ALSTON&BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

ALSTONSECURITY.COM JANUARY 4, 2017

2016 Breach Notification Roundup
Part II: U.S. and EU Data Breach Notification Regulations Highlights and Trends

By Kim Peretti, Jason Wool and Nameir Abbas

Frameworks requiring breach notifications of various kinds significantly expanded in scope in 2016 at both the state and federal levels. (For "2016 Breach Roundup Part I: U.S. State Data Breach Notification Laws Highlights and Trends," click here). However, at least in the U.S., some of the new federal requirements may not be in place for long. As the Obama Administration nears its end, we saw several U.S. agencies push through regulations that include breach notification requirements against a backdrop of not insignificant opposition from many in the private sector and members of government. This casts doubt on whether the regulations will remain in place, at least as is, once President-elect Trump takes office. Meanwhile, as if in anticipation of the election results, at least one state (New York) took steps to impose first-in-the-nation cyber risk management regulations on the financial services industry that would go beyond the federal regulations on the same topic that are already in place.

In the EU, 2016 saw the finalization of two landmark pieces of legislation—the General Data Protection Regulation and the Network and Information Security Directive—both of which contain breach, or incident, notification requirements. A new, mandatory breach notification requirement also became effective in the Netherlands. Taken together, these legislative developments herald the arrival of a new regulatory environment for information security in the EU, where breach notification is largely voluntary and guidance-based today outside of specific industries, such as the telecommunications sector. We anticipate a significant increase in corporate compliance activities related to data breach response planning in the run-up to the effective dates of these new requirements.

Notable U.S. Updates for 2016

FCC – Likely effective June 2, 2017 (47 C.F.R. § 64.2006)

Overview

In late October, the Federal Communications Commission (FCC) approved new privacy rules applicable to broadband and other telecommunications services. Published in the *Federal Register* on December 2, 2016, the new rules constitute a substantial overhaul of the FCC's existing Customer Proprietary Network Information (CPNI) rules as well as a significant expansion of the jurisdictional scope of FCC privacy regulations. These changes are consistent with the classification of broadband as a Title II telecommunications service in the FCC's 2015 Open Internet Order.

Expanding the scope and breadth of the existing CPNI reporting rule

Although the CPNI rules have long required carriers to report to law enforcement and provide notifications to individuals following certain CPNI data breaches, the new rules are far more detailed. In this context, a breach is defined as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[1] In turn, "customer proprietary information" is defined as individually identifiable CPNI, personally identifiable information and content of communications that a carrier acquires while providing telecommunications service. In the context of broadband service, the FCC states that CPNI would include information such as broadband service plans, geolocation, MAC addresses or other device identifiers, IP addresses and domain name information, traffic statistics, port information, application header, application usage, application payload and customer premises equipment and device information.[2]

Notification to customers

A telecommunications carrier will now be required to notify affected customers of any breach without unreasonable delay and no later than 30 calendar days after it reasonably determines that a breach has occurred, subject to law enforcement needs. Importantly, the notification is not required if the carrier determines that no harm to customers is reasonably likely to occur as a result of the breach. The notice can be provided by mail or email or other electronic means if the customer agrees for data breach notification purposes.

Notification to the FCC

The carrier must also notify the FCC of any breach affecting 5,000 or more customers no later than seven business days after the carrier reasonably determines that a breach has occurred and at least three business days before notifying affected customers. This requirement does not apply, however, if the carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Notice must be made through a central reporting system made available by the FCC. For incidents affecting less than 5,000 customers, the report must be made without unreasonable delay and no later than 30 calendar days after the carrier reasonably determines a breach has occurred, unless the carrier can reasonably determine no harm to customers is reasonably likely to occur as a result of the breach.

---

1 47 C.F.R. § 64.2002(c).

2 Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016) at ¶ 53.

Notification to law enforcement

Breaches affecting 5,000 or more customers must also be reported to the FBI and the U.S. Secret Service no later than seven business days after the carrier reasonably determines that a breach has occurred and at least three business days before notifying affected customers, unless the carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Notice must be made through a central reporting system made available by the FCC.

Documentation

Carriers must maintain specific records of all breaches and any notifications provided to customers for at least two years.

Outlook

It is possible that we will see a quick repeal or other nullification, such as forbearance, of the new CPNI rules and possibly the Open Internet Order as well in light of widespread opposition to the rules by the telecommunications industry and some members of President-elect Trump's FCC transition team. Notably, the new CPNI rules passed on a partisan basis, with both Republican commissioners dissenting in the final rulemaking. It is therefore unlikely that the new rules will survive long in the new Administration.

