INFORMATION EXPOSED

2017 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: 2017 Data Breaches in New York State," analyzes the data breach notices my office received in 2017. In all, companies and other entities reported a record-high 1,583 breaches to my office in 2017. The breaches exposed the personal records of 163 million individuals in the U.S., including 9.2 million New Yorkers. The reported data breaches in 2017 represent the greatest exposure rate of New Yorkers' personal information since the NYAG started receiving data breach notices in 2006.

New York State's current data security law has proven inadequate to address the ever-growing threat of data breaches. New York law only requires a person or commercial entity conducting business in New York State to report a data security breach if it involves "private information," defined as a consumer's name in combination with a social security number, financial account information, or driver's license number.

However, current law does not require most companies to maintain reasonable data security, except if the company collects social security numbers. Companies also are not required to report breaches of certain critical data types, including username-and-password combinations, and biometric data like the fingerprint you use to unlock an iPhone.

To address these inadequacies in the law, my office introduced the Stop Hacks and Improve Electronic Data security, or SHIELD Act, which would require companies to adopt administrative, technical, and physical safeguards for sensitive data. These standards would apply to any business that holds sensitive data of New Yorkers, whether they do business in New York or not.

The standards are tailored to the sensitivity of the data retained and the size and complexity of the business. The SHIELD Act also expands the types of data that trigger reporting requirements in the event of exposure to include username-and-password combinations, biometric data, and HIPAA-covered health data.

My office is also preparing new legislation that would require companies like Facebook to notify my office, and in turn consumers, as soon as they learn that their users' personal data has been misused.

As information increasingly drives commerce and government, the challenges presented by data security breaches will continue to grow. Data security laws must keep pace with emerging data security threats. However, organizations can also do more to prevent breaches 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.

My office will continue to engage industry stakeholders and security experts, as well as lawmakers, in order to make New York's data security laws a model for the nation. 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

2017 Data Breaches Reported to the New York Attorney General's Office

In 2017, companies and other entities reported a record-breaking 1,583 breaches to the New York State Office of the Attorney General ("NYAG"). The breaches exposed the personal records of 9.2 million New Yorkers.

The information exposed consisted overwhelmingly of social security numbers, accounting for 40% of records exposed, followed by financial account information (such as credit card numbers), accounting for 33% of records exposed. Hacking was the leading cause of the data security breaches at 44%, with 25% of breaches due to negligence. In 2017, we saw an increase of more than 23% in the total number of reported security breaches affecting New York residents from the previous year, and the number of New Yorkers who had their records exposed more than quadrupled from 2016, increasing by 7,691,025. In 2017, the exposure rate of New Yorkers' personal information was the highest since the NYAG started receiving data breach notices in 2006.

General Business Law § 899-aa

In 2005, General Business Law § 899-aa was added to New York State Business Law requiring any person or commercial entity conducting business in New York State to report a data security breach involving "private information" to the NYAG, among other state agencies. State Technology Law § 208 also requires state governmental entities to report breaches of private information. "Private information" is defined as including a consumer's name in combination with a social security number, financial account information, or driver's license number. The reports must be timely and done without unreasonable delay.

In 2017, hacking accounted for over 44% of data security breaches, up from 40% in the previous year. It accounted for 94% of the total personal information exposed, largely as a result of the mega-breach at consumer reporting agency Equifax. (See Figures 1 and 2.) Employee negligence, which consists of a combination of inadvertent exposure of records, insider wrongdoing, and the loss of a device or media, accounted for 25% of reported breaches.

IN FOCUS: 25% OF ALL DATA SECURITY BREACHES WERE CAUSED BY HUMAN ERROR – EMPLOYEE BEHAVIOR THAT CAN BE RECTIFIED WITH MORE TRAINING AND VIGILANCE. IT IS CRITICAL THAT — MOVING FORWARD — COMPANIES PUT IN PLACE POLICIES AND PROCEDURES TO PREVENT NEGLIENCE WHEN PROTECTING CONSUMER DATA.

