Ignoring NY SHIELD Act's Cybersecurity Mandate Proves Costly

New York's Cybersecurity mandate under the New York SHIELD Act became effective on March 22, 2020. This unfortunate timing, considering its alignment with the beginning of COVID-19 shutdowns, created an almost unspoken moratorium on enforcement of the Act until recently. Two years post-enactment, the NY Attorney General's Office (NYAG) has revealed its increased focus on compliance with SHIELD, including recent settlements associated with data breaches suffered by EyeMed, Inc., Wegmans Food Markets, Inc. and Carnival Corporation.

In EyeMed, the company suffered a data breach in 2020 when cybercriminals gained access to an EyeMed email account containing sensitive emails with attachments dating back six years. The categories of information compromised included names, addresses, social security numbers and insurance account numbers. The NYAG investigation revealed that the hacker used the compromised account to send phishing emails to EyeMed clients, seeking to obtain login credentials. The breach affected approximately 2.1 million U.S. residents, including 98,632 New York residents.

Upon notification, the NYAG investigated EyeMed's cybersecurity practices at the time of the breach. As a result of the investigation and subsequent enforcement proceeding, the parties reached a settlement obligating EyeMed to pay New York State $600,000 for its violation of SHIELD cybersecurity requirements, and implement the following changes immediately:

- Maintain a comprehensive, written information security program and require multi-factor authentication for ALL administrative or remote access accounts;
- Encrypt sensitive consumer information;
- Conduct penetration testing to identify and remediate any security flaws within the network;
- Implement and maintain logging and monitoring of network activity; and
- Permanently delete consumer personal information when no longer required for legitimate business purpose.

Following EyeMed, in June, the NYAG settled with Wegmans for $400,000 after discovery of its "poor cybersecurity systems and practices." Wegmans will now pay New York State significant monetary penalties for maintaining unsecured, misconfigured cloud storage containers open to public access for multiple years; failing to inventory and maintain long-term logs of cloud assets; possessing customers' sensitive personal information without a reasonable business purpose; failing to secure user passwords; and not regularly conducting security testing of cloud assets. The compromised data included customer names, email addresses, mailing addresses, drivers' license numbers as well as login credentials for Wegmans accounts.

In addition to the monetary penalty, Wegmans must also implement the following new measures:

- Maintain appropriate asset management practices;

- Establish policies and procedures to ensure appropriate access controls of cloud assets containing personal information;
- Maintain a reasonable vulnerability disclosure program;
- Implement appropriate practices for customer authentication and account management;
- Establish appropriate password policies and procedures for customer accounts; and
- Update data collection and retention practices.

The NYAG expanded upon the last bullet point to warn consumer facing organizations to only collect customer's personal information for reasonable business purposes.

Lastly, NYAG, along with 45 other state attorneys general, recovered $1.25 million from Carnival for a 2019 data breach resulting from its "reckless data security measures." Carnival publicly reported that an unauthorized actor gained access to employee email accounts in March 2020 but notified multiple attorney general offices of "suspicious email activity" nearly 10 months before. The categories of information compromised included names, addresses, passport numbers, driver's license numbers, payment card information, health information and some social security numbers.

Carnival agreed to strengthen its security and breach response by:

- implementing a breach response and notification plan;
- requiring MFA for remote email access and strong, complex passwords;
- logging and monitoring potential security events;
- implementing and requiring email security training for employees; and
- continuing to undergo independent information security assessments.

The NYAG's actions serve as a warning to any organization that collects, stores, transmits or maintains electronic data of New York residents. The measures outlined above should be in place at your organization and if any aspect is lacking, it should be corrected immediately. Failure to act now could be devastating to your business, both with respect to the costs and consequences of a reportable data breach and the significant regulatory fines that may be imposed.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including cybersecurity planning and prevention. If you have any questions about the information presented in this memo, please contact Jessica Copeland or any attorney in Bond's cybersecurity and data privacy practice.

Jessica was part of a panel held by *Buffalo Business First* in honor of Cybersecurity Awareness Month. For a full recap on that discussion, click here.

BOND SCHOENECK & KING ATTORNEYS