INFORMATION EXPOSED

Historical Examination of Data Breaches in New York State

From the Office of:

New York State Attorney General

Eric T. Schneiderman

Dear Fellow New Yorker,

Every day, New Yorkers share personal information with companies, government agencies, and other organizations, either out of necessity or simply for the sake of convenience. When we do, we trust these institutions to protect our sensitive data from unauthorized access. That is why New York has a data breach notification law. If an unauthorized individual accesses your personal information, the institution that suffered the data breach must notify you, as well as my office, as soon as possible. An institution that fails to provide this notification is liable for damages and enhanced penalties.

This report, "Information Exposed: Historical Examination of Data Breaches in New York State," analyzes the data breach notices my office has received for the last eight (8) years. It reveals that the number of reported data security breaches in New York more than tripled between 2006 and 2013. As a result, in just eight years, the number of victims in New York has exploded. Over 22 million personal records have been exposed since 2006, jeopardizing the financial health and well-being of countless New Yorkers and costing the public and private sectors in New York — and around the world — billions of dollars. This report offers fresh statistics and analysis of the scope, complexity, and cost of data breaches in New York State.

As information increasingly drives commerce and government, the challenges presented by data security breaches will continue to grow. There may be no foolproof defense against certain threats, like hacking attacks by sophisticated thieves. However, organizations can do more to prevent other types of breaches, such as insider wrongdoing and inadvertent disclosures, by ensuring that they have the best data security practices in place. This report provides recommendations that individuals and organizations can implement to protect themselves from data loss.

While the defensive measures we recommend for individuals and businesses can be helpful, the scope of the data breach problem detailed in this report demands a systemic response. Moving forward, my office plans to take a collaborative approach to address the complex problems surrounding data security. By engaging industry stakeholders and security experts, as well as lawmakers, we can ensure that organizations across the state have access to the tools and information necessary to promote the best data security practices. By doing so, we can continue to enjoy the many benefits of technological innovation without putting ourselves at risk.

Sincerely,

Eric T. Schneiderman
Attorney General

KEY FINDINGS

Businesses, charitable organizations, and public agencies routinely collect personal information from New Yorkers, including Social Security and credit card numbers. The New York State Office of Attorney General (NYAG) has received notifications of organizations experiencing data breaches since the New York State Information Security Breach & Notification Act took effect in 2005. This report summarizes, analyzes, and provides context to the broader trends revealed by eight years of New York State security breach data.

Data Breaches Are An Increasing Menace

Nearly 5,000 individual data breaches were reported to the NYAG by businesses, nonprofits, and government entities between 2006 and 2013. Together, these breaches exposed 22.8 million personal records of New Yorkers. The number of data security breaches reported annually to the NYAG more than tripled between 2006 and 2013 – and 2013 was a record-setting year, during which 7.3 million records of New Yorkers were exposed. So-called mega-breaches are also becoming increasingly common: Five of the ten largest breaches reported to the NYAG have occurred since 2011.

NEW YORK STATE DATA SECURITY BREACH SUMMARY

Breaches exposed 22.8 million personal records of New Yorkers between 2006 and 2013.

The number of reported data breaches tripled between 2006 and 2013.

In 2013, data breaches cost entities conducting business in New York upward of $1.37 billion.

Hacking attacks accounted for over 40 percent of data security breaches, between 2006 and 2013.

Five of the 10 largest breaches occurred in the past three years.

Value Of Information & Negligence Drive Data Breaches

The overall cost of data security breaches is nothing short of staggering: In 2013 alone, breaches are estimated to have cost organizations doing business in New York State over $1.37 billion. Hacking intrusions – in which third parties gain unauthorized access to data stored on a computer system – were the leading cause of data security breaches among organizations conducting business in New York State, accounting for roughly 40 percent of all breaches between 2006 and 2013. Hacking attacks are driven primarily by the black-market value of personal information, which can fetch up to $45 per record. Reports of insider wrongdoing and inadvertent exposure have increased over the past eight years, with incidents of insider wrongdoing reaching their highest level in 2013. Although instances of lost or stolen equipment/documentation declined in recent years, these incidents are responsible for a significant portion of data breaches and personal record loss since 2006.

Reduce Risk By Taking Action

Organizations and individuals can take practical steps to both prevent data security breaches and mitigate potential harm in the event of a breach. The NYAG strongly suggests that all organizations collect electronic information devise and implement a comprehensive data security plan. Individuals should take steps such as monitoring financial statements and practicing their own data-minimization techniques to protect themselves against threats.

INTRODUCTION: BIG DATA POSE BIG CHALLENGES

Never before have electronic data been so integral to the operations of so many organizations across New York State. Public and private organizations alike have harnessed the power of "Big Data" to provide better services and products to consumers and constituents. Big data have become increasingly affordable. In fact, according to a recent report from the White House, the cost of creating, capturing, managing, and storing digital information has dropped to only one-sixth the cost in 2005.[1]

At the same time, data security breaches became an increasing threat to our digital security. According to a January 2014 Pew Research poll, nearly one-fifth of all Americans (18 percent) reported having had personal information, such as a Social Security number, credit card or bank account information, stolen in their lifetime, an increase of seven percent since July 2013.[2] An even higher proportion (23 percent) reported having their e-mail or social networking accounts compromised, according to the same report.

Data security breaches are more than simply a privacy concern – they can have harmful consequences. Studies by the Javelin Strategy and Research Group[3] and by LexisNexis[4] estimated approximately one-fourth of all records lost in data security breaches are used for fraudulent purposes such as identity theft. In 2012, direct and indirect identity theft losses totaled $24.7 billion in the United States, a figure that exceeded the losses in all other categories of property crime combined.[5]

Since December 2005, the NYAG has collected information reported to the Office under the New York State Information Security and Breach Notification Act. The information in those notices, and the trends and patterns that emerged over eight years of analysis, paint a sobering picture of the state of data security in New York.

NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT

Effective December 7, 2005 as Business Law 899-aa

The Information Security Breach and Notification Act (Business Law 899-aa) ensures New York State residents' right to know when a security breach has exposed their personal information. A more detailed summary and the full-text of New York State Business Law 899-aa is located in Appendix C.

KEY TERMINOLOGY

Data Security Breach ("Breach"):
An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. A breach can expose anywhere from a handful to millions of records.

