IC ANALYST PRIVATE SECTOR PROGRAM

2013
ANALYST PRIVATE SECTOR PROGRAM

The Current and Future Landscape of Identity Theft:

Findings of the "Identity Theft and Nexus to Illicit Activity" Team

Executive Summary. Identity theft (IDT) is a term describing multiple criminal activities that are underestimated, complex, and continuously changing. Surveys of individual victims have estimated IDT as affecting 11.5 million individuals, or 7% of the U.S. population, with total annual loss estimated at $21 billion in the United States.[1] However, this figure is likely a gross underestimation as it captures only one aspect of IDT: individuals suffering financial loss. Indeed, the definition of IDT is often considered to be overly restrictive: it focuses solely on individual victims, typically requires financial loss, and neglects varieties of IDT emerging in the online environment. We propose an expanded definition of IDT that broadly reflects the current landscape: the unauthorized use of an individual's or entity's set of unique characteristics that define the individual or entity in order to conduct illicit activity. The impact and consequences of IDT are expected to be significantly higher with this expanded definition.

IDT crimes can be classified into discrete groups: crimes that target individuals and organizations for financial gain, and crimes that target individuals and organizations for a social or political goal. Having reviewed the current and anticipated trends in IDT, we offer recommendations that span implementing technological changes, updating industry standards, developing incentives for businesses that maintain security proactively, expanding international cooperation, and implementing educational initiatives.

Introduction and Expanded Definition. IDT is a precipitating crime that is often a springboard for other illicit activity, traditionally involving financial fraud and cybercrime, but possibly also including manipulation of public sentiment, disruption of commerce, and links to terrorism. A review of open-source literature and interviews with subject matter experts[2] suggest that IDT is considered to be both increasingly technologically sophisticated, exploiting vulnerabilities in new technology and changes in policy, and victimizing both individuals and organizations. IDT is becoming increasingly popular among gangs and organized crime because it is comparatively more profitable and less risky than traditional street crime.[3] With its recent growth in the cyber environment, IDT has been projected to expand vis à vis a "Crime as a Service" (CaaS) model: malicious actors or groups may "purchase" an IDT crime or cyber attack from a computer-savvy provider.[4]

EXPANDED DEFINITION

Identity = Unique set of characteristics that define an entity or individual.

Identity Theft = Unauthorized use of an individual or entity's identity to conduct illicit activity.

As such, a more appropriate expanded definition of IDT must reflect the current and future landscape (see sidebar).

Current and Anticipated State of IDT Crimes. A perpetrator's primary motivations for committing IDT (financial or sociopolitical) and the victims targeted in IDT crimes (individuals or organizations) are represented in ***Exhibit 1***. The most commonly understood type of IDT is represented in the upper left quadrant: targeting individuals for financial gain.

Exhibit 1. Illicit Activity by Victim Level and Perpetrator Motivation

	PERPETRATOR MOTIVATION	
	Financial Gain	**Sociopolitical Goal**
Individual Victim	• Financial information (accounts; credit and debit cards) • Mobile commerce, including virtual currency • Identity documents (Social Security card, passport, driver's license)	• Social media attacks coupled with social engineering • Identity documents for anonymity and free movement (e.g., entry into the United States)
Organization Victim (Corporation or Government)	• Medical benefits, entitlements, and payments • Tax refunds • Wire transfers, corporate loans, account takeovers • Phishing coupled with social engineering	• Reputational/integrity attacks (data breaches, hacking social network accounts) • Disruption (denial of service, data breaches, hacking social networking accounts, account takeovers) • Terrorism (provide entry to the United States and funding for activities)

***Individuals Targeted for Financial Gain*.** Identity information is essential for thieves to commit most financially motivated IDT. Physical copies of identity documents (e.g., driver's licenses) are no longer essential for many types of commerce, as transactions are increasingly conducted online.

- Documents/benefits fraud and credit card fraud are currently the most commonly reported varieties of IDT. The Federal Trade Commission reports that in 2012 government documents/benefits fraud (46%) was the most common, followed by credit card fraud (13%), telephone or utilities fraud (10%), and bank fraud (6%).[5]
- Use of cards as a payment method continues to increase worldwide: $11.27 billion in 2012 attributed to IDT, up 14.6% over 2011.[6]
- Synthetic identity fraud, which is gaining ever more attention, is more difficult to detect as an identity is created by combining bits of information from multiple individuals or by mixing real and fictitious information. Because there is often no apparent victim, statistics on synthetic IDT are unknown.
- Data suggest that adolescents and senior citizens may be particularly vulnerable to financially motivated IDT.[7] Both groups may be more trusting of others, with adolescents being particularly technology dependent and overly relaxed about sharing personal information. Children are also becoming a target for identity thieves: 1 in 40 households with children under 18 experienced child identity fraud.[8]
- **As we approach 2017**, one should expect identity thieves to continue exploiting new technologies associated with mobile payment applications and mediums. Greater utilization of virtual currencies by consumers and producers may also spur a growth in IDT in this medium. Some credit card compromises may decrease if certain proposed technologies (e.g., pin and chip[9]) are more widely adopted. More traditional IDT schemes (e.g., mail theft, Dumpster diving) will continue but diminish in frequency because of the general decline of those media.[10]