Figure 1: Data Security Breach Cause (Chart)

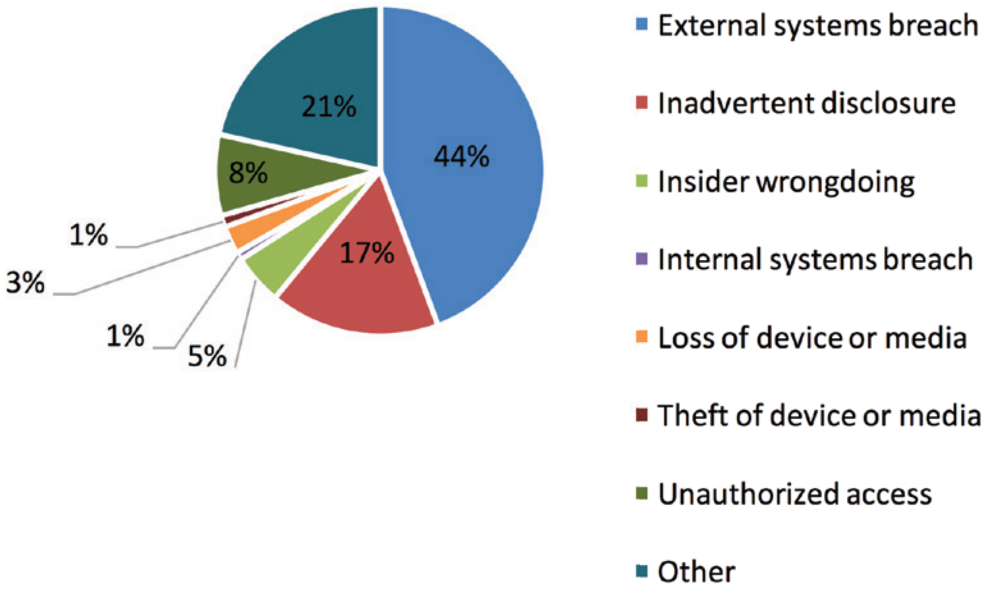

Figure 2: Data Security Breach Cause (Table)

Data Security Breach Cause	Number of Breaches (% of Total)	Personal Records Exposed in NY (% of Total)	Personal Records Exposed in US (% of Total)
External systems breach	699 (44%)	8,783,104 (94%)	153,732,117 (94%)
Inadvertent disclosure	263 (17%)	69,319 (<1%)	500,297 (<1%)
Other (e.g. skimming)	339 (21%)	236,742 (2.5%)	4,437,622 (3%)
Insider wrongdoing	78 (5%)	10,428 (<1%)	274,565 (<1%)
Loss of device or media	43 (3%)	8,761 (<1%)	62,774 (<1%)
Theft of device or media	18 (1%)	16,248 (<1%)	2,330,403 (1.4%)
Unauthorized access	125 (8%)	86,705 (<1%)	137,366 (<1%)
Internal systems breach	12 (<1%)	225,158 (2%)	225,158 (<1%)
Unknown	5 (<1%)	139 (<1%)	1,605,312 (1%)
Total	**1583**	**9,286,604**	**163,305,614**

Social Security Numbers and Financial Account Information are Hackers' Primary Targets

Social security numbers and financial account information represented the information most frequently exposed in 2017, accounting together for 73% of breaches. Social security numbers were exposed in 40% of reported breaches and financial account information accounted for 33% of total breaches in 2017. (See Figures 3 and 4.) While the percentages for the other categories of exposed information are not as high, some still account for a sizable percentage of total personal records exposed; for instance, driver's license numbers figured in 9% of reported breaches. (See Figure 4.)