Personal Information:
Information that can be used to distinguish or trace an individual's identity. Personal information includes name, Social Security number, biometric records, date and place of birth, mother's maiden name, driver's license number, or financial account information.

Personal Records:
When an entity reports a data security breach to the NYAG, it is required to provide the number of New York residents believed to have been affected by the breach. An individual may have had three pieces of personal information compromised during the breach, but the organization will account that information as affecting one New Yorker. As such, the phrase "personal records" is a unitary term referencing the total personal information exposed during a given breach that is attributable to a given New Yorker.

Note: The personal records associated with the same individual may have been exposed in multiple breaches.

DATA BREACHES ARE AN INCREASING MENACE

In the days before Thanksgiving 2013, a highly coordinated hacking conglomerate based in Russia installed a piece of malicious software on Target's point-of-sale credit card processing system.[6] By the time the national retailer became aware of the breach, the hackers had siphoned off personal information, including credit card numbers, of between 70 million and 110 million consumers nationwide.[7]

While the Target breach was widely publicized, it was only one example of the imminent threat data security breaches pose to organizations that collect, store, or disseminate sensitive personal information. While the extent of the Target breach was certainly alarming, the size and mission of an organization do not necessarily predict the likelihood of a breach. In fact, during the eight-year period analyzed, a widely diverse set of organizations, ranging from local family businesses to large multinational corporations, reported data security breaches to the NYAG. The trend is clear: Data security is a serious challenge for organizations of all kinds.

2013: A RECORD-SETTING YEAR FOR DATA SECURITY BREACHES IN NEW YORK

More than 900 data security breaches exposed the personal records of 7.3 million New Yorkers in 2013. This record-setting data loss was driven largely by two retail mega-breaches (Target and Living Social) that have led some to dub 2013 "The Year of the Retailer Breach."[8] Though hacking incidents cause fewer than half of the total breaches in New York, they accounted for 96.4 percent of the total personal record loss in 2013. Hacking was not the only data security breach category to reach record highs – 2013 was also a record year for insider wrongdoing and inadvertent data disclosure events.

Data Breaches Grew in Frequency and Scope

Data breaches compromised 22.8 million personal records of New Yorkers between 2006 and 2013. More than 3,000 businesses, nonprofits, and government entities reported a data security breach to the NYAG during that eight-year period, totaling nearly 5,000 breaches. As shown in Figure 1 on the next page, hacking was the leading cause of data security breaches, accounting for roughly 40 percent of all breaches, followed by lost or stolen equipment/ information (24%), and insider wrongdoing (10%).

Figure 1: Hacking Was Leading Data Breach Category in New York State

Data Security Breach Cause	Number of Breaches (% of Total)	Personal Records Exposed (% of Total)
Hacking	2,009 (40.78%)	14,416,488 (63.3%)
Lost or Stolen Equipment/Documentation	1167 (23.69%)	6,032,389 (26.51%)
Insider Wrongdoing	511 (10.37%)	1,229,779 (5.40%)
Inadvertent	997 (20.24%)	912,547 (4.01%)
Recovery By Law Enforcement[i]	80 (1.62%)	65,974 (0.29%)
Other	26 (0.53%)	29,609 (0.13%)
Website Compromise	53 (1.08%)	22,460 (0.10%)
Third Party Unauthorized Access	14 (0.28%)	14,500 (0.06%)
Unknown	32 (0.65%)	14,470 (0.06%)
Misplacement/Misdirection	19 (0.39%)	13,248 (0.06%)
Skimming	18 (0.37%)	1,190 (0.01%)
Total	**4,926**	**22,752,654**

Source: New York State Security Breach Reporting Forms (2006-2013)

UNDERREPORTED BREACHES: HEARTLAND PAYMENT SYSTEMS & TJX COMPANIES

While the number of personal records exposed during the eight-year period is startling in its own right, underreporting suggests the total sum of compromised records was likely much higher. For approximately six months between 2008 and 2009, a team of Russian hackers penetrated Heartland Payment Systems, one of the country's largest credit card processing systems. By the time the breach was discovered, an estimated 130 million credit card records were stolen across North America.[9] However, when Heartland Payment Systems reported the breach to New York State, it could not provide an accurate estimate of personal record loss. As a result, the number of personal records of New Yorkers compromised as a result of this breach is not fully enumerated in the breach logs.[ii] An almost identical situation occurred in 2007, when TJX Companies (owner of T.J. Maxx, Marshalls, and Bob's Stores) experienced a massive data security breach.[iii] In filings to the Securities and Exchange Commission, TJX Companies indicated that credit card information for 45.6 million Americans had been stolen during the breach,[10] but they also could not provide an accurate number or estimate of personal record exposure.

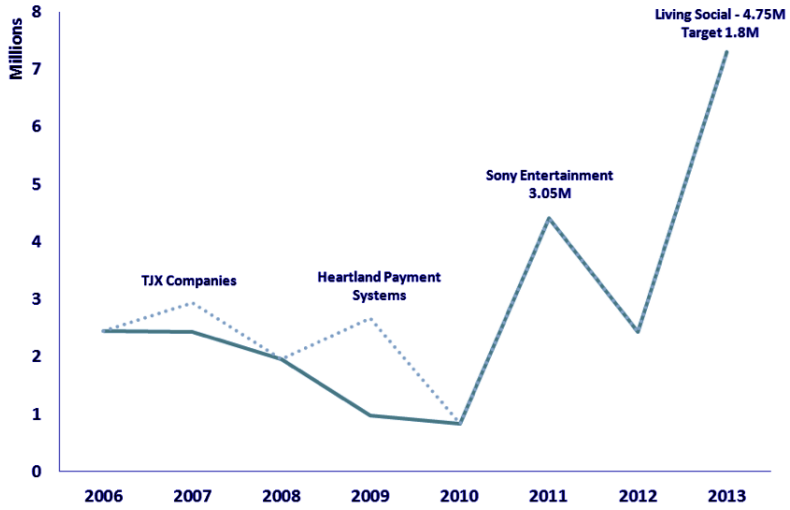
[i] This category refers exclusively to notifications made by American Express to New York State. When law enforcement agencies report fraudulent activity of New Yorkers' accounts to American Express, they also report it to the NYAG

[ii] Although Heartland Payment Systems did not report a number of personal record exposures to the NYAG, five independent entities that used Heartland's services made notifications to the NYAG in 2009, totaling 13,463 personal records of New Yorkers

