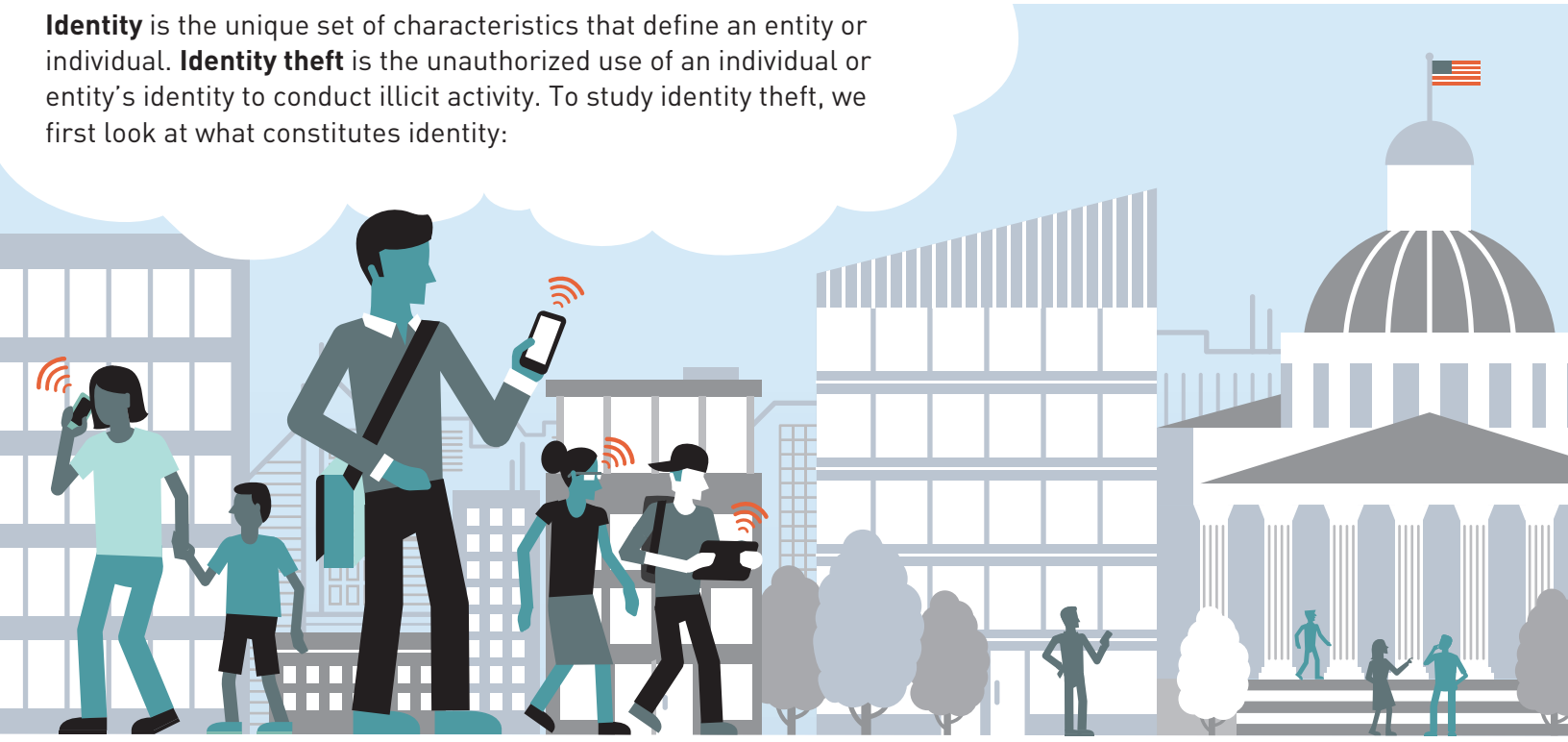


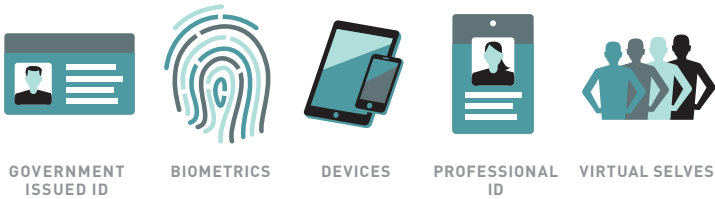
THE CHANGING FACE OF IDENTITY THEFT

THE CURRENT AND FUTURE LANDSCAPE

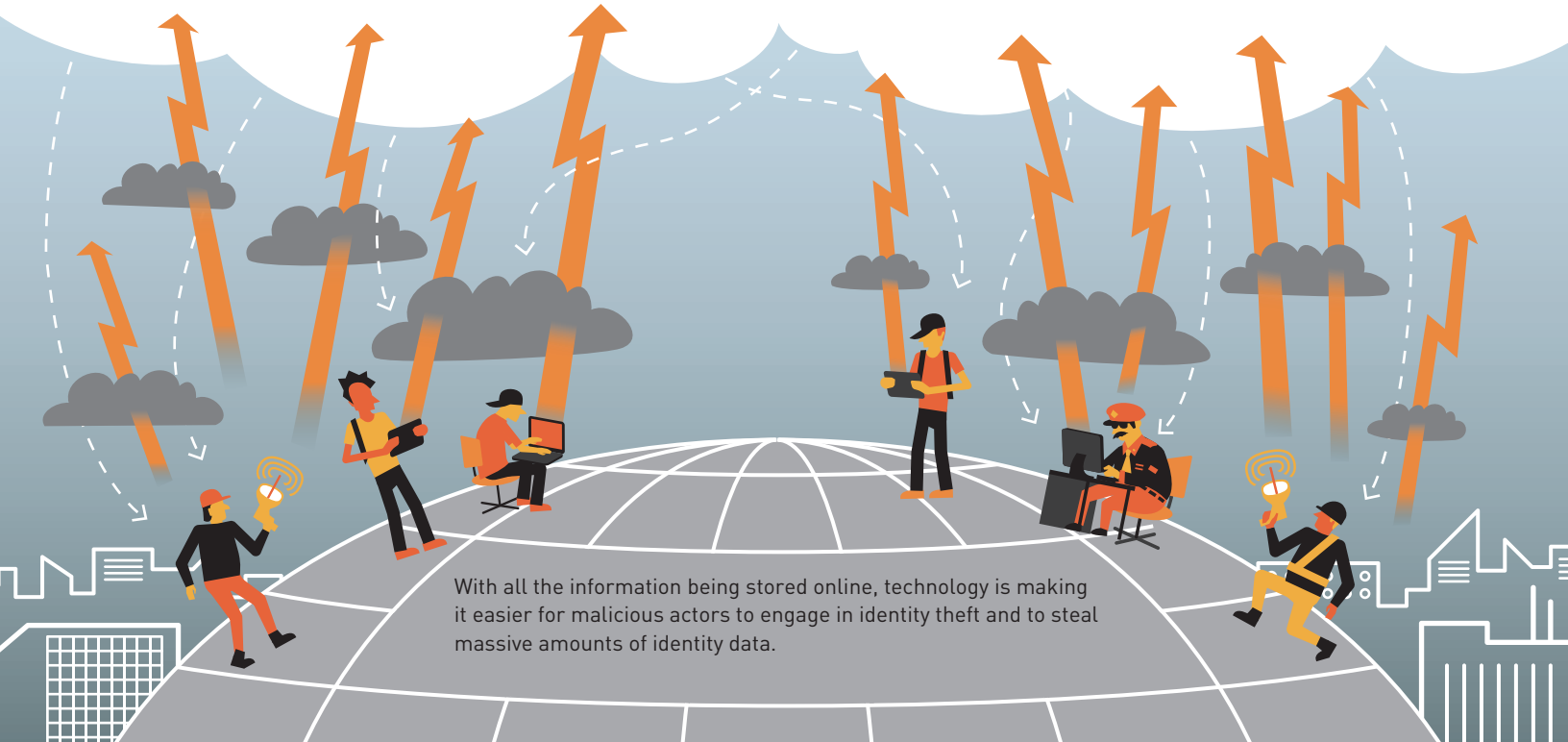
Identity is the unique set of characteristics that define an entity or individual. **Identity theft** is the unauthorized use of an individual or entity's identity to conduct illicit activity. To study identity theft, we first look at what constitutes identity:



IDENTITY FOR THE INDIVIDUAL



IDENTITY FOR THE ORGANIZATION



With all the information being stored online, technology is making it easier for malicious actors to engage in identity theft and to steal massive amounts of identity data.

Identity Theft 2013

The following statistics illustrate the scope and cost of identity theft in 2013.



Credit, debit and prepaid cards worldwide experienced gross fraud losses of

\$11.27 BILLION in 2012

Identity theft accounts for an annual loss estimated at



in the U.S.

CHILD ID FRAUD



1 in 40 households with children under 18 have experienced child ID fraud.

IRS FRAUD



The IRS could issue approximately **\$26 billion** in fraudulent tax returns resulting from ID theft between 2013 and 2018.

MEDICAL ID FRAUD



Nearly **1.8 million** Americans are victims of medical ID theft every year. This is not only costly but it also threatens lives.

SMALL BUSINESS

Small business presents a high degree of potential exposure to identity theft via online means. **More than 77%** of small and medium-sized business owners believe their company is safe from cyber threats, however...