***Organizations Targeted for Financial Gain*.** The primary target of much of the organization-level IDT for financial gain appears to be a combination of benefits providers (including the U.S. government) and small businesses. The former group often lacks the experiential risk management that private industry uses to detect potential fraud.[11] The latter group often lacks necessary resources to combat malicious actors who steal information or hijack systems for financial gain.

- In 2012, it was reported that over the next 5 years the Internal Revenue Service (IRS) could issue approximately $26 billion in fraudulent tax returns resulting from IDT.[12] The IRS issued 770,000 Identity Protection Personal Identification Numbers to previous IDT victims in processing year 2013: 3 times as many as were issued in the previous processing year.[13]
- From 2012 to 2013, the number of medical IDT victims increased by 19% in the 1-year base rate, from 1.5 million medical IDT victims in 2012 to 1.8 million victims in 2013. Medical IDT in 2013 had an estimated total out-of-

pocket cost to victims of approximately $12.3 billion.[14] Medical IDT may also complicate medical treatment (e.g., incorrect blood type, inaccurate test results and diagnoses). In addition, the victims' own insurance claims could be denied or their insurance could be canceled.

- Small business presents a high degree of potential exposure to IDT via online means. Almost 90% of U.S. businesses have fewer than 20 employees,[15] and 77% of owners of small or medium-sized businesses felt their companies were safe from cyber threats, although 83% had no cybersecurity plan.[16]
- Three-fourths (75%) of reported data breach cases are financially motivated.[17]
- A corporate IDT scheme gaining traction in the United States involves fraudulent business tax returns for dissolved or inactive companies found in state registries. Federal tax credit is applied for on behalf of the targeted (though inactive or dissolved) company for financial gain.
- Corporate IDT may occur where a recognized brand name, good business credit, or preexisting business relationships are exploited for fraudulent purchases or activities. Identity thieves may alter business registration information and seek to exert control over a business's operations via the "perceived authority" to operate on its behalf (e.g., a perpetrator may be able to initiate the fraudulent sale of assets, conduct transactions in the business' name, or open or access business bank accounts).
- **As we approach 2017**, one should expect the U.S. government and small businesses to be increasingly targeted for exploitation because of the actual or perceived lack of negative consequences (e.g., limited penalties and law enforcement) to identity thieves. Compromises of data aggregators who possess individuals' identifying information will likely become more prevalent.

Individuals Targeted for Sociopolitical Goals. Attacks on individuals targeted for sociopolitical reasons are generally undertaken with the goal of influencing others or exacting revenge on another. Identity thieves may conduct a combination of social media searches and social engineering to acquire enough of an individual's identifying information to impersonate him or her. Social media have become ideal venues to create and cultivate influence.

- Recently, it was reported that the President of Iran, Hassan Rouhani, tweeted that he wished "all Jews, especially Iranian Jews, a blessed Rosh Hashanah." Afterward, it was discovered that Mr. Rouhani does not have a Twitter account, suggesting that someone else with a political agenda sent the tweet to sway public sentiment.[18]
- A recent revenge-associated IDT case involved a spurned boyfriend who took over his former girlfriend's online identity to solicit sex. Numerous men arrived at the former girlfriend's home expecting sexual encounters.[19]
- **As we approach 2017**, one should expect more instances of identities stolen for the purpose of affecting the physical world through propaganda or revenge.

Organizations Targeted for Sociopolitical Goals. An organization's most valuable assets are its public image—also referred to as its brand—and its intellectual property. Negative publicity may tarnish an organization's image and may decrease the organization's perceived or real value, as reflected in the share price of the entity's stock. IDT has been facilitated by the online environment, with the perpetrators having political or social agendas (e.g., embarrass an institution, bring attention to a cause ["hacktivism"], influence public sentiment).