[iii] Although TJX Companies did not report a number of personal record exposures to the NYAG, independent entities made notifications of information loss due to the breach, totaling 12,086 personal records of New Yorkers

The annual number of data security breach occurrences reported to the NYAG has more than tripled since 2006, with increases almost every year. Over half the total data security breaches reported to the NYAG have occurred in just the past three years. Figure 2, below, charts the number of personal records exposed each year between 2006 and 2013. The solid series depicts the number of personal records exposed that were reported to the NYAG. Considering the magnitude of the TJX Companies and Heartland Payment System breaches, the second "dotted" series adds a conservative estimate of the potential number of personal records exposed by both the TJX Companies and Heartland Payment Systems breaches.[iv]

Figure 2: Number of Personal Records Exposed Volatile but Trending Upward



Source: New York State Security Breach Reporting Forms (2006-2013)

Mega-breaches: Large-Scale Events Drive Data Loss

In just eight years, 28 mega-breaches[v] were reported to the NYAG, exposing approximately 18.2 million personal records of New Yorkers. Despite constituting only a sliver of reported breach events between 2006 and 2013, these 28 mega-breaches were responsible for nearly 80 percent of personal records exposed. What's more, mega-breaches are a growing phenomenon – five of the 10 largest breaches reported to the NYAG occurred in the past three years. Figure 3, on the next page, lists the top 10 breaches since 2006 in terms of numbers of personal record exposures. Also shown below, reports of hacking intrusions and lost or stolen equipment are the two primary drivers of mega-breaches. Hacking, detailed in the next section, poses a particularly nefarious challenge to data security, as large volumes of sensitive information are typically obtained for the express purpose of committing fraud.

[iv] The NYAG estimated the number of New Yorkers affected by the Heartland Payment Systems and TJX Companies breaches using the 2013 Target breach as a rough benchmark. While more records were exposed during the Heartland Payment Systems breach than in the Target breach, the NYAG conservatively estimated the Heartland breach to have affected at least 1.7 million New Yorkers. With TJX Companies, where approximately 1/3 of the number of personal records were exposed, the NYAG conservatively estimated that at least 500,000 New Yorkers were affected by the TJX Companies breach.

[v] Data breach events during which the personal records of at least 100,000 New Yorkers were compromised.

Figure 3. Five of Ten Largest Breaches Occurred Since 2011

Reporting Entity	Year	Personal Records Exposed	Cause of Breach
LivingSocial	2013	4,750,000	Hacking
Sony Entertainment	2011	3,050,000	Hacking
Target Corporation	2013	1,797,000	Hacking
Heartland Payment Systems	2008-09	1,700,000	Hacking
NYS Electric & Gas	2012	1,699,905	Hacking
BNY Mellon Bank	2008	1,602,567	Lost/Stolen Hardware/Documentation
CS STARS	2006	722,000	Lost/Stolen Hardware/Documentation
North Bronx Healthcare	2011	595,509	Lost/Stolen Hardware/Documentation
TJX Companies	2007	500,000	Hacking
TD Ameritrade Holding Corp	2007	486,738	Hacking

Source: New York State Security Breach Reporting Forms (2006-2013)

Retailers and Health Care Providers Are Particularly Vulnerable to Data Security Breaches

Certain industries were particularly susceptible to data security breaches during the eight years analyzed. Since 2006, a total of 241 institutions (approximately 8 percent of all reporting entities) reported three or more data security breaches to the NYAG. As shown below in Figure 4, retailers are the most likely to experience three or more data breaches. This is largely because retailers' payment systems (particularly restaurant payment systems) have become a favorite target of hackers.[11] Data breaches in the health care industry have exposed the largest number of personal records of New Yorkers since 2006. As the health care industry moves toward increasing digitization, it has become a repository for large troves of sensitive information, making the industry uniquely susceptible to data loss, particularly through lost or stolen electronic storage equipment.

Figure 4: Retail Services Are Most Likely to Be "Multiple Breach Entities"

Industry Type	Entities With 3+ Breaches	Personal Records Exposed
Retail Services	54	163,319
Financial Services	31	624,000
Health Care	29	1,012,269
Banking	27	560,208
Insurance	20	72,138
Professional Services	16	788,280
Educational Inst.	15	103,787
Government Agency	14	86,548
Loan Services	9	133,866
Hospitality	8	16,091
Technology	7	13,195
Telecommunications	4	80,963
Credit Reporting	3	3,120
Credit Card Company	2	237,296
Nonprofit	1	507
Public Utility	1	50,456
Grand Total	**241**	**3,946,043**

Source: New York State Security Breach Reporting Forms (2006-2013)

VALUE OF INFORMATION& NEGLIGENCE DRIVE DATA BREACHES

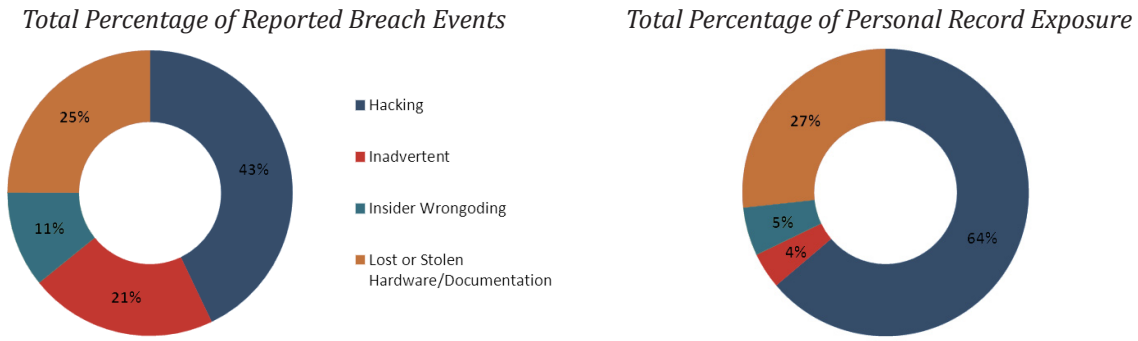
The personal information that makes up personal records is a valuable commodity on the digital black market. Freshly acquired stolen credit card numbers can fetch up to $45 per record, while other types of personal information, such as Social Security numbers and online account information, can command even higher prices. [12] Nonfinancial information can be more valuable, as fraudulent use of this data is more difficult to detect and the information can be used for a broader range of purposes.[13] For example, a stolen Facebook account can provide an access point to a wide range of user accounts (many people use the same password across multiple online platforms), or can be used as a vehicle to steal information (i.e. through phishing – sending links that provide hackers with access to a computer) from others within that individual's social network.[14] For criminals, stealing data can be as lucrative as drug trafficking, but with far less risk and fewer barriers to entry. [15] This combination of high profit potential and low risk drives the market for hacking breaches.

