



Identity Theft: Take Control of the Inevitable Reality

IT ADVISORY

AUDIT ■ TAX ■ ADVISORY

Discussion Topics

- **Why ID Theft is a significant problem?**
- **What is an Identity?**
- **Identity Lifecycle**
- **Why ID theft occurs?**
- **Common means of ID Theft**
- **FTC's settlement with a retailer**
- **Measures to prevent ID Theft and Fraud**
- **State requirements**
- **Industry initiatives**
- **Consumer Rights**
- **Case Study**
- **Key Takeaways**
- **Appendix A – Credit reporting bureaus accessing credit reports**
- **Appendix B – Additional Resources**



Why ID Theft is a significant problem?

- 8th consecutive year ID theft is the #1 complaint, 32% of the complaints in 2007 were related to ID theft -ftc.gov
- 8.4 million ID fraud victims in United States in 2007 with losses of \$45 billion - Javelin Strategy & Research
- Bank account numbers typically sell on the U.S. black market for approx. \$400, compared with \$5 or less for credit card numbers – Gartner, Inc.

Why ID Theft is a significant problem? (contd.)

ID Theft and Fraud Incidents	Implications
<ul style="list-style-type: none"> Hannaford Brothers and Sweetbay - estimated 4.2 million credit and debit card numbers were stolen. <p>Source: infoworld.com</p>	<ul style="list-style-type: none"> About 1,800 cases of fraud reported so far Two class action lawsuits filed against Hannaford
<ul style="list-style-type: none"> TJX - more than 45 million credit and debit card numbers stolen from its systems <p>Source: informationweek.com</p> <p>Tens of millions of dollars in fraudulent charges have been made on the cards and millions of cards have been cancelled and reissued by the Banks.</p>	<ul style="list-style-type: none"> TJX estimates total costs at \$256 million. Offered free credit-monitoring services for three years (approx \$200/year/person) Cash reimbursements, Shopping vouchers and a promised three-day customer appreciation event, during which the company plans to offer 15% discounts on all goods.
<ul style="list-style-type: none"> Hard drive containing personal information about veterans including Social Security numbers went missing from a Birmingham, Ala., Veteran Affairs medical research facility. <p>Source: govexec.com, privacyrights.org & identity theft resource center</p>	<ul style="list-style-type: none"> Estimated 535,000 SSN numbers are at risk. More than \$20 million allocated for VA to respond to data breach notification, legal costs, and compensating the victims.

What is an Identity?

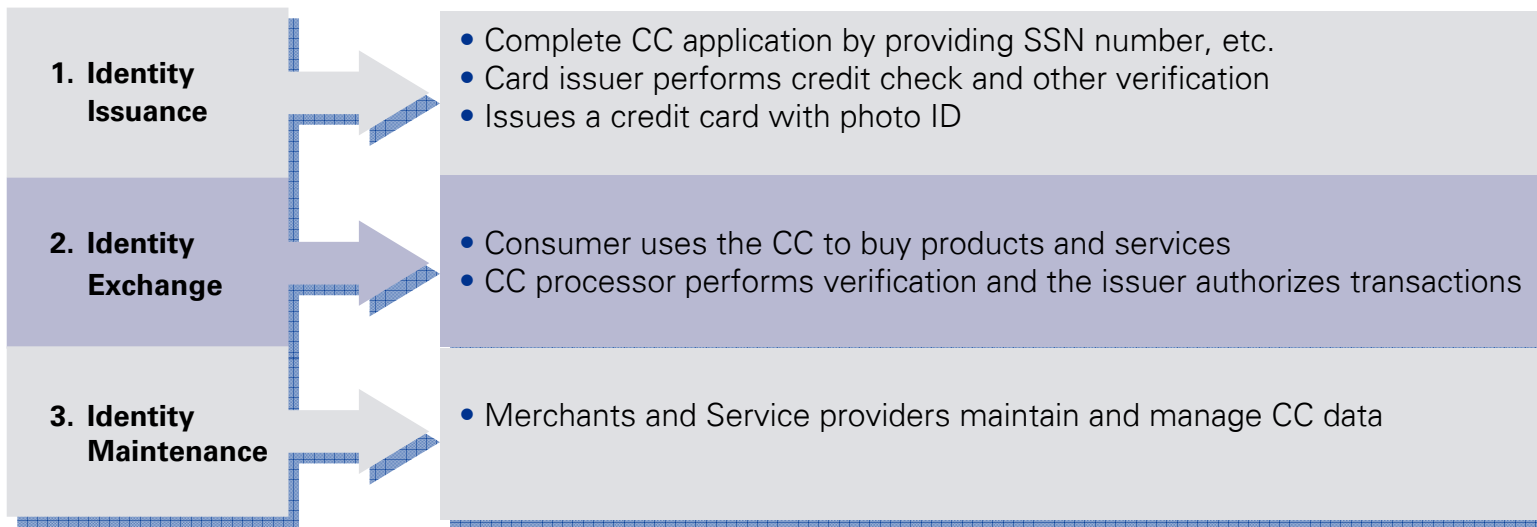
Common forms of Identity used:

