Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | November 2016

Introduction

We focus this month's issue on two key areas – first, the ongoing court debate about insurance issues in connection with security breaches. Mary Borja and Ted Brown look at recent developments involving "breachless" claims – situations where there are allegations of security failings without an actual incident. Parker Lavin and Ted Brown look at a separate new decision involving coverage issues for data breaches under a Commercial General Liability (CGL) policy.

On a broader note, our TMT team looks at the most significant regulatory development of the past month – the issuance by the Federal Communications Commission (FCC) of new privacy and security provisions for the broadband industry. The team goes into the details of these rules – which will have a material impact on these providers – and we'll be watching future challenges to these rules going forward.

As always, please let me know if you have questions or comments on any of these topics, or if we can be of assistance in connection with any of these developments. Please let me know if you have thoughts on topics you would like us to address in future issues of *Privacy in Focus*. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

-Kirk Nahra, Privacy Practice Chair

The FCC's Broadband Privacy Order: A New Privacy Framework

On November 2, 2016, the Federal Communications Commission (FCC or Commission) released the text of its Report and Order imposing broad and complex privacy and security obligations on broadband internet access service (BIAS). The new rules, along with FCC "guidance" about best practices, regulate the data collection and use practices of BIAS providers, telecommunications carriers providing telecommunications services, and interconnected VoIP services. They do not apply to "edge" providers or others in the Internet ecosystem.

The FCC revised existing privacy rules to harmonize requirements across Title II carriers and services, addressing fallout