Paradigm

INTERNATIONAL SOCIETY OF PRIMERUS LAW FIRMS

SPRING 2017

A History of Integrity Drives Primerus into the Future

Primerus, A Look Back Over 25 Years

Why Clients Turn to Primerus – Time and Again

+

Current Legal Topics:

Asia Pacific

Europe, Middle East & Africa

Latin America & Caribbean

North America

Disclosure of Cyber Attacks to the Public and Regulators: Changing Standards?

The first-of-its-kind New York State (NYS) Cybersecurity Regulation requires covered companies to notify the NYS Department of Financial Services (NYSDFS) for "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse" a computer system. The NYS regulation appears to go beyond the disclosure requirements of current regulations and laws, including through public filings (10-Ks and 8-Ks), state data breach laws, the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). This article will explore several current disclosure laws, how they differ from each other, in what circumstance each applies, and what corporate counsel must do to keep their companies safe in the face of existing legal ambiguity.

Khizar A. Sheikh

Khizar A. Sheikh is a member of Mandelbaum Salsburg P.C., and chairs its cybersecurity and privacy law group. He focuses his practice on cybersecurity, privacy, data and technology transactional and litigation matters. He counsels clients ranging from individuals to emerging growth companies to publicly traded, global organizations, in a variety of industries, including businesses in the banking and financial services, consumer retail, healthcare, professional services and education sectors.

Jacob Shulman, a law student at Rutgers Law School, assisted with the research for this article.

Mandelbaum Salsburg P.C.
3 Becker Farm Road, Suite 105
Roseland, New Jersey 07068

973.821.4172 Phone

ksheikh@lawfirm.ms
lawfirm.ms

Disclosure Requirements of Several Current Regulations and Laws

State Data Breach Laws

Most states and some territories have enacted laws requiring notification of security breaches involving personally identifiable information (PII). The primary purpose of these laws is to prevent identity theft. Most of these laws apply to any organization that collects PII from individuals in the state (even if not stored in that state). Some, but not all, of the laws create exemptions for organizations that are already covered by HIPAA or the GLBA.

PII is typically defined as an individual's name plus one or more of the following: (i) social security number (SSN), (ii) driver's license number or state issued ID card number, (iii) account number, credit card number or debit card number combined with any code or password needed to access an account. Some state definitions of PII are broader than the general definition (e.g., California includes email addresses, and Illinois includes fingerprints and other biometric data, etc.).

For the most part, breach is defined as the unlawful and unauthorized *acquisition* of PII that compromises the security, confidentiality or integrity of PII. In some states, notification is triggered by access, and not acquisition (e.g., Connecticut and New Jersey). If a breach occurs, organizations must notify the residents that are affected by the breach, in some cases law enforcement (e.g., New York and California, etc.), and in other cases they must make a public disclosure via publication. As for timing, organizations must generally notify as soon as practicable, although several states have specific time requirements, ranging from five calendar days to 90 days (many are 45 days).

A formal incident response plan is typically not required by state laws, but note that several states have specific requirements on storing information and security plans (e.g., Massachusetts requires organizations to draft and update a written information security plan).

HIPAA

Like state data breach laws, HIPAA focuses on the risk of harm to consumers and identity theft. HIPAA requires covered entities[1] and their vendors (business associates) to provide notification following a breach of

unsecured protected health information (PHI).[2] PHI is information collected from an individual, and is created or received by a covered entity and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and that identifies, or can identify, that individual.

A breach may result when there is an impermissible PHI use or disclosure that compromises security or privacy. Following a breach, covered entities must provide notification to affected individuals, the Department of Health and Human Services (HHS), and, in certain circumstances, to the media. This notification must be made to affected individuals within 60 days, and to HHS, within a specific time frame that is dependent on the size of the breach.

10-K and 8-K Disclosure[3]

In 2011, the SEC instructed organizations to report cyber incidents that could have a "material adverse effect on the business" and "when necessary in order to make other disclosures . . . not misleading," but did not define how organizations should analyze. Note that this obligation has little to do with protecting against identity theft, but rather disclosing "timely, comprehensive and accurate information about risks and events that a reasonable investor would consider important to an investment decision."[4] While the SEC has yet to bring an enforcement action against a public company for violating this guidance (but has brought enforcement actions relating to cybersecurity against broker-dealers), the recently disclosed Yahoo data breach may present its first test opportunity.[5] It appears that the SEC has requested documents to determine whether the company could have, and should have, reported a hacking attack cyber incident sooner that it did.