Not all data security breaches are created equal. For example, the causes of an accidental breach can range from a simple mistake to broad negligence, while a hacking attack can originate with a single disgruntled employee with limited technical proficiency, or a highly sophisticated international hacking syndicate. Consequently, breach events can vary widely in terms of scope and scale. For instance, incidents of inadvertent exposure, such as a small business accidentally faxing a document to a subcontractor without redacting a customer's name and credit card number, tend to expose fewer personal records despite occurring relatively frequently. Hacking attacks, which are often undertaken with the explicit goal of stealing information, tend to compromise many more personal records of New Yorkers.

The Big Four

Four data breach categories accounted for almost all breaches in New York State. The four primary categories of data breaches are: hacking, inadvertent exposure, insider wrongdoing, and lost or stolen equipment/documentation. These four categories accounted for 95 percent of the total breach events reported to the NYAG and over 99 percent of total personal record loss between 2006 and 2013. Figure 5, below, depicts the percentage of breach events, and the percentage of personal records exposed by those events, that were attributable to each of those four categories.

Figure 5: Most Data Breaches Attributable to Four Types; Some Categories Inflict Greater Record Loss



Source: New York State Security Breach Reporting Forms (2006-2013)

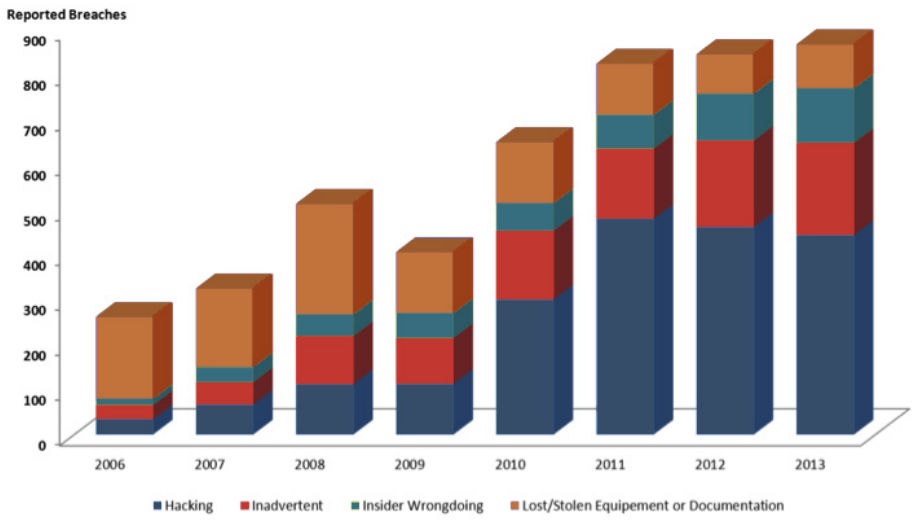
NEW TECHNOLOGY, NEW THREATS

The rapid pace of innovation — particularly in mobile technology — will continue to provide additional platforms for hackers to exploit. Countless Americans store huge amounts of personal information on their mobile devices, and malware created to exploit mobile software platforms has started to proliferate.[16] Additionally, mobile phone users often connect to unsecured and unencrypted public WiFi networks that can be easily penetrated by an experienced hacker.[17] Americans seem largely unaware of these threats, as they increasingly use mobile devices to conduct sensitive transactions, such as mobile banking, despite the fact that many of those activities have proven vulnerable to hacking attacks.[18]

Value of Information Incentivizes Hacking and Insider Wrongdoing

The number of hacking incidents reported to the NYAG showed the most dramatic increase over the eight-year period analyzed. A mere 34 instances of hacking were reported to the NYAG in 2006; those grew to over 400 reported incidents in every year since 2011, increasing most dramatically between 2009 and 2011. During that period, easy-to-use "crimeware"[19] applications such as "ZeuS" source code became widely available, according a 2014 RAND Corporation report on Cybercrime Tools and Stolen Data.[20] After the original code for "ZeuS" was published publicly, thousands of variations were created, allowing the program to flourish and largely evade eradication. To date, "ZeuS" and its primary offshoot, "Citadel," remain a hacker favorite for stealing information.[21] Figure 6, below, illustrates the larger trends in the top four categories of breaches between 2006 and 2013. Reports of insider wrongdoing and inadvertent exposure have increased steadily over the past eight years as well, with incidents of insider wrongdoing reaching their highest level in 2013.

Figure 6: Hacking Grows to Dominate Reported Data Security Breach Types

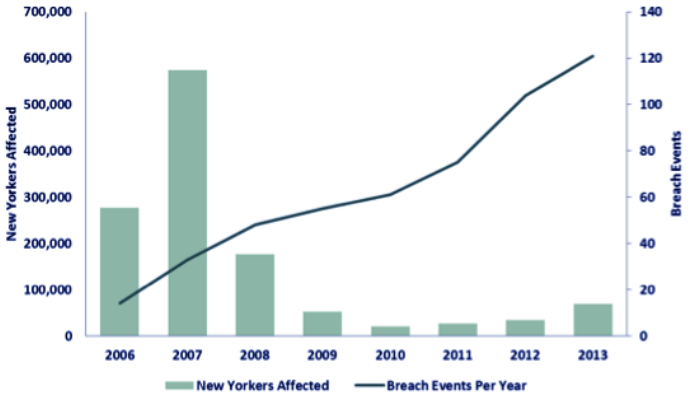


Source: New York State Security Breach Reporting Forms (2006-2013)

Despite increased awareness and prevention efforts, hacking events are likely to continue their meteoric rise. Hackers and the black markets where they exchange tools and information are becoming increasingly sophisticated and specialized.[22] In fact, some security experts believe that hackers actually coordinate to stagger large-scale breach events in order to preserve the scarcity of stolen information, thereby inflating prices for stolen data.[23]

Threats to data security are not always external — instances of insider wrongdoing grew to an all-time high in 2013. Like hacking, insider wrongdoing presents a unique but important challenge to data security, as compromised personal records are often obtained exclusively for fraudulent purposes. As shown in Figure 7 below, instances of insider wrongdoing have steadily increased since 2006 and reached a record high of 121 reported instances in 2013. However, with the exception of 2007, the volume of personal records exposed generally decreased during that time. In 2007, there was a jump in the number of personal records belonging to New Yorkers that were exposed, mainly due to a single event – the Certegy Check Services breach, which accounted for approximately 80 percent (470,696) of New Yorkers' records affected that year.