- SSN,
- Drivers License,
- Passport,
- Birth Certificate,
- Club Membership
- Credit Cards with photo
- Government issued ID Cards,
- User ID/Password

Identity Lifecycle

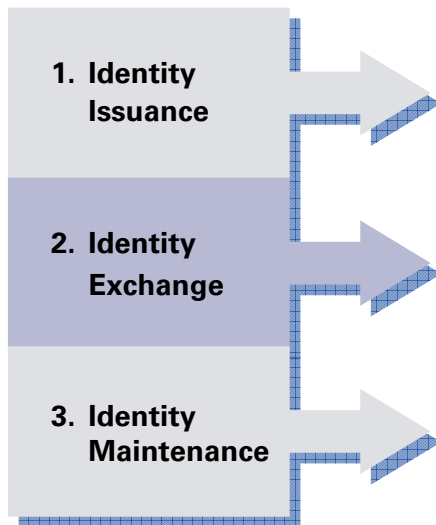
Identity Lifecycle

Example – Consumer applying for a credit card (CC)



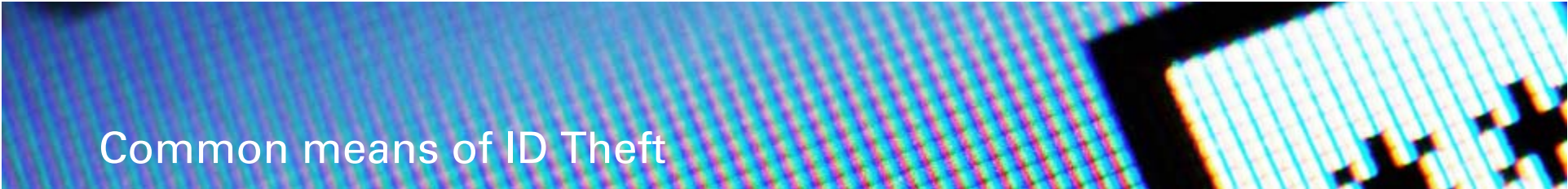
Why ID Theft Occurs?

Identity Lifecycle



Common Reasons for ID Theft

- Inappropriate distribution and protection of:
 - Identification documents
 - Credential issuance security (User ID / Passwords, Security Tokens, Verifiable Information)
- Inadequate validation of credentials
- Poor data and transaction handling
- Inadequate controls over consumer credit information
- Information system breach
- Misuse of user data
- Excessive data collection and storage



Common means of ID Theft

Traditional – Physical methods

- Computer backup theft
- Dumpster diving
- Shoulder surfing
- Direct access to information
- Theft of wallet or purse
- Mail theft and rerouting
- Disgruntled personnel
- Disguised ATMs (Skimming)
- Social engineering (fake telephone calls)

Electronic – Internet related methods

- Hacking
- Phishing
- Pharming and Redirectors
- Keyloggers and password stealers
- Spyware and Trojans

FTC Announces settlement against TJX

According to FTC, the settlements will require that TJX **implement comprehensive information security programs** and obtain audits by independent third-party security professionals every other year for 20 years.

#	FTC charged that TJX:	Security Focus Areas
1	Created an unnecessary risk to personal information by storing it on, and transmitting it between and within, its various computer networks in clear text ;	Data Classification, Information Protection (e.g. Encryption)
2	Did not use readily available security measures to limit wireless access to its networks , thereby allowing an intruder to connect wirelessly to its networks without authorization ;	Access Management (Wireless Security), Secure Architecture
3	Did not require network administrators and others to use strong passwords or to use different passwords to access different programs, computers, and networks;	Password Management
4	Failed to use readily available security measures, such as firewalls, to limit access among its computers and the Internet	Access Management (Firewall protection), Secure Architecture
5	Failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations , such as patching or updating anti-virus software .	Security Monitoring, Update Anti-Virus and System patches, Perform Self-Assessments

Measures to Prevent ID Theft and Fraud

Commercial

- Information Security Management Framework, e.g. ISO 27001 PDCA (Plan, Do, Check, Act) model
- Information Protection across the Information Lifecycle
 - Inventory
 - Classification
 - Protection (Access / Authentication / Encryption)
- User Awareness
- Privacy
- Incident Response management and notification
- Fraud monitoring

Data Lifecycle Protection





Measures to Prevent ID Theft and Fraud (contd.)

Personal

- Shred personal information
- Carry credit cards that you use
- Review credit report annually
- Purchase from secure and genuine websites
- Update anti-virus and spam software
- Don't carry your SSN card
- Lock your mailbox

State Requirements

Currently, 39 of the 50 US states have laws pertaining to the disclosure requirements in the event of a security breach.