MOTIVES

75% of reported data breach cases are financially motivated.



Identity Theft 2017

Identity thieves use technology to keep one step ahead of security experts and law enforcement. By 2017, identity thieves will reach into every part of our lives and into institutions and organizations from anywhere in the world. Here is a snapshot of the emerging trends in identity theft in 2017.

MOTIVATION:
SOCIO-POLITICAL
TARGET:
ORGANIZATIONAL

REPUTATION
Phishing attacks target institutions to access data or impersonate the organization for social/political causes. These attacks harm organizations' credibility and impact their mission and are increasingly launched by anarchist or national criminal groups.



ORGANIZATIONAL



WIRE TRANSFERS
Through hacking and social engineering, criminals create fraudulent documents impersonating real companies and transfer money. Wire transfers are worth tens or hundreds of thousands of dollars and are a growing target for criminals.



PHISHING
Spear phishing allows thieves to masquerade as a company or organization for financial gain. Hundreds of thousands of phishing attacks are sent each day and tens of thousands of people reply.

MOTIVATION:
FINANCIAL
TARGET:
ORGANIZATIONAL



TAX REFUNDS
With just a name, address and Social Security Number, organized crime groups file millions of fraudulent tax returns early to obtain refunds before individuals file their genuine returns.

DISRUPTION

Hackers attack websites, internal information and security systems in order to disrupt or cripple organizations and businesses. Attacks become more widespread shutting down entire businesses, industries or locations for longer periods.



TERRORISM

Identity theft provides hundreds of potential terrorists entry into the United States. Fake identities or fraudulent account numbers are used by terror networks to launder money or to finance their operations.



MEDICAL FRAUD

A single medical insurance card is worth 40 times more than a Social Security card on the black market. Health care cooperatives have become a prime target for identity thieves. Erroneous information increasingly shows up on medical records leading to serious health risks, even death.



SOCIO-POLITICAL

FINANCIAL

TARGETING VULNERABLE GROUPS

Criminal groups increasingly target children, the elderly and other vulnerable groups. Online gaming sites for kids have become a prime target for identity thieves.



BANK ACCOUNTS

Bank account numbers remain one of the biggest targets for criminals and organized crime. Large-scale theft of millions of account numbers and online transactions become commonplace across borders where criminals can evade law enforcement.



SOCIAL MEDIA ATTACKS

Thieves impersonate people on social media, harming their reputation by taking over or creating false social media pages and posting pictures or other defamatory information.



MOBILE ID

Mobile devices are the primary means of identification. The devices include fingerprint information, bank and payment accounts, airplane tickets, pins and passwords. The depository of information becomes an irresistible target for identity thieves.



MOTIVATION:
SOCIO-POLITICAL
TARGET:
INDIVIDUAL

DOCUMENT THEFT

Thieves use stolen documents, including passports and driver's licenses, for illegal purposes including entry into the United States. RFID chips on some passports become a target giving thieves more information on victims and more credibility in forging new documents.



INDIVIDUAL

DOCUMENTS and IDENTIFICATION

Thieves, especially organized gangs, steal documents, mail, account numbers and payments from individuals for fraudulent use and financial gain. Securing communications becomes urgent.



MOTIVATION:
FINANCIAL
TARGET:
INDIVIDUAL

Our Recommendations

EDUCATION

Design and implement a public education campaign leveraging schools, online users and companies.

GOVERNANCE

Designate a single agency and dedicate a single database for incident reporting and measurement.

INCENTIVES

Increase funds for law enforcement to pursue identity theft by adding manpower, resources and training.

Design and implement incentives for public and private compliance with best practices in identity security and privacy standards.



LEGAL / LEGISLATIVE

Adopt strict privacy regulations to better protect people and entities in virtual and physical environments.

Regularly revisit a globally-accepted legal definition of identity theft to encompass evolving perspectives.

Strengthen existing legislation and increase penalties for identity theft domestically and internationally. Evaluate annually to keep pace with criminals.

PROTECTION

Encourage individual and institutional online identities to obfuscate the location, source or one's identification through employing multiple virtual identities and/or proxies – rendering the act of identity theft increasingly difficult and complex.

TECHNICAL

Adopt a multifactor ID system for transactions and documents of significance.

2013 Identity Theft and Nexus to Illicit Activity Team



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



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



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



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



Karen Lissy
RTI International
klissy@rti.org



John D. King
Department of the Army
National Ground Intelligence Center
john.d.king50.civ@mail.mil



Jason Thomas
Thomson Reuters
jason.thomas@trssl.com



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



Kristin Schwomeyer
WellPoint
kristin.schwomeyer@wellpoint.com

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 (US 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 US Secret Service.