Figure 7: Insider Wrongdoing Rises But Exposes Fewer Personal Records Since 2006



Source: New York State Security Breach Reporting Forms (2006-2013)

WHO MONITORS THE MONITORS? CERTEGY CHECK SERVICES EXPOSES 470,696 PERSONAL RECORDS

Despite making up only a small portion of insider wrongdoing breach events, credit reporting services exposed more New Yorkers' personal records than any other industry. This fact is troubling, considering that companies are typically encouraged to provide credit monitoring services to customers following a breach event. The Certegy Check Services data security breach event is one particularly nefarious example. Certegy Check Services is a consumer reporting agency that helps retailers determine whether to accept a personal check from consumers at checkout. In 2007, a database analyst stole the personal information of approximately 8.5 million individuals and sold the information to advertising list broker JAM Marketing, which in turn sold the information to a variety of direct marketing firms.[24] Certegy Check Services ultimately paid fines and provided credit monitoring services for those affected by the breach. The database analyst is currently serving 57 months in federal prison for fraud.[25] JAM Marketing, which claimed it was unaware that the information had been stolen, escaped penalty for the breach.

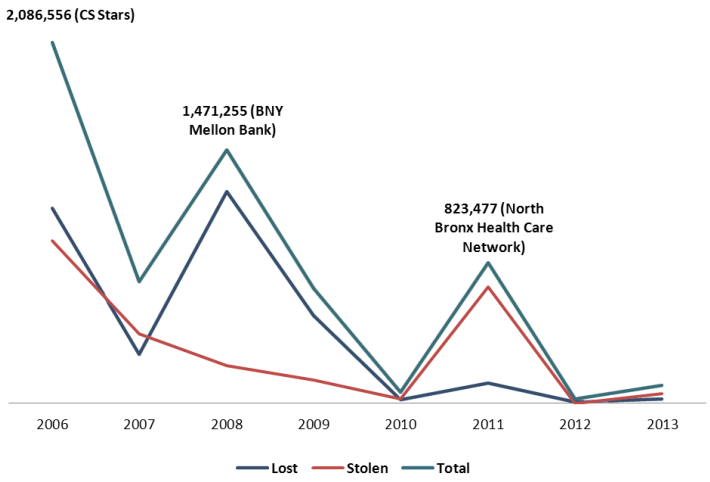
Information Also Exposed Through Preventable Circumstances

The theft or loss of equipment or documentation containing personal information accounted for almost a quarter of total breach events. Laptops and mobile devices can be stolen solely for the value of the electronic equipment, and lost equipment does not always fall into the wrong hands. Reports of stolen/lost equipment peaked at the height of the recession in 2008 and gradually declined before experiencing a recent uptick. Whether personal records were actually disclosed during these events is often unclear. The amount of personal record exposure caused by these types of breaches has been volatile, largely because of a few large events. For example, the spike in 2008, shown in Figure 8 below, is largely attributable to the loss of BNY Mellon's back-up tapes, which exposed 1.2 million personal records of New Yorkers. Overall, the volume of personal records exposed by lost or stolen equipment and documents declined significantly since 2006.

"LOST" VS. "STOLEN" HARDWARE/DOCUMENTATION: BNY MELLON AND NORTH BRONX HEALTH CARE NETWORK (NBHCN)

The BNY Mellon and NBHCN incidents are two large breaches that illustrate the thin line between hardware/information being reported as "stolen" or "lost." In both instances, tape drive storage devices (i.e. "back-up tapes") that were being transported to a storage facility by a third party delivery service disappeared in transit. However, BNY Mellon reported that one tape was "lost," while NBHCN noted that its tapes had been left unattended in an unlocked vehicle for a short duration and were therefore "stolen." In both events, large amounts of highly sensitive and personal information were put at risk, including Social Security numbers, bank account information, and health records.

Figure 8: Lost and Stolen Information/Documentation Declining; Two Events Cause Spikes



Source: New York State Security Breach Reporting Forms (2006-2013)

DATA BREACHES HAVE BILLION-DOLLAR CONSEQUENCES

Data security breaches have significant financial consequences, particularly for the organizations involved. According to a report published by Symantec and the Ponemon Institute in 2013,[26] each personal record compromised during a data breach costs an entity approximately $188. By that estimate, based on NYAG data, breaches cost organizations doing business in New York State over $1.37 billion in 2013 alone.[vi]

Why are the breaches so costly to organizations? After a data breach is discovered, organizations expend significant resources investigating the incident, rectifying security lapses, and notifying those affected, including providing written notice, staffing help centers, and providing free credit monitoring services for affected customers. In certain instances, the organization may also incur sizable legal fees from litigation surrounding the breach. There are also indirect economic consequences associated with a breach. After major breaches that affected millions of customers, both Sony Entertainment and Target experienced a crisis in both consumer and investor confidence. In the year following its 2013 breach, the Target Corporation reported a 46 percent decrease in net earnings and experienced a similarly sharp decrease in stock price.[27] Sony Entertainment experienced a 6 percent stock price decrease and incurred estimated revenue losses of more than $1 billion [28] after approximately 77 million accounts were stolen from its PlayStation Network during a hacking attack in 2011.[29]

Quantifying costs for individual victims of data breaches is more complicated, as not every breach will result directly in financial loss. According to LexisNexis' "True Cost of Fraud" report, approximately 25 percent of victims of data breaches subsequently suffer identity theft.[30] While the Bureau of Justice Statistics found that only 14 percent of those victimized by the identity theft incur out-of-pocket costs,[31] this statistic likely obscures the true costs of identity theft. For example, approximately 30 percent of individuals who experienced the misuse of personal information for fraudulent purposes spent over a month clearing up associated financial and credit problems.[32]

[vi] Calculation: $188 per record x 7,300,222 records exposed = $1,372,441,736.

