Office of the New York State Attorney General Letitia James

Protecting consumers' personal information

Tips for businesses to keep data safe and secure

April 19, 2023

Message from the New York State Attorney General

In today's digital age, so much of New Yorkers' personal information is stored online, and all too often companies do not take the necessary measures to protect it. Last year, the Office of the New York State Attorney General (OAG) received 4,000 data breach notifications, in which we were informed that consumers' personal information may have been compromised. We reviewed every notification, opened dozens of investigations, and penalized companies millions of dollars for their failure to adopt reasonable safeguards to protect customer information or properly inform customers of the incident.

Businesses can and must do better to protect New Yorkers' digital data. New Yorkers should not have to worry that their information may end up in the wrong hands the next time they make an online purchase, book a trip, sign up for a class, or just browse the internet. If organizations take relatively simple steps to secure their systems, we can turn the corner on the data breach trend.

This guide[1] is intended to help companies strengthen their data security and protect New Yorkers' digital data. We know that most businesses want to do the right thing, and we want to share what we have learned from our experience investigating and prosecuting businesses following cyber security breaches. We also want to put companies on notice that they must take their data security obligations seriously, and at a minimum, take the reasonable steps outlined in this report.

I hope the tips offered in this report help organizations strengthen their online security to keep New Yorkers safe. By coordinating with industry leaders, experts, consumer advocates, and regulators, New York is continuing its commitment to a stronger, more secure technological future for every New Yorker.

Sincerely,
Letitia James
New York State Attorney General

[1] This report is for informational purposes only and should not be construed as a statement of the law, legal advice or as policy of the state of New York. The document may be copied, provided that (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the New York State Attorney General, and (3) all copies are distributed free of charge.

OAG data security recommendations

Under New York law, businesses must use reasonable safeguards to protect New Yorkers' personal information. When it appears that a business has failed to do so, OAG will investigate and, if appropriate, take action. This report highlights findings from several of OAG's recent investigations and offers straightforward guidance that can help businesses strengthen their data security programs and better protect consumer information.

1. Maintain controls for secure authentication

If your business stores customer information, strong authentication procedures can help ensure that only authorized individuals can access the data. Your company's policies and procedures should:

a. Use a secure method of authentication

For many password-protected systems, a stolen password may be all that is needed for a cybercriminal to gain access to confidential and sensitive information. Unfortunately, cybercriminals have developed myriad ways of getting their hands on passwords. Thus, in many cases, password-based authentication on its own is not a secure mechanism for authenticating users. Businesses should use a more secure alternative, such as multi-factor authentication, especially for administrative or remote access accounts. Importantly, this applies to internal employee accounts as well as customer accounts.

Two recent cyberattacks OAG investigated illustrate the risks of authenticating using passwords alone. In 2022, we announced a settlement with EyeMed after attackers gained access to a corporate email account containing sensitive customer data. EyeMed had failed to require multi-factor authentication at login, which could have thwarted the attacker's attempts to access the account. The intrusion granted the attacker access to emails and attachments dating back six years, including consumers' names, addresses, Social Security numbers, and insurance account numbers.

Similarly, in 2022, we announced a settlement with Carnival Cruise following an attacker's unauthorized access of Carnival employee email accounts. The breach exposed sensitive customer and employee information, including passport numbers, driver's license numbers, payment card information, health information, and social security numbers. Note that consumer notice was particularly difficult in these cases because the businesses lacked visibility into this data that was stored in email over many years, causing months of delay.

b. Require lengthy and secure passwords

The difficulty in keeping track of multiple passwords leads people to use easy-to-remember passwords and use them over and over again. Perhaps unsurprisingly, the most common password is: password. The second most common: 123456. Remember every additional character makes a password much more difficult to crack. And adding symbols and numbers make it that much more difficult. If a given computer could crack the six-character password in one second, it would take more than two million years to crack a 12-character password.[2] The Carnival breach likely involved automated password guessing called a brute force attack.

Further, in addition to imposing password complexity requirements, which may result in users simply adding a number or special character to the end of an easily guessed password (like Password1 or Password!), businesses should consider comparing user-chosen passwords against breached password databases and prohibiting the use of context-specific passwords, such as the name of the user/company or date of birth.

c. Secure passwords against attack

It is critical to secure passwords against attack. In most cases this requires "hashing," a process that turns passwords into a string of letters and/or numbers so that they cannot be read or used if they fall into the wrong hands. Businesses should use a method of hashing that is not susceptible to password cracking attempts. This typically requires both the selection of an appropriate hashing algorithm, and the use of additional random characters, sometimes called "salt."