Figure 3: Type of Information Acquired (Chart)

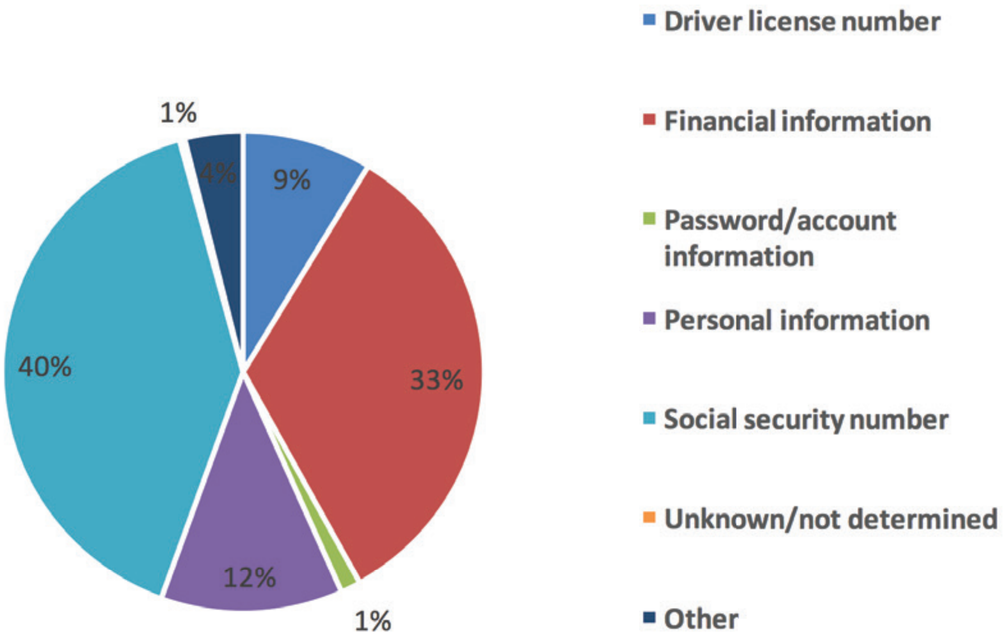

Figure 4: Type of Information Acquired (Table)

Type of Information Acquired	Number of Breaches (% of Total)	Personal Records Exposed in NY (% of Total)
Social Security number	926 (40%)	7,787,820 (29%)
Financial information	766 (33%)	8,233,552 (31%)
Driver license number	200 (9%)	4,154,827 (15%)
Personal information	281 (12%)	1,894,452 (7%)
Password/account information	31 (1%)	284461 (1%)
Unknown/not determined	8 (<1%)	1166 (<1%)
Other	90 (4%)	4,587,332 (17%)
Total	**1583 (2302 including overlapping)**	**9,286,604 (26,943,610 including overlapping)**

Two Mega-breaches in 2017

IN FOCUS: IN MAY-JULY 2017, HACKERS INFILTRATED EQUIFAX SERVERS AND STOLE THE PERSONAL INFORMATION, INCLUDING SOCIAL SECURITY NUMBERS, OF NEARLY HALF THE COUNTRY'S POPULATION (145 MILLION NATIONWIDE AND 8.4 MILLION IN NY ALONE). THIS REPRESENTED ONE OF THE LARGEST BREACHES OF CONSUMER PERSONAL INFORMATION IN U.S. HISTORY AND IS ATTRIBUTABLE TO HUMAN ERROR. THE BREACH SHATTERED THE PUBLIC'S TRUST IN EQUIFAX AND OTHER CREDIT REPORTING AGENCIES. EQUIFAX'S STOCK PRICE DROPPED OVER 33% AND A NUMBER OF EQUIFAX EMPLOYEES LOST THEIR JOBS, INCLUDING THE C.E.O. EQUIFAX FACES A NUMBER OF CLASS ACTIONS AND INVESTIGATIONS BY LOCAL, STATE, AND FEDERAL OFFICIALS INCLUDING THE NYAG.

There were two mega-breaches (a breach that affects over 100,000 New Yorkers) in 2017. Most notably, the breach at consumer reporting agency Equifax, which compromised the social security numbers of over 145 million people in the United States, including 8,447,840 in New York. Intruders accessed the Equifax computer system after the company failed to patch a known vulnerability in its web application software. The next most voluminous breach was at Gamestop, discovered by the company on April 18, 2017, in which over 111,000 New Yorkers had their financial information exposed to hackers.