REDUCE RISK BY TAKING ACTION

Despite the risks posed by data security breaches, individuals and organizations can take practical steps to better protect themselves against threats. While it may be impossible to completely prevent data loss, organizations that implement data security plans can greatly reduce the harm caused by a data security breach. The need for a comprehensive data security plan is not limited to large corporations or those who deal heavily in data. A survey conducted by the Ponemon Institute in 2013 indicated that more than half of U.S. small businesses have experienced at least one data breach.[33] Individuals can also take steps to protect themselves from a breach, and safeguard their personal and financial information if they are the victim of a breach.

Steps For Organizations To Protect Themselves

The NYAG encourages businesses to adopt sound data security practices for all levels of data. When combined with other publicly available data, even seemingly innocuous information can identify individuals and leave them susceptible to identity theft or financial fraud. Sensitive personal information including email addresses, phone numbers, and zip codes, should be protected under the same guidelines as highly sensitive information such as Social Security numbers, credit card numbers, and physical addresses.

The NYAG recommends following these five simple steps to help protect sensitive personal information against unauthorized disclosures.

1. **Understand Where Your Business Stands**

   The first step toward effective data security is to understand what information your business requires for its operation, what data have already been collected and stored, how long the data are needed, and what steps have been taken to ensure security. Organizations should review how sensitive information is acquired, how it is shared with third parties, and what access controls are in place.

2. **Identify and Minimize Data Collection Practices**

   Put simply, data that do not exist cannot be stolen or lost. Collect only information that you need, store it only for the minimum time that you need it, and deploy data minimization tactics wherever possible. For example, if your company uses a point-of-sale system, ensure that expiration dates are not stored with credit card numbers. Reduce the use of highly sensitive data points, such as Social Security numbers, unless absolutely necessary, and minimize the length of retention for such data. Delete any information you no longer need.

3. **Create an Information Security Plan That Includes Encryption**

   Creating a comprehensive Information Security Plan is a complex but necessary endeavor. Studies show that entities with an effective plan will not only articulate technical standards but will also incorporate training, awareness, and detailed procedural steps in the event of data breaches. The plan should:

   - Require a privacy policy that reflects the unique business practices and organizational features of the company or organization. The policy should

use clear language and be made conspicuously available to customers and employees.

- Incorporate procedures restricting access to records and files containing personal information to employees for whom access is essential for their job function. Assign a unique identifier to each employee who has access to the system and require passwords that are reasonably designed to maintain system integrity.

- Frequently monitor systems for unauthorized use or access.
- Implement effective technical safeguards for sensitive personal information:
    - Require encryption of all stored sensitive personal information – including on databases, hard drives, laptops, and portable devices.
    - Minimize storage of sensitive personal information on devices connected to the Internet.
    - Implement hashing and salting of stored user passwords.[vii]
    - Incorporate firewalls and up-to-date security software to protect corporate networks.
    - Ensure that all devices issued to employees require secure authentication to access encrypted sensitive personal information.
- Implement education and training programs for employees on the proper use of computer systems, including accessing and transferring data, and regarding cybersecurity threats such as phishing.
- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to and use of personal information. The traditional "delete" function on a computer is usually not sufficient because a file may continue to exist on a hard drive. A better practice is to use software such as a wipe utility program to permanently erase data from a hard drive, scanners, and other devices.
- Establish an oversight committee or chief data security officer position to ensure implementation and adoption of the plan and periodic review.
- Annually review your organization's data practices for compliance with state and federal laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and various state data security and notification laws.

4. Implement Information Security Plan

Successful implementation of a thoughtfully designed plan can be one of the most effective ways to minimize the risk of a data breach. Elements to consider when implementing a plan include:

- Ensuring employees are trained and aware of the plan.
- Ensuring third parties with whom you might share data are aware of your plan and the procedures it entails.
- Conducting regular audits to ensure compliance with the plan.

[vii] "Hashing" turns passwords into a "fingerprint," allowing the storage of passwords that cannot be read or translated back. It also allows the company to verify that a user's password is correct. "Salting" makes password hashing more secure by adding a random string of characters to passwords before their hash is calculated, which makes them harder to crack.

- Conducting regular reviews of the provisions of the plan to ensure it continues to conform with evolving industry best practices.

Remember to investigate all security incidents immediately and thoroughly. In the event of a breach, the law may require you to notify consumers, law enforcement, state Attorney Generals' offices, credit bureaus, and other businesses.

5. Offer Mitigation Products in the Event of a Breach

While not required by law, New Yorkers affected by a data breach should be provided with mitigation services for free. These include credit monitoring, which provides alerts, usually by email, whenever an application for new credit is submitted to a consumer credit reporting agency, and a security freeze, which blocks new credit accounts. This is especially necessary in breaches that compromise a person's Social Security number or driver's license number, as it allows "new account" fraud — one of the most harmful types of identity theft. The cost of clearing up "new account" identity theft can easily reach into the thousands of dollars and require hundreds of hours attending to administrative burdens.

Steps For Individuals To Protect Themselves

The NYAG suggests that consumers guard against threats in the following ways:

- Create strong passwords for online accounts and update them frequently. Use different passwords for different accounts, especially for websites where you have disseminated sensitive information, such as credit card or Social Security numbers.
- Carefully monitor credit card and debit card statements each month. If you find any abnormal transactions, contact your bank or credit card agency immediately.
- If possible, do not write down or store passwords electronically. If you do, be extremely careful of where you store passwords. Be aware that any passwords stored electronically (such as in a word processing document or cell phone's notepad) can be easily stolen and provide fraudsters with one-stop shopping for all your sensitive information. If you hand-write passwords, do not store them in plain sight.
- Do not post any sensitive information on social media. Information such as birthdays, addresses, and phone numbers can be used by fraudsters to authenticate account information. Practice data minimization techniques. Don't overshare!
- Always be aware of the current threat landscape. Stay up to date on media reports of data security breaches and consumer advisories.

Those who believe they have been victimized by a data security breach must take action. However, the appropriate action will vary depending on the nature of the breach.

1. **User Names and Passwords**
   For user names and passwords, change them immediately on the relevant account, and monitor the account for unusual activity. If you use the same user name or password on other accounts, change those as well.