This regulatory focus on cyber disclosures is present in Federal Trade Commission (FTC) enforcement efforts as well. While not specifically focused on data breach notification (mainly because there is no federal data breach law), the FTC has been active against companies whose disclosures or omissions mislead consumers and violate Section 5 of the FTC Act. For example, in the recent Ashley Madison settlement, the company was required to pay $1.6 million after deceiving consumers by making assurances that personal information was private and securely protected, while, in reality, using "lax" security protections, including not having an adequate information security policy or incident response plan.

NYSDFS Cyber Regulation (December 2016 Revision[6])

The NYSDFS regulation does not focus on the risk of identity theft (although one of its stated goals is to protect NYS residents) or investor decisions, but on proper disclosure to the NYS regulator. The regulation applies to any banks, insurance companies or other financial services institutions regulated by NYSDFS that have 10 or more employees, or $5 million or more in revenue, or $10 million or more in assets. Like with HIPAA, vendors to covered organizations will be impacted through required contractual provisions.

Organizations must protect all nonpublic information, which is defined as all electronic information that is not publicly available and is: (i) business information whose tampering, unauthorized disclosure, access or use, would cause a "material adverse impact"; (ii) any personal identifier in combination with a SSN, drivers' license number or non-driver identification card number, account number, credit card or debit card number, any security code, access code, or password that would permit access to an individual's financial account, or biometric records; or (iii) any information, except age or gender, in any medium created by or derived from a health care provider or an individual and that relates to the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, the provision of health care to any individual, or payment for the provision of health care to any individual. Note that an incident response plan is explicitly required.

Each organization must notify the NYSDFS when "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on an information system" has

occurred and: (i) notice is required under another law or regulation; and (ii) has a reasonable likelihood of materially harming any material part of the normal operations of the organization, as promptly as possible but in no event later than 72 hours from a determination. There is no specific requirement to notify affected individuals, but the NYS data breach law still applies, as well as federal laws such as the GLBA.

What Corporate Counsel Must Do to Keep Their Companies Safe

We have touched on several laws, but because of space constraints, we do not address in detail every law that gives rise to disclosure obligations (e.g., various international laws, the FTC Health Breach Notification Rule, GLBA, specific SEC rules, such as Regulation S-P, to name several), which may apply depending on the types of information involved. Nonetheless, we can see that the NYSDFS regulation is different, in terms of applicable incidents, protected information and notification time frame. These differences follow a trend in state breach laws. States are generally expanding their PII definitions while shrinking the notification time periods. Corporate counsel must understand all laws, regulations and obligations (including contractual) that may apply to their organization.

Trying to ignore these obligations, before or after a breach, is not a viable option. Regulators have begun fining organizations for failing to notify in a timely manner.

Corporate counsel must also help their organizations draft their incident response plans with these varying laws in mind to ensure such plans are legally compliant. We often see incident response plans written by information technology professionals, which, while sometimes technologically robust, lack consideration of the liability risks.

Finally, note that for each of these and other laws, the information generator (controller) is ultimately liable for any breach or unauthorized access/acquisition, even if information is processed by a third party vendor. This risk can be mitigated through the proper contracts and insurance.

1 Covered entities are defined as health plans, health care clearinghouses and health care providers who electronically transmit health information.

2 Similar breach notification provisions are implemented and enforced by the Federal Trade Commission (FTC) for vendors of personal health records under the HITECH Act.

3 Form 10-K is an annual report that gives a summary of an organization's financial performance. Form 8-K is the form on which organizations report the occurrence of significant current corporate events.

4 See sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

5 In September 2006, Yahoo revealed than a state-sponsored attacker harvested personal data belonging to "at least" 500 million users. Just three months later, it admitted that some employees were aware of it as early as 2014, but waited years before making a disclosure. This issue is threatening to derail the acquisition of Yahoo by Verizon, which is reportedly seeking a $1 billion discount (or almost 20%) of the deal price.

6 After first introducing the proposed cybersecurity regulation in September 2016, the NYSDFS updated it on December 28, 2016, after "carefully consider[ing] comments submitted." This updated draft will be subject to an additional final 30-day comment period, which means that the regulation may change again before this article is published. For now, the effective date is March 1, 2017.