Additionally, over 30,000 New Yorkers had their financial information exposed after large breaches at the Online Traffic School, Polish & Slavic Federal Credit Union, InterContinental Hotels Group, and Spiraledge, Inc. Eleven more breaches that compromised between 10,000 and 30,000 New Yorker's personal information were reported in 2017. Following those, the most common breaches compromised relatively fewer numbers of New Yorkers' personal information.

Figure 5: Total Number of Breaches and NY Residents Affected by Range of 2017 Reported Breaches (Table)

Range of Total NY Residents Affected	Total # of Breaches
1-9	781
10-99	418
100-499	198
500-999	55
1000-4999	84
5000-10000	15
10000-25000	11
25,000-100,000	5
100,000+	2
Unknown	14
Total	**1583**

More Breach Events Affect a Small Number of Consumers Rather than a Large Number of Consumers

In 2017, the majority of breaches affected "only" one to nine people per breach, with about two-thirds of breaches affecting under 100 people per breach. Compared to 2016, in 2017 there were 55 more breaches that affected just one personal record and 83 more that affected between two and ten personal records. Thus, while the record number of records exposed in 2017 was a result of one large mega-breach at a multinational company (i.e., Equifax), it is clear that breaches come in all sizes, and no organization is exempt from the risk of a data breach.

This Report Echoes Trends Identified in Prior Reports

In 2016, NYAG reported a record 1,281 data breaches notices, representing a 60%increase over the 2015 reporting year. The 2016 breaches exposed the personal records of 1.6 million New Yorkers, representing a threefold increase over the prior year. The 2017 shattered those records. There were also a higher number of breaches affecting smaller amounts of people than in 2016. In 2014, NYAG issued a comprehensive report entitled, "Information Exposed: Historical Examination of Data Security in New York State." The 2014 report analyzed the data breach reports the office received between 2006 to 2013 and how they impacted New Yorkers.

The Attorney General's Office recommends that organizations follow these simple steps to help protect sensitive personal information against unauthorized disclosures:

- **Understand Where Your Business Stands:** The first step toward an effective data security policy is to understand what information your business requires for its operation, what data has already been collected and stored, how long the data is needed, and what steps have been taken to ensure security. Organizations should review how sensitive data is acquired, how sensitive information is being shared with third parties, and what access controls are in place.
- **Identify and Minimize Data Collection Practices:** Put simply, data that does 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.
- **Create an Information Security Plan That Includes Encryption:** Creating a comprehensive Information Security Plan is a necessary endeavor. Studies show that entities with an effective plan will articulate not only technical standards, but will incorporate training, awareness, and detailed procedural steps in the event of data breaches. Encryption of sensitive information should be an element of any plan. Read more about what a comprehensive security plan should include in NYAG's 2014 report.
- **Implement an 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 aware of the plan and conducting regular reviews to ensure the plan continues to conform with evolving best practices.
- **Take Immediate Action in the Event of a Breach:** 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 Attorneys General, credit bureaus, and other businesses.
- **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 whenever an application for new credit is submitted to a consumer credit reporting agency, and a security freeze, which blocks new credit accounts. The cost of clearing up the consequences of identity theft can easily reach into the thousands of dollars and require hundreds of hours attending to administrative burdens.

The Attorney General's Office 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.
- **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.

The Attorney General's Office recommends taking the following steps if you believe you have been victimized by a data security breach:

- **User Names and Passwords:** Change user names and passwords 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.
- **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 at 1-877-438-4338 or complete the form online here. 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 and/or security freeze on your credit report by notifying each of the credit reporting agencies (Equifax, TransUnion, and Experian). A security freeze is the strongest protection for your credit and remains on your credit file until you remove it or choose to lift it temporarily when applying for credit services.

Contact information for the credit reporting agencies:

Equifax 1-800-525-6285

Experian 1-888-397-3742

TransUnion 1-800-680-7289

STATE OF NEW YORK

EXCELSIOR

ATTORNEY GENERAL