- The Associated Press's social media account was hacked in April 2013, falsely reporting that two bombs had exploded at the White House. This corporate IDT resulted in public uncertainty, which was immediately reflected in a precipitous fall in the New York Stock Exchange.[20]
- Reuters' news blogs were compromised in August 2012 with the posting of an interview stating that Syrian rebels had retreated from a military location. Soon afterward, the Free Syrian Army denied that any such interview or retreat had taken place and blamed the Syrian government for the false blog post.[21]
- **As we approach 2017**, organizations should expect an increase in being targeted to promote sociopolitical agendas, especially if the media continue to provide a forum for others to publicize their agendas.

Recommendations.

1. Adopt a multi-factor identification system to increase security for transactions and documents of significance. Current single-factor authentication (e.g., password) is insufficient to protect an individual's identity when conducting transactions of significance (e.g., online purchases). Multi-factor authentication (i.e., a combination of what you know and who you are) is a promising alternative to improve security for transactions and documents of significance (e.g., renewing a driver's license).

2. Designate a single agency and dedicate a central database for incident reporting and measurement of IDT cases. Presently, businesses and individuals may elect to contact any of a multitude of agencies or other reporting structures to alert others of an IDT-related incident (e.g., 9-1-1, the U.S. Secret Service or the Federal Bureau of Investigation, the Internet Crime Complaint Center [iC3], the Federal Trade Commission's Consumer Sentinel, the affected financial institution). A significant portion of individual IDT (estimated at 38%[22] or higher[23]) goes unreported to law enforcement, possibly because of confusion about where or how to report it. Clear guidance on reporting incidents and a single source for reporting would create a central location to store these data, assist with deconfliction for coordinating responses and linking similar cases, and allow for data collection to measure and better understand trends in IDT. Such an approach would also serve as an incentive for more timely and thorough reporting.

3. Increase funds for law enforcement to pursue IDT by adding manpower, resources, and training. Investigation into IDT incidents requires continuous training and adequate resources for law enforcement investigators. IDT case investigations are hobbled by budget cuts and limited resources. Especially in the cyber environment, IDT investigations are complex, requiring creativity, persistence, and international cooperation to determine attribution and realize resolution.

4. Design and implement a public education campaign leveraging schools, online users, and companies. Public awareness campaigns should begin by targeting vulnerable populations to highlight what common tactics are used and how users may protect themselves. Students and seniors should receive age-appropriate lessons as they explore the online environment. Small businesses should be the subject of particular focus to help them better allocate limited resources.

5. ***Design and implement incentives for public and private compliance with best practices in identity security and privacy standards.*** Encourage government and small businesses to invest in appropriate security infrastructure so that identifying data are securely stored, transferred, and sanitized.

6. ***Regularly revisit a globally accepted legal definition of IDT to encompass evolving perspectives.*** Continue to encourage broad international adoption of a globally accepted definition of IDT, as well as international law enforcement cooperation.

7. Strengthen existing legislation and increase penalties for IDT domestically and internationally, and evaluate annually to keep pace with criminals. Adopt strict privacy regulations to better protect people and entities in both virtual and physical environments. Although state statutes differ, current laws related to IDT are generally limited, and the penalties associated with committing IDT should be revisited to keep pace with emerging trends. States that have adopted innovative policies to protect children's credit[24] should serve as models where measurable benefit is realized.

8. Encourage individual and institutional online identities to obfuscate their location, source, or identification through employing multiple virtual identities or and proxies**.** This approach would effectively challenge perpetrators to verify the identity of their target against multiple alternatives, rendering the act of IDT increasingly difficult and complex.

2013 IDENTITY THEFT AND NEXUS TO ILLICIT ACTIVITY TEAM

Jynika Craig
Federal Bureau of Investigation
jynika.craig@ic.fbi.gov

Jason Kerben
Office of the Director of National Intelligence
jasonk@dni.gov

John D. King
Department of the Army (NGIC)
john.d.king50.civ@mail.mil

Edward T. Lanoue
HSBC Bank
ed.t.lanoue@us.hsbc.com

Karen Lissy
RTI International
klissy@rti.org

Chris Sailer
Bill and Melinda Gates Foundation
chris.sailer@gatesfoundation.org

Kristin Schwomeyer
WellPoint
kristin.schwomeyer@wellpoint.com

Jason Thomas
Thomson Reuters
Jason.Thomas@trssllc.com

Brett Yellen
Department of Homeland Security
Brett.Yellen@hq.dhs.gov

Acknowledgments. We extend our grateful appreciation to the following individuals and organizations for generously sharing their expertise and opinions: Stephen Coggeshall (ID Analytics), Chuck Cohen (Indiana State Police), Marc Goodman (Singularity University), Donald Rebovich (Utica College), Jonathan Rusch (U.S. Department of Justice); Department of Homeland Security—Homeland Security Investigations; Microsoft; Nike; Seattle Police Department; Social Security Administration—Office of the Inspector General; T-Mobile; and the U.S. Secret Service.
Published November 2013

---

[1] Javelin Research and Strategy. (2013). *Identity theft/fraud statistics*. Arlington, VA: Author. Retrieved from http://www.statisticbrain.com/identity-theft-fraud-statistics/

[2] Please refer to the Acknowledgments section to see the names of the agencies and individuals who were consulted in preparing this document.