2. **Credit Card Numbers**
   For breaches involving credit card numbers, Social Security numbers and other sensitive numbers, create an Identity Theft Report by filing a complaint with the Federal Trade Commission and printing your Identity Theft Affidavit. You can call the

Federal Trade Commission (FTC) at 1-877-438-4338 or complete the form online at: http://bit.ly/NYAGDATA. Use the Identity Theft Affidavit to file a police report and create your Identity Theft Report. An Identity Theft Report will help you deal with credit reporting companies, debt collectors, and any fraudulent accounts that the identity thief opened in your name. You may also want to put a fraud alert (a red flag that signals to credit grantors that you may have been a victim of suspicious activity) and/or a security freeze (which prevents your credit file from being reported to third parties) on your credit report by notifying each of the credit reporting agencies (Equifax, TransUnion, or Experian). A security freeze remains on your credit file until you remove it or lift it temporarily when applying for credit services.

CREDIT AGENCY CONTACT INFORMATION

Equifax
1-800-525-6285

Experian
1-888-397-3742

TransUnion
1-800-680-7289

APPENDIX A: METHODOLOGY

Data security breaches between 2005 and 2009 were recorded in Microsoft Word documents, while 2010-2014 breaches were recorded using Microsoft Excel Spreadsheets. After the data were successfully combined into one spreadsheet, a significant amount of "cleaning" was necessary to correct inconsistencies that prevented accurate analysis.

This process also included standardizing breach events into broader categories for analysis, since some notice descriptions were often brief and/or ambiguous. Despite best efforts, some descriptions were simply too ambiguous, and were therefore categorized as "other." Examples of these descriptions include other criminal acts ("extortion,""mail tampering," and "check counterfeiting") and the unexplainable ("files found outdoors" and "student chose user PIN of another"). Breach events that were recorded without any discernable descriptions were categorized as "unknown."

The construction of the "hacking" category included descriptions such as "computer virus" or "malware," as well as "unauthorized intrusion" or "unauthorized access." Based simply on those descriptions, some of the unauthorized access/intrusion categories could have been misclassified.

APPENDIX B: WHAT'S NOT REPORTED

This report is an analysis of the data breach notification reports received by the NYAG over the course of many years, as required by state law. Under New York State law, notification is required only if personally identifying information like a name, in addition to a protected number, like a credit card or Social Security number, is disclosed. Thus, this report does not include any information about the thousands of data breaches that involved disclosure of other sensitive information but did not require notification under law.

For example, in 2011, hackers gained access to data from online shoe and clothing retailer Zappos, owned by Amazon.com. Over 24 million customers' personal details and account information were stolen, including names, email addresses, billing and shipping addresses, the last four digits of credit card numbers, and "cryptographically scrambled" versions of website passwords. The information accessed did not evoke New York's data breach notification laws because it did not include the customers' full credit card or Social Security numbers. Thus, Zappos did not submit a data breach notification form to the NYAG, and the details of this breach are not provided in this report. Zappos did, however, provide direct notice to its customers, including New York residents.

This report also does not provide any information on total consumer losses from data breaches. This information is not required to be disclosed during the notification process and would be collected only if the NYAG conducted a follow-up investigation.

APPENDIX C: NEW YORK DATA SECURITY BREACH NOTIFICATION LAW

In late 2005, New York State Business Law was amended by adding Article 39F Section 899-aa,[34] requiring any person or commercial entity conducting business in New York State, who owns, licenses, maintains, or disseminates as a third party computerized data that includes private information to disclose all breaches of the security of the computerized data system containing private information to the State Police, Department of Consumer Protection, and the Office of the Attorney General. A similar provision, State Technology Law §208, requires state governmental entities to make the same notifications.[35] Breach notification must be made as quickly as possible and without unreasonable delay, consistent with the needs of law enforcement or measures necessary to determine the scope of the breach and/or restore reasonable integrity to the system.

The law also stipulates that entities have a "notification obligation" to any New Yorker whose private information was acquired (or reasonably believed to have been acquired) during the breach. Notification can be made either by mail or phone (email with consent), or if larger in scale (costing over $250,000 to make the notifications), through conspicuous notice such as through the entity's website or via notification of major media outlets. If more than 5,000 New Yorkers were affected, the entity is also required to notify the credit reporting agencies (Equifax, Experian, and TransUnion) as to the timing, content, and distribution of the notices and the approximate number of New Yorkers affected. The Attorney General may bring action if any of the aforementioned articles are not satisfied by the breached entity, and the court may impose fines ranging from $10 to $150,000.

Information for the log is gleaned from the New York State Security Breach Reporting Form, available in PDF form on the NYAG's website. A copy of this form is shown in Appendix D of this report. Entities are also required to submit a copy of the correspondence sent to individuals affected by the breach – from which, at times, additional information is garnered for the logs.

General Business Law §899-aa.
Notification; person without valid authorization has acquired private information.
1. As used in this section, the following terms shall have the following meanings:
(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;
(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:
(1) Social Security number;
(2) driver's license number or non-driver identification card number; or
(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good-faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state Attorney General and furnished upon request to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which conducts business in New York State, and which owns or licenses computerized data which includes private information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Any person or business which maintains computerized data which

includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds $500,000, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article, he may bring an action in the name and on behalf of the people of the State of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action, the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including

consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $10 per instance of failed
notification, provided that the latter amount shall not exceed $150,000.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state Attorney General, the Department of State and the Division of State Police as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

APPENDIX D: NEW YORK STATE SECURITY BREACH REPORTING FORM

NEW YORK STATE SECURITY BREACH REPORTING FORM

Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
_____
Street Address: _____
City: _____ State: _____ Zip Code: _____

Submitted by: _____ Title: _____ Dated: _____
Firm Name (if other than entity): _____
Telephone: _____ Email: _____
Relationship to Entity whose information was compromised: _____

Type of Organization (please select one): [ ] Governmental Entity in New York State; [ ] Other Governmental Entity; [ ] Educational; [ ]Health Care; [ ]Financial Services; [ ]Other Commercial; or [ ]Not-for-profit.