Department of Defense – Effective October 21, 2016 (48 C.F.R. § 252.204-7012)

Overview

After issuing several interim rules, the Department of Defense (DoD) issued a final rule in October on Network Penetration Reporting and Contracting for Cloud Services. The rule, which amends the Defense Federal Acquisition Regulation Supplement (DFARS), includes an updated breach notification requirement.

Rapid reporting requirements

As finalized, the revised clause requires contractors that discover a cyber incident affecting a covered contractor information system or covered defense information, or that affects the contractor's ability to perform operationally critical support requirements identified in the contract, to conduct a forensic review for evidence of compromise of covered defense information and report the incident to the DoD via a web portal within 72 hours of discovery.

In this context, "covered defense information" is certain information described in the National Archives' Controlled Unclassified Information (CUI) Registry, which requires safeguarding pursuant to laws, regulations and government-wide policies, and is marked or otherwise identified in the contract and collected, developed, received, transmitted, used or stored in support of the performance of the contract.[3]

Before these changes, the rapid reporting requirement in this clause applied only to unclassified controlled technical information; now, however, the requirement applies to a much broader set of unclassified information.

---

[3] 48 C.F.R. § 252.204-7012(a).

Outlook

The rapid reporting rules were broadly opposed by the private sector in the years leading to the finalization of the regulation in late 2016. Although the new DFARS clause is less likely to be repealed than the FCC's CPNI rules, it is possible the Trump Administration will be amenable to softening the requirements of the new rule.

New York Department of Financial Services – March 1, 2017 (with additional transitional periods) (23 NYCRR 500.01–22)

Overview

In September, the New York Department of Financial Services (DFS) issued a proposed regulation that would impose detailed cybersecurity and cyber risk management requirements on jurisdictional entities, including breach notification. The DFS issued a revised version of the regulation in December 2016 that made several important changes to the original rules. In announcing the rules, Governor Andrew Cuomo rightly referred to proposed regulations as "first-in-the-nation." Indeed, the nature, breadth and scope of the new rules are possibly unprecedented at the state level.

Notification to the superintendent

Covered entities will be required to notify the superintendent no later than 72 hours after determining a cybersecurity event meeting one of two criteria has occurred: (1) a cybersecurity event about which notice must be provided to any government body, self-regulatory agency or other supervisory body; or (2) one that has a reasonable likelihood of materially harming any material part of the covered entity's operations.

A "cybersecurity event" is defined as an act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on the information system.

Wide applicability within the financial services industry

Once finalized, the DFS regulation will apply to any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York banking law, insurance law or financial services law. According to DFS's website, it supervises "nearly 1,900 banking and other financial institutions with assets of more than $2.9 trillion" and "all insurance companies that do business in New York," which includes "nearly 1,700 insurance companies with assets exceeding $4.2 trillion."

Potential indication of states ramping up cyber regulatory efforts

The DFS rules are another harbinger of some states (particularly New York and California) adopting an increasingly regulatory approach to cybersecurity, in contrast with the Obama and past Administrations' historic preference for light-touch regulation, public-private partnerships and voluntary cyber risk management frameworks. This activity may be even further catalyzed by the Trump Administration's apparent pro-business, antiregulation philosophy.

Food & Drug Administration – Draft issued January 22, 2016
(Postmarket Management of Cybersecurity in Medical Devices)

In draft guidance issued early this year, the Food & Drug Administration (FDA) provided guidance on the applicability of its "reports of corrections and removals" requirements in 21 C.F.R. 806.10 in the context of cyber vulnerabilities identified in post-market medical devices. The guidance provides that most actions taken by manufacturers to address vulnerabilities in medical devices will constitute "cybersecurity routine updates or patches" and therefore will not be reportable as a correction or removal. The guidance defines "routine updates and patches" as updates or patches that increase the security of the device or remediate identified vulnerabilities associated with controlled risks. Routine updates and patches do not include updates and patches that reduce risks to health or that correct a violation of the Federal Food, Drug, and Cosmetic Act, which are reportable under the regulation.

Notable EU Updates for 2016

General Data Protection Regulation (EU) – Enforceable May 2018 (REGULATION (EU) 2016/679)

Overview

The GDPR will introduce pan-EU breach notification requirements for data controllers and data processors. Whereas currently the existence of legal breach notification requirements varies by member country, the new regulation will standardize a minimum set of obligations applicable to all processing taking place within the scope of the law.

