CYBERSECURITY AND DATA PRIVACY

INFORMATION MEMO

APRIL 11, 2024

Four Years Strong: Reflecting on the Impact of the SHIELD Act

In March 2020, the Cybersecurity Mandate within New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into effect. In its entirety, the SHIELD Act expanded breach notification obligations for organizations and for the first time set forth a cybersecurity mandate for all organizations processing New York resident data to implement a series of safeguards to protect that data. However, March 2020 also marked the beginning of the COVID-19 pandemic, which caused many organizations to overlook the significance of the SHIELD Act and halt their compliance efforts. During the past four years, the New York Attorney General's Office (NYAG) has penalized several for profit and not for profit entities under the SHIELD Act, as demonstrated in recent settlements with US Radiology Specialist, Inc. (US Radiology), Healthplex, Inc. (Healthplex) and Refuah Health Center, Inc. (Refuah).

For example, in August 2022, US Radiology (a managed service provider for several partner companies including Windsong Radiology), reported a data breach as required by the SHIELD Act. According to the NYAG findings detailed in the settlement agreement between US Radiology and NYAG, US Radiology suffered a ransomware attack in December 2021 that affected nearly 100,000 patients. In January 2021, a US Radiology vendor learned of a vulnerability within its firewall and released a patch to address the vulnerability. However, US Radiology's hardware could not support the patch and it delayed upgrading its hardware. A hacker was able to access the following personal information: names, dates of birth, patient identification numbers, driver's license numbers, passport numbers and Social Security numbers. The NYAG's investigation revealed that US Radiology failed to adopt reasonable security practices to protect customer personal information. The parties entered a settlement that mandated US Radiology to pay $450,000 in fines and adopt the following security practices:

- Enhance and maintain its existing written information security program that ensures the security, integrity and confidentiality of patients' personal information;
- Create and implement an IT asset management program for identifying, reporting and prioritizing replacement or updates of IT assets;
- Encrypt patients' personal information that it collects, stores, transmits and/or maintains;
- Develop and maintain a penetration testing program that regularly identifies and remediates any and all security vulnerabilities found during testing; and
- Implement policies and procedures that seek to permanently delete their patients' personal data when there is no reasonable business purpose to retain it.

Following US Radiology, in December 2023, the NYAG settled with Healthplex for $400,000. In November 2021, an attacker successfully gained access to an employee email account through a phishing attack. The attacker gained access to over twelve years of emails causing Healthplex to notify approximately 90,000 members and 64,000 New York State residents. Some of the stolen information included names, member identification numbers, addresses, dates of birth, driver's license numbers, email addresses, phone numbers, financial information, and Social Security numbers. In addition to the monetary penalty, Healthplex was required to:

- Employ a Chief Information Security Officer that will report to the CEO and Healthplex's Board of Directors;
- Implement and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of private information;
- Encrypt member private information as defined by the SHIELD Act;

- Dispose of personal information when there is no business purpose to retain it; and
- Implement a reasonable email retention schedule for all employee accounts that contain private information.

Most recently, in January 2024, the NYAG entered into a settlement with Hudson-Valley based healthcare provider, Refuah. In May 2021, Refuah suffered a ransomware attack that impacted approximately 300,000 patients. According to the settlement, threat actors gained access to a system used for viewing security footage and migrated to Refuah's private network by using stolen login credentials for an administrative account. Notably, the stolen credentials were from a former IT vendor that were not disabled, deleted or changed. Before deploying malware, the threat actors exfiltrated approximately a terabyte of data. The affected personal information included patient names, addresses, phone numbers, Social Security numbers, state identification numbers, financial information and various health information.

According to the NYAG's investigation, Refuah failed to have an adequate data security program with appropriate safeguards, which included the failure to maintain appropriate controls limiting access to sensitive data. Specifically, Refuah failed to decommission inactive user accounts, rotate user account credentials, use multi-factor authentication and restrict employee access to only the data that is necessary for their business functions.

As a result of the NYAG's investigation, the parties entered into a settlement agreement requiring Refuah to pay $450,000 in fines and invest $1.2 million in strengthening its information security program, which includes:

- Maintaining a comprehensive information security program designed to protect the security, confidentiality and integrity of consumer information;
- Implementing and maintaining policies and procedures that limit access to consumer information;
- Requiring the use of multi-factor authentication to remotely access resources and data;
- Regularly rotate credentials that are used to access resources and data;
- Conducting audits at least semi-annually to ensure users only have access to resources and data necessary for their business functions;
- Encrypting all consumer information, whether stored or transmitted;
- Implementing controls to monitor and log all security and operational activity of the company's networks and systems; and
- Developing, implementing and maintaining a comprehensive incident response plan.

The NYAG has remained steadfast in its commitment to protect New York State residents' data from organizations with inadequate cybersecurity safeguards. Further, these settlements signify a trend that the NYAG is particularly paying close attention to the healthcare industry. Organizations should use these settlements as a guide to implement sound cybersecurity and privacy practices throughout their business.

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

BOND SCHOENECK & KING ATTORNEYS