Number of Persons Affected:
Total (Including NYS residents):_____ NYS Residents:_____
If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [ ] Yes [ ] No

Dates: Breach Occurred:_____ Breach Discovered:_____ Consumer Notification:_____

Description of Breach (please select all that apply):
[ ]Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[ ]Internal system breach; [ ]Insider wrongdoing; [ ]External system breach (e.g., hacking);
[ ]Inadvertent disclosure ; [ ]Other specify): _____

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[ ]Social Security Number
[ ]Driver's license number or non-driver identification card number
[ ]Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:
[ ] Written [ ] Electronic [ ] Telephone [ ] Substitute notice
List dates of any previous (within 12 months) breach notifications: _____

Identify Theft Protection Service Offered: [ ]Yes [ ] No
Duration: _____ Provider: _____
Brief Description of Service: _____

ENDNOTES

1. Podesta, John , John Holdren, Penny Pritzker, Ernest Moniz, and Jeffrey Zients, "Big Data: Seizing Opportunities, Preserving Values," The White House, 1 May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
2. Madden, Mary, "More online Americans say they've experienced a personal data breach," Pew Research Center, 14 April 2014, http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/.
3. "2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters," Javelin Strategy & Research, 2013, https://www.javelinstrategy.com/brochure/276#DownloadReport.
4. "2013 LexisNexis True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud," LexisNexis, September 2013, http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf.
5. Harrell, Erika, and Lynn Langton, "Victims of Identity Theft, 2012," U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, December 2013, http://www.bjs.gov/content/pub/pdf/vit12.pdf.
6. Krebs, Brian, "A First Look at the Target Intrusion, Malware," Krebs on Security, 15 January 2014, http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/.
7. Finkle, Jim, and Mark Hosenball, "Exclusive: More well-known U.S. retailers victims of cyber attack-sources," Reuters, 12 January 2014, http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112.
8. "2014 Data Breach Investigations Report," Verizon Enterprise Solutions, 2014, http://www.verizonenterprise.com/DBIR/2014/.
9. Krebs, Brian, "Heartland Payment Systems," Krebs on Security, 2013-2014, http://krebsonsecurity.com/tag/heartland-payment-systems/.
10. Vijayan, Jaikumar, "TJX data breach: At 45.6M card numbers, it's the biggest ever," Computerworld, 29 March 2007, sec. News, http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever.
11. Perlroth, Nicole, "Russian Arrested in Guam on Array of U.S. Hacking Charges," New York Times , 7 July 2014, sec. Security, http://bits.blogs.nytimes.com/2014/07/07/russian-arrested-in-guam-on-array-of-u-s-hacking-charges/?_php=true&_type=blogs&_r=0charges/?_php=true&_type=blogs&_r=0.
12. Ablon, Lillian, Martin Libicki, and Andrea Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/ RR600/RR610/RAND_RR610.pdf.
13. Ibid.
14. Callahan, Michael, "Why Your Twitter Account May Be More Valuable Than Your Credit Card," Juniper Networks, 24 March 2014, http://forums.juniper.net/t5/Security-Mobility-Now/Why-Your-Twitter-Account-May-Be-More-Valuable-Than-Your-Credit/ba-p/234270.
15. Ablon, Lillian, Martin Libicki, and Andrea Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/ RR600/RR610/RAND_RR610.pdf.
16. "Mobile devices are a leading data breach threat," Risk Management and Safety Eline, 3 April 2014, http://www.associatedfinancialgroup.com/Data/eLineNewsletters/RiskManagement/Vol13/No4apr14/riskartApr14.asp.
17. Kassner, Michael, "Convenience or security: You can't have both when it comes to Wi-Fi," TechRepublic, 24 June 2013, http://www.techrepublic.com/blog/it-security/convenience-or-security-you-cant-have-both-when-it-comes-to-wi-fi/.
18. Constantin, Lucian. "Security analysis of mobile banking apps reveals significant weaknesses," Computerworld, 9 January 2014, sec. News, http://www.computerworld.com/s/article/9245298/Security_analysis_of_mobile_banking_apps_reveals_significant_weaknesses.
19. "2014 Data Breach Investigations Report," Verizon Enterprise Solutions, 2014, http://www.verizonenterprise.com/DBIR/2014/.
20. Ablon, Lillian, Martin Libicki, and Andrea Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/

rand/pubs/research_reports/ RR600/RR610/RAND_RR610.pdf.

21. "2014 Data Breach Investigations Report," Verizon Enterprise Solutions, 2014, http://www.verizonenterprise.com/DBIR/2014/.
22. Ablon, Lillian, Martin Libicki, and Andrea Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/ RR600/RR610/RAND_RR610.pdf.
23. Ibid.
24. Abramovich, Giselle, "Certegy's ID breach lost 8.5 million names," Direct Marketing News, 8 August 2007, sec. Miscellaneous, http://www.dmnews.com/certegys-id-breach-lost-85-million-names/article/98116/.
25. McGlasson, Linda, "Certegy Reaches Data Breach Settlement," Bank Info Security, 20 April 2010, sec. Articles, http://www.bankinfosecurity.com/certegy-reaches-data-breach-settlement-a-2441.
26. 2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.
27. Harris, Elizabeth, "Data Breach Hurts Profit at Target," New York Times, 26 February 2014, sec. Business Day, http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html.
28. Osawa, Juro, "As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill," Wall Street Journal, 9 May 2011, sec. Asia Technology, http://online.wsj.com/news/articles/SB10001424052748703859304576307664174667924.
29. Sherr, Ian and Nick Wingfield, "Play by Play: Sony's Struggles on Breach," Wall Street Journal, 7 May 2011, sec. Technology, http://online.wsj.com/news/articles/SB10001424052748704810504576307322759299038.
30. "2013 LexisNexis True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud," LexisNexis, September 2013, http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf.
31. Harrell, Erika, and Lynn Langton, "Victims of Identity Theft, 2012," U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, December 2013, http://www.bjs.gov/content/pub/pdf/vit12.pdf.
32. Ibid.
33. Munich RE, "Survey Shows Small Businesses Have Big Data Breach Exposure," Hartford Steam Boiler and Ponemon Institute, 6 March 2013, http://www.hsb.com/HSBGroup/Subpage.aspx?id=579.
34. New York State General Business § 899-aa. Available: http://public.leginfo.state.ny.us/
35. New York State Technology Law § 208. Available: http://public.leginfo.state.ny.us/
36. NYS Division of Homeland Security. "New York State Security Breach Reporting Form." 17 June 2013, http://www.dhses.ny.gov/ocs/breach-notification/documents/State-Data-Breach-Form.pdf.