for criminal offenses

Cost and recovery



Business

- Cost for businesses: hard (easy to calculate considered 'cost of doing business') and soft (indirect costs).
- FTC estimates $33 billion a year.
- In case of credit card fraud cost passed to merchants. Identity theft losses – cost of doing business.
- Other costs: reduction of confidence in financial infrastructure, reduction of corporate productivity and leads to higher costs for consumers, and compromises economic infrastructure.
- Fear of identity theft is the fastest growing barrier to online services like electronic billing

Government

- White-collar crimes cost $11,400 per case (up to $25,000)
- White collar inmates cost government $17,400 per annum, while an average probation cost is $2,900.
- National security threats, public safety threats, burdens created by illegal immigration, costs associated with introduction of national ID system, increased public paranoia, and overall decrease in confidence in benefits of the information age.

Why in the US more than anywhere else

- There is no single factor that makes identity theft possible.
- Factors change through time and differ from country to country.
- Set of specific factors and environments that create fertile ground for committing identity theft called **identity theft enablers.**

Enablers

- **CREDIT REPORTING AGENCIES**
  Equifax, TransUnion, and Experian. The most complete set of information on consumers in the. Multi multibillion dollar industry. The system is geared toward facilitating the growth of the credit industry and its own protection, and not protection of individual customers

- **SOCIAL SECURITY NUMBERS**
  One of the main tools used to steal identity, due to its use for purposes not intended by the original design

- **INSTANT CREDITS**
  Merchants, based on credit scores provided by credit reporting agencies, approve instant credits to customers who can prove their credit worthiness, not their identity.

Enablers

- **CONVENIENCE CHECKS**
  Unlike cards, in most cases the use of convenience checks does not require any authorization, and the checks are not covered by a $50 liability limit.

- **FUNCTIONAL LITERACY**
  OECD: "ability to understand and employ printed information in daily life."
  National Institute for Literacy: "50% of the adult population in the US considered illiterate, with 44 million that cannot read a newspaper or fill out a job application (compared to 24% in the UK)"

- **TECHNOLOGIES**
  Old technologies do not provide tamper proof documents while new technologies allow production of high quality, 'better then the originals' documents

Enablers

- **PRIVACY LAWS**
  U.S. privacy laws only adequately protect privacy within individual's home. Contrary to practices in other European countries, US laws do not ban collection of personal information without consumer's permission

- **INTERNET**
  Only 10 percent of data compromises take place over the Internet.

- **IDENTIFICATION DOCUMENTS**
  An average American carries more IDs than a citizen of any other nation, yet those documents have few security features and are not standardized. Issued by 8,000 uncoordinated jurisdictions.

Enablers

- **INFORMATION AVAILABILITY**
  Personal identifying information on any citizen of this country is more widely available than ever before thanks to relatively new industry of data mining

- **ECONOMY OF SCALE**
  In the US in 2000, there were 1.5 billion credit cards held by 158 million cardholders – an average of ten credit cards per cardholder, with over three billion solicitation letters sent in a year

- **NON-CASH PAYMENT INSTRUMENTS**
  The number of non cash transactions in the US represents more than 60% of all cash transactions in the 14 most developed countries with only 36% of population. Checks account for more than 60% of consumer non cash transactions with over 15 checks written per month per person (three to five times more than in UK and Canada, and at least 15 times more than in other European countries).

- **OUTSOURCING**
  In-house data breaches pose the biggest threat to information security

Conclusion

- Understanding identity theft and how it differs from other frauds important for proper prevention, detection, and recovery.

How to mitigate risk

- Monitor your accounts online
- Move your financial transactions online
- Review your financial information no less than once per year
- Never provide personal information unless you initiate the contact
- Install and regularly update firewall, anti-spyware, anti-virus, and browser software
- Reduce unnecessary access to your personal information wherever possible

Third party protection services

Monitoring	• A paid for subscription service that monitors for suspicious activity or changes to your credit file (e.g., credit inquiries, employment changes, new accounts and address changes) • Detects potential fraud
Fraud alert	• • A message that is placed on your credit report, requiring lenders and merchants to confirm your identity before issuing a new line of credit • Intended to prevent fraud
Credit freeze	• Locks down your credit file at the credit reporting agencies, which are prohibited from issuing your credit history to any lender, creditor, etc. • Prevents fraudulent new accounts from being opened in your name
Public records mining	• Scans public records and Internet sites to detect if your personal information is out there (credit card numbers, Social Security numbers, etc.) • Detects potential identity theft (your information has been found, but may not have been misused for financial gain)

What to do if IDT occurs:

- Contact your bank, credit card company or merchant *immediately*
- Close any accounts that may have been compromised.
- Ask your financial provider about their fraud resolution teams
- Place a credit alert at all three of the credit bureaus (Equifax, Experian and TransUnion)
- Be informed of your data breach notification rights
- Consider placing a credit freeze
- File a report with your local police
- Notify the Federal Trade Commission
- Sign up for a credit monitoring service