[3] Federal Bureau of Investigation. (2011). *2011 National Gang Threat Assessment: Emerging trends*. Retrieved from http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment

[4] Goodman, M., & the DHS Identity Theft and Nexus to Illicit Activity Team. (2013, July 26). *The future of identity theft* (report of site visit to Seattle, WA).

[5] Federal Trade Commission. (2013). *Consumer Sentinel Network data book for January–December 2012*. Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf

[6] The Nilson Report. (2013, Aug. 19). Global credit, debit, and prepaid card fraud losses reach $11.27 billion in 2012; up 14.6% over 2011 according to the Nilson Report. *MarketWatch*. Retrieved from http://www.marketwatch.com/story/global-credit-debit-and-prepaid-card-fraud-losses-reach-1127-billion-in-2012-up-146-over-2011-according-to-the-nilson-report-2013-08-19?goback=%2Egde_2196752_member_270999551

[7] Bureau of Justice Statistics. (2010). *National Crime Victimization Survey supplement: Victims of identity theft, 2008*. Retrieved from http://www.bjs.gov/content/pub/pdf/vit08.pdf

[8] Identity Theft Assistance Center. (2012, December). *2012 child identity fraud report*. Summary available at http://www.identitytheftassistance.org/pageview.php?cateid=47#childIDfraudReport

[9] Frellick, M. (2011, August 10). Visa reverses course on chip-and-PIN credit cards. *Credit Card Guide.* Retrieved from http://www.creditcardguide.com/creditcards/news/visa-reverses-chip-pin-credit-cards-1365/#ixzz2ibYl9sJt

[10] For example, New Zealand recently announced that it is curtailing mail service given its decline in use ("New Zealand moving to 3 days a week mail service," retrieved from http://abcnews.go.com/Technology/wireStory/zealand-approves-days-week-mail-service-20653147).

[11] Telephone conversation with Stephen Coggeshall, ID Analytics, 3 Sept 2013.

[12] *Identity theft and tax fraud: Joint Hearing before the Committee on Ways and Means, Subcommittees on Oversight and Social Security,* 112th Cong. (2012) (testimony of J. Russell George). Retrieved from http://www.treasury.gov/tigta/congress/congress_05082012.pdf

[13] *Ibid*.

[14] Ponemon Institute. (2013, September). New research reveals medical identity theft is up, affects 1.84 million U.S. victims [press release]. *Medical Identity Fraud Alliance.* Retrieved from http://medidfraud.org/press-release-2013-survey-on-medical-identity-theft/

[15] U.S. Census Bureau. (2010). *Statistics about business size from the U.S. Census Bureau*. Retrieved from http://www.census.gov/econ/smallbus.html

[16] Symantec. (2012). New survey shows U.S. small business owners not concerned about cybersecurity; majority have no policies or contingency plans [press release]. Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

[17] Verizon Business. (2013). *2013 data breach investigations report*. Available from http://www.verizonenterprise.com/DBIR/2013/

[18] FARS News Agency. (2013, September 5). Iran denies media reports about President Rouhani's New Year tweet to Jews. Retrieved from http://english.farsnews.com/newstext.aspx?nn=13920614000756

[19] Calm, C. (2012, February 12). Ex-boyfriend posts fake sex ads on Craigslist. *AZ Family.* Retrieved from http://www.azfamily.com/news/Ads-offering-sex-with-ex-girlfriend-land-man-in-jail--140308753.html

[20] Kelly, S. M. (2013, April 23). AP twitter hack falsely claims explosions at White House. *Mashable.* Retrieved from http://mashable.com/2013/04/23/ap-hacked-white-house/

[21] Martin, A. (2012, August 3). Reuters blogs hacked with fake story about Syrian rebel retreat. *Atlantic Wire.* Retrieved from http://www.theatlanticwire.com/technology/2012/08/reuters-blogs-hacked-fake-story-about-syrian-rebels/55394/

[22] Federal Trade Commission, op. cit.

[23] Bureau of Justice Statistics, op. cit.

[24] Examples are the Child Identity Protection Program of the Utah attorney general (https://cip.utah.gov/cip/SessionInit.action) and protection of children in foster care in other states (http://www.foxnews.com/us/2011/10/09/new-law-protects-foster-children-from-identity-theft/).