Notification to supervisory authorities

Article 33 of the GDPR requires processors to notify controllers "without undue delay after becoming aware of a personal data breach." Once it becomes aware of a personal data breach, the regulation requires a controller to notify the competent supervisory authority of a breach without undue delay but not later than 72 hours following discovery. This reporting is not required, however, if the personal data breach is "unlikely to result in a risk to the rights and freedoms of natural persons." The regulation sets certain minimum content requirements for this notification. It also requires controllers to document certain aspects of breaches to demonstrate compliance to supervisory authorities.

Article 4 defines a "personal data breach" broadly as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Notification to data subjects/safe harbor

Data controllers must also communicate breaches to affected data subjects without undue delay if the breach is likely to result in a "high risk" to the rights and freedoms of the individuals.[4]

However, notification to impacted individuals is not required when (1) the controller has implemented "appropriate technical and organisational protection measures" that were applied to the data impacted in

[4] Regulation (EU) 2016/679, Article 34(1).

the breach, particularly measures that render the data unintelligible to those not authorized to access it (e.g., encryption); (2) subsequent security measures taken ensure that high risks to the affected individuals' rights and freedoms are no longer likely to materialize; or (3) it would involve disproportionate effort, in which case controllers must make a "public communication" or similar measure so that data subjects are informed in an equally effective manner.

Netherlands – Effective January 1, 2016 (Wet bescherming persoonsgegevens)

Entities that operate in the Netherlands must now comply with a new set of data breach notification requirements as of this year. Pursuant to the new requirements, which arise from a 2015 amendment to the country's Data Protection Act, data controllers must notify the Dutch data protection authority (DPA) of any security breach impacting personal data that leads to a risk of, or actual, serious adverse consequences. This notification must be provided "immediately," which the DPA has interpreted in recent guidance as within 72 hours.

Notification to data subjects/safe harbor

If the breach is likely to adversely affect the personal privacy of the individuals whose personal data was compromised in the incident, the data controller must notify the data subjects without delay. This notification is not required, however, if the controller has taken appropriate technical protection measures that render the personal data in question incomprehensible or inaccessible to anyone that is not entitled to access the information, such as encryption.

Network and Information Security Directive – Members must transpose by May 2018 (Directive (EU) 2016/1148)

Notification to competent authorities and/or CSIRTs

Around the same time as the GDPR, the EU also implemented the Network and Information Security Directive (NISD), which will, among other things, require operators of essential services and digital service providers to make certain notifications following security incidents. Operators of essential services (certain critical infrastructure operators that are reliant on networked systems in sectors such as energy and banking) will be required to notify competent authorities or national computer security incident response teams (CSIRTs) of incidents "having a significant impact on the continuity" of their essential services.[5] These notifications must be made "without undue delay." Digital service providers will similarly be required to notify competent authorities or national CSIRTs without undue delay following any incident "having a substantial impact" on the provision of certain defined services (online marketplace, online search engine and cloud computing services) offered within the EU. For both types of entities, the NISD provides criteria to be used in determining whether an incident's impact is significant or substantial, respectively.

More than data breaches

The NISD defines an "incident" as any event having an actual adverse effect on the "security of network and information systems," which is in turn defined as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality

5 Directive (EU) 2016/1148 at Article 14(3).

of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems." Accordingly, incidents that have an actual adverse effect on systems' ability to resist attacks on data or service availability and integrity, and which affect the continuity of essential services, would require notification. This is fundamentally different from the other breach notification requirements discussed in this update, which are primarily concerned with the confidentiality and security of personal data and not continuity of operations. Moreover, the NISD is mostly concerned with an entire other species of incident—those primarily affecting the integrity or availability critical data and systems.

Deadline for transposition

The European Parliament formally adopted the NISD on July 6, 2016, and the directive entered into force in August. EU member states will have 21 months to transpose NISD into law, or until May 2018.

Conclusion

Although it is difficult to predict, we expect 2017 to be a year of relaxing U.S. federal agency cybersecurity requirements (or, at a minimum, enforcements), including breach notification requirements, on the private sector. It is possible that states such as New York and California will take additional actions to fill the void in cybersecurity regulation if it seems that the federal government is not taking a proactive enough role.

In the EU, we expect that GDPR and NISD implementation efforts will continue unabated, with additional countries proactively coming into compliance with various aspects of the laws before the applicable deadlines, including breach notification.

If you have any questions or would like additional information, please contact Kimberly Peretti, Jason Wool or Nameir Abbas.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333