Generally the laws provide:

1. **Notification guidelines:** how soon a company is required to inform customers of a data breach. In California, this is "as soon as possible, without unreasonable delay."
2. **Penalty for failure to disclose:** whether or not there are civil or criminal penalties for a failure to disclose. In California, a company cannot be penalized for its lack of promptness alone.
3. **Private right of action:** whether this option exists for consumers in that state. In California, this is available.
4. **Exemptions:** what kinds of breaches, if any, companies are exempt from reporting. California allows exemptions for encrypted data that's lost and publicly available government data. In California there is no such thing as an immaterial breach, while other states do have a definition of immaterial breach.

Industry Initiatives

Identity Theft Prevention and Identity Management Standards Panel (IDSP)

- Lead by the American National Standards Institute (ANSI) and the Better Business Bureau (BBB)
- IDSP Phase 1 – evaluating existing standards, guidelines, best practices related to this issue, and identifying gaps and make recommendations to augment the current guidelines and standards.
- IDSP Phase 2 - facilitate implementation of the recommendations

ISO – Variety of activities that focuses on Data protection, privacy, etc.

- Significant effort centers around ISO 27001 – Information Security Management System (ISMS)

Extended Validation (EV)SSL

- Organizations can obtain EV SSL certificates for their websites and demonstrate greater assurance to their customers of visiting a legitimate website, e.g. green address bar in IE 7 and other browsers

Consumer Rights

Rights

- **The Fair Credit Reporting Act (FCRA):** Limited access to the credit report, file a dispute if you recognize a false item
- **The Fair and Accurate Credit Transactions Act (FACT Act):** Additional protection against ID Theft, grants consumers the right to access their reports at no charge once every 12 months.
 - Identity theft victims who file police reports may block fraudulent information from appearing on their credit reports
 - Consumers may receive additional free reports if identity theft is suspected
- **The Fair Credit Billing Act:** Provides consumers with a legal dispute process, limits responsibility for unauthorized charges to \$50
- **The Electronic Fund Transfer Act:** provides consumer protections for ATM, debit card, and other electronic account transactions, including fund transfers.
- **The Fair Debt Collection Practices Act:** if the debt is determined to be accurate, collection activity will resume.

Case Study – Payment Solution Provider (PSP)

PSP accounted for a large number of total phishing mails sent

- Result – Bad user experience and financial loss to customers

Strategies adopted to minimize phishing attacks:

- Customer education
- Outbound email signing
- Visual identification
- Warn about unsafe browsers
- Extended Validation (EV) SSL
- Anti-fraud warning pages – white lists and blacklists
- Site shutdown
- Two-factor Authentication
- Fraud models
- Law enforcement and regulators/policy makers

Outcome of the strategy

- PSP reduced the amount of phishing mails sent by approx. 85%

Key Takeaways

Commercial

- Establish appropriate governance structure
- Leverage a comprehensive security framework
- Inventory and classify sensitive data
- Appropriately protect sensitive data through access controls and encryption
- Provide user awareness training (employees and customers)
- Enforce security policy and procedures
- Regularly monitor your security policies and controls
- Establish an Incident Response program

Personal

- Shred personal data
- Periodically review credit report
- Purchase from secure and genuine websites
- Update anti-virus and spam software

Contacts

Shahed Latif

Partner

KPMG Information Protection Services

slatif@kpmg.com

(650) 404-4217

Vijay Jajoo

Director

KPMG Information Protection Services

vjajoo@kpmg.com

(415) 963-8698



Appendix A – Credit reporting bureaus accessing credit reports

- **Equifax**
www.equifax.com
- **Experian**
www.experian.com
- **TransUnion**
www.transunion.com
- **Annual Credit Report Request Service**
www.annualcreditreport.com

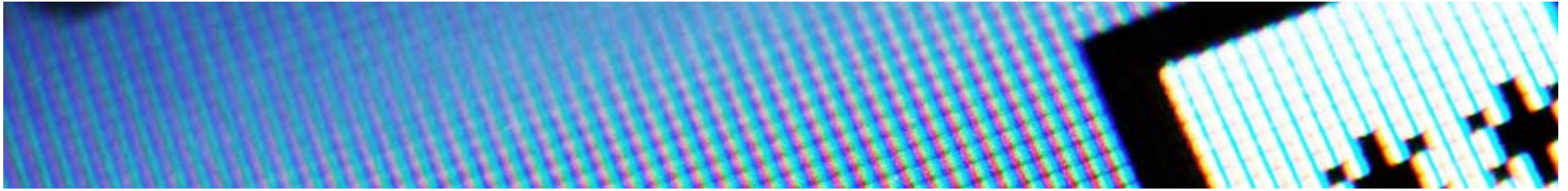
Appendix B - Additional Resources

Government Agencies

- **U.S. Federal Trade Commission**
Consumer Response Center: (877) 382-4357, or online at www.ftc.gov
ID Theft hotline: (877) 438-4338, or online at www.consumer.gov/idtheft
FTC Identity Theft Affidavit Instructions and Form: www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf
- **U.S. Postal Service**
www.usps.gov/websites/depart/inspect
- **U.S. Social Security Administration**
www.ssa.gov

Checking Account Fraud

- **ChexSystems**
If you are unable to open a checking account because of identity theft, contact: (800) 428-9623
- **TeleCheck**
(800) 710-9898



All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.