LANTERN
BY LABATON

CONSUMER ALERT

WHAT TO DO IF YOU'VE BEEN INVOLVED IN A DATA BREACH

Nowadays, it seems like data breaches happen so frequently that you can hardly keep up. Nearly every week you see headlines about another large company suffering yet another major data breach. As our lives become increasingly reliant on technology, we become more susceptible to having our sensitive personal information exposed. We provide information to companies every day and do not know if the company is improperly securing or storing the data.

When planning a data breach, hackers target specific types of companies. Some types of breaches are:

- Medical Facilities: These breaches can expose your health insurance or Medicare information, insurance policy numbers, treatment history, and prescription information. In certain circumstances your billing information can be exposed, including your credit card or Social Security card numbers.

- Financial Institutions: Breaches of financial institutions like banks are some of the most severe. Often, your bank has your most sensitive financial information. These breaches can expose your banking information, credit card or debit card numbers, and bank account numbers. They can also expose personal information like your name, address, date of birth, email, and Social Security Number.

- Utilities: There is a growing trend of hackers targeting utilities like your cell phone, cable, or internet provider. These breaches can expose financial information like your credit card or debit card number and payment history or personal information like your name, address, email address, passwords, and Social Security numbers. Some of the large wireless companies have been victims of a data breach.

- Educational Institutions: Institutions like schools and colleges are a popular target among hackers. These entities collect personal information like names, birth dates, addresses, ID numbers, Social Security numbers and bank information.

Thus, it is important to know what to do if you believe you were involved in a data breach.

1. Confirm the Breach Occurred: If you believe you were involved in a data breach, you should first confirm there was a data breach. A common tactic by hackers is to send emails to consumers posing as a company you have an account with saying there has been a data breach. Typically, the hacker's email will prompt you to click a link. If you receive any suspicious emails, don't click the links. Instead, contact the company directly or search for news stories on the internet to confirm the breach. In addition, companies are required to report data breaches to certain State Attorneys General offices. You can sometimes view a list of the data breaches on their website.

2. Determine the Type of Breach: You should determine the type of breach that occurred and what information was likely targeted by hackers. For example, if your cell phone

provider was hacked, it is unlikely that your medical information was exposed. However, if your hospital was breached, it is reasonable to assume that your medical information is at risk.

3. **Reset Your Passwords**: You should change the passwords for all your online accounts. Most people use the same or similar passwords for all their online accounts. So, if one password was exposed, there is a chance a hacker could gain access to all your online accounts.

4. **Monitor Your Accounts**: After your reset your passwords, it is important to monitor your online accounts for any suspicious activity. Be on the look out for strange charges that you do not recognize or any phishing emails.

5. **See if You Have a Claim**: Many companies simply have inadequate data security measures in place to protect their users' sensitive personal information, giving rise to legal claims against the company. Further, some states, like California, have data security laws that allow certain consumers that had certain categories of information exposed to recover either their actual damages or a minimum statutory penalty. If you believe you were involved in a data breach, you should retain copies of suspicious emails, records of fraudulent charges, or file an identity theft report, which will be helpful in proving your claim.

Labaton Sucharow's lawyers are available to address any questions you may have regarding these developments. Please contact the Labaton Sucharow lawyer with whom you usually work or the contacts below.

Jonathan Gardner:
jgardner@labaton.com / 212.907.0839

Melissa H. Nafash:
mnafash@labaton.com / 212.907.0861

Jonathan Waisnor:
jwaisnor@labaton.com / 212.907.0623

Brandon Heitmann:
bheitmann@labaton.com / 212.907.0673