Our office has repeatedly taken action against businesses that failed to secure their customers' passwords. For example, OAG recently secured a settlement with Wegmans after an investigation uncovered that the company had been using an outdated hashing method on some customer passwords, including a hashing algorithm that could easily be subverted.

[2] Jean-Paul Delahaye, *The Mathematics of Hacking*, Scientific American, April 12, 2019, https://www.scientificamerican.com/article/the-mathematics-of-hacking-passwords (last accessed March 4, 2023)

2. Encrypt sensitive customer information

With cyber threats continually evolving, no safeguard can be 100 percent effective. That is why it is crucial that businesses not only defend against unauthorized access, but also put controls in place in case those defenses fail. For most businesses that handle sensitive customer information, those controls should include encryption, a process of scrambling information that can only be reversed using a secret key, called the decryption key.

In our recent CafePress case, we found that a popular online marketplace had failed to securely encrypt buyer and seller information, including the social security numbers and tax identification numbers associated with more than 180,000 seller accounts, which were left in plain text. A cybercriminal that gained access to the company's system was able to steal this information and ultimately offered it for sale on the dark web. Had the information been encrypted, it would have been protected even in the hands of a cybercriminal.

3. Ensure service providers use reasonable security measures

Businesses that entrust customer information to their service providers are responsible for ensuring those service providers use appropriate security measures to protect that information. Failing to do so can put customer information at risk. In 2022, we settled with T-Mobile following a breach in which an unauthorized actor gained access to customer information stored on its vendor's network. The information that was accessed included names, addresses, dates of birth, Social Security numbers, identification numbers (such as driver's license and passport numbers), and related information used in T-Mobile's own credit assessments.

In the settlement with OAG, T-Mobile agreed to detailed vendor management provisions designed to strengthen its vendor oversight going forward. Those include maintenance of a T-Mobile vendor contract inventory, including vendor risk ratings based on the nature and type of information that the vendor receives or maintains; imposition of contractual data security requirements on T-Mobile's vendors and sub-vendors; establishment of vendor assessment and monitoring mechanisms; and appropriate action in response to vendor non-compliance, including contract termination.

Businesses that rely on service providers should take reasonable steps to ensure their providers implement appropriate security measures, including those described in this report. In most cases, this would include diligence in selecting service providers with appropriate data security programs, building security expectations into contracts with service providers, and monitoring the service providers' work to ensure compliance.

4. Know where you keep consumer information

A business cannot properly protect customer information if it does not know where that information is kept. Our Wegmans case highlights the dangers of losing track of customer data. In that matter, a security researcher contacted the grocery retailer after discovering that one of the company's cloud storage containers was configured to allow public access to its contents. The container included database backup files with the information of over three million customers. When the security researcher contacted the company, the company's security personnel were unaware that the old backup files were even stored in that location.

The company could have avoided this incident altogether if it had maintained an inventory of assets that contained customer information. With an asset inventory, it would have known those cloud containers had files with customer information and therefore could have conducted appropriate security testing, which may have identified the misconfiguration sooner.

With personnel turnover and changing practices over time, it's crucial to maintain an asset inventory that tracks where personal information is kept so that it can be appropriately secured. Maintaining the security of an asset inventory is also very important.

5. Guard against data leakage in web applications

Sensitive information should never be disclosed through a website or app without appropriate authentication. In many cases, it's not necessary – or appropriate – to disclose such information at all. Instead, sensitive information should typically be masked, for example by sending only the last four digits of a credit card number. Businesses should audit their web applications to ensure that sensitive data is only transmitted in unmasked form when appropriate.

6. Protect customer accounts impacted in data security incidents

Successful cyberattacks may not only grant attackers access to customer information – in certain cases, they can give attackers access to customers' online accounts as well. When an attacker has compromised the security of a customer's account – for example, by stealing customer login credentials or breaking into the account – businesses should take action to secure the account and protect the customer from further harm.

We recently took action against a business that failed to protect customer accounts that had been impacted in a data security incident. In 2018, attackers infiltrated Zoetop's systems and stole a variety of customer information, including the login credentials to tens of millions of SHEIN customer accounts. For the vast majority of these accounts, however, Zoetop failed to take any steps to protect its customers, for example by resetting account passwords or alerting customers that their accounts were at risk. Following an investigation, the OAG secured a settlement that required the company to adopt enhanced incident response policies.

When customer login credentials or accounts have been, or are reasonably likely to have been, compromised, there are several steps a business should take. First, it should act quickly to block attackers' access to the accounts. In most cases, this requires immediately resetting the passwords of the accounts that were likely impacted in the attacks. In some cases, it may also be appropriate to take additional steps, like freezing the relevant accounts. Second, in most cases, the business should quickly notify impacted customers. Notice enables customers to take steps to protect themselves, for example by reviewing their online accounts or financial statements for fraud and securing other online accounts that use the same compromised login credentials.

7. Delete or disable unnecessary accounts

Old, unused accounts, sometimes referred to as orphan accounts, are favorites of attackers probing for access into protected systems. These accounts are typically unmonitored, and frequently use credentials that remain unchanged for years. In a recent breach reported by a school vendor, attackers were able to access company systems using the access key of a former employee. Although the employee had left the company years prior to the attack, the account and access key remained unchanged because the company did not cull inactive accounts or require credentials to be updated.

Businesses should have processes in place to delete or disable accounts with access to sensitive information when employees leave or vendor engagements end. Most businesses should also regularly audit accounts to identify those that have been inactive for an extended period of time.

8. Guard against automated attacks

Credential stuffing continues to be one of the most common forms of attack on customer accounts. This type of attack typically involves repeated attempts to log in to online accounts using usernames and passwords stolen from other online services. Cybercriminals often use automated software, or "bots," that are capable of cycling through hundreds of login attempts simultaneously without manual input. Once a cybercriminal successfully logs into an account, they may be able to make purchases using a credit card saved to the account, steal a gift card saved to the account, use customer data saved to the account in a phishing attack, or sell the login credentials on the dark web.

Our office has also taken action over a company's failure to appropriately respond to successful credential stuffing attacks. In a recent lawsuit against Dunkin' Donuts, we alleged that tens of thousands of Dunkin' customer accounts had been compromised in a series of online attacks. Although Dunkin' was aware of these attacks, the company failed to take any action to protect customers whose accounts it knew had been compromised, such as notifying impacted customers of the breach, resetting account passwords to prevent further unauthorized access, or freezing stored value cards registered with the customer accounts.

For many businesses, credential stuffing attacks are unavoidable. That's why businesses that maintain online accounts for their customers should have a data security program in place that includes effective safeguards for protecting customers from credential stuffing attacks. In January 2022, we released a Business Guide for Credential Stuffing Attacks that detailed four areas in which safeguards should be maintained, and specific safeguards that have been found to be effective.

9. Provide clear and accurate notice to consumers

When consumer information falls into attackers' hands, notice enables consumers to take steps to protect themselves. That is why it is critical that businesses provide consumers with notice that is both timely and accurate. When a business instead issues statements that are misleading in an effort to downplay the scope or severity of an attack, it can give consumers a false sense of security. It can also violate New York law.

We recently took action to hold a company accountable for misleading statements made following an attack. As noted above, in 2018, attackers infiltrated Zoetop's systems and stole a variety of customer information. Zoetop first learned of the attack from its payment processer, which wrote that it had information "indicating that [Zoetop's] system[s] have been infiltrated and [credit] card data stolen." In a public statement following the breach, however, Zoetop falsely wrote that it had "no evidence" credit card information had been taken from its systems. Zoetop also publicly represented, falsely, that it was in the process of notifying customers who had been affected in the attack. In fact, Zoetop failed to notify the vast majority of customers whose login information had been stolen.

Notice is a critical aspect of incident response. Businesses should take care to provide notice that is timely, and that clearly and accurately conveys material information about the attack.

Conclusion

> New York prides itself on being a national leader for innovation and progress. We excel at generating exciting new technology that can improve lives, but we must ensure that consumers can navigate the digital world safely and responsibly. As cybercriminals' techniques and tactics continue to improve, so must our efforts to stop them. Organizations can take relatively simple steps to secure their systems, and reduce or eliminate data breaches. This guide should help organizations strengthen their data security programs so that they can provide New Yorkers the best data security in the country.