Español

A.G. Schneiderman Announces Record Number Of Data Breach Notices For 2017

Hacking Continues to Drive the Explosion of Data Breaches; 2017 Saw Exposure of Personal Records of 9.2 Million New Yorkers – Quadruple the 2016 Number

AG Schneiderman to Introduce Legislation to Require Companies like Facebook to Provide Notification if Users' Personal Info is Misused; AG Also Calls on Albany to Pass His SHIELD Act

AG Offers Tips for NY Consumers and Businesses to Protect Themselves

NEW YORK – Attorney General Eric T. Schneiderman today released "Information Exposed: 2017 Data Breaches in New York State," documenting the record number of data breach notices filed with his office in 2017. In 2017, companies and other entities reported 1,583 data breaches to NYAG, exposing the personal records of 9.2 million New Yorkers – quadruple the number of New Yorkers impacted in 2016.

Attorney General Schneiderman announced that he would introduce legislation to require Facebook and other social media sites to notify his office and New York consumers when they learn that users' personal data was obtained and misused in violation of the law or the platform's terms of service.

Attorney General Schneiderman also urged the State legislature to pass his Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which was introduced by Attorney General Schneiderman last fall and would close major gaps in New York's data security laws. Under the SHIELD Act, companies would have a legal responsibility to adopt "reasonable" administrative, technical, and physical safeguards for sensitive data; the bill also would expand the types of data that trigger reporting requirements.

"Data breaches can cause personal crises for New Yorkers every time they happen – driving down credit scores and destroying financial lives," said **Attorney General Schneiderman**. "We saw a record number of data breaches in 2017, jeopardizing the personal information of 9.2 million New Yorkers. My office will continue to hold companies accountable for protecting the personal information they manage – but it's also time for Albany to bring our laws into the 21st century and ensure that New Yorkers are not needlessly victimized by weak data security and criminal hackers."

As detailed in today's report, New Yorkers' exposed information consisted overwhelmingly of social security numbers, accounting for 40% 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 another 25% of breaches due to negligence. 2017 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, largely due to the Equifax breach. In 2017, the exposure rate of New Yorkers' personal information was the highest since 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 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.

Hacking & Negligence Continue As Main Causes of Data Breaches

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.

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.)

Two Mega-breaches in 2017

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 Yorkers' personal information were reported in 2017. Following those, the most common breaches compromised relatively fewer numbers of New Yorkers' personal information.

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 breaches 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.

"The number of data breach notices the Attorney General received last year confirms that New Yorkers are at risk. It is clear that we must update our data security laws to protect people's personal information. As the Chair of the Senate Consumer Protection Committee, I want to thank Attorney General Schneiderman for educating the public about this important issue, and we will continue to advocate for legislation that keeps New Yorkers safe from data breaches," said **State Senator David Carlucci**.

"The massive data breaches which impacted more than half of all adult New Yorkers last year alone serve as an ongoing reminder that any of us could become a victim of identity theft at any time," said **Laura J. Ehrich, Associate State Director, AARP New York.** "AARP applauds Attorney General Schneiderman for continuing to push his proactive SHIELD ACT legislation to protect our personal information from would-be thieves who could literally ruin our lives. We thank Senator Carlucci and Assemblyman Titone for sponsoring this bill. Now as always, we urge everyone to take advantage of AARP's Fraud Watch Network for practical information and tips on how to protect yourself."

"In these times of ever increasing reports of data breaches and identity theft, it is even more important to be vigilant with your own personal information and take steps to safeguard your identity," said **Lynette**

Baker, Director of Outreach & Marketing, Consumer Credit Counseling Services of Rochester.

Attorney General's Press Office: (212) 416-8060

nyag.pressoffice@ag.ny.gov

Press Release Archive

- September 2018
- August 2018
- July 2018
- June 2018
- May 2018
- April 2018
- March 2018
- February 2018
- January 2018
- December 2017
- November 2017
- October 2017

VIEW ALL PRESS RELEASE ARCHIVES

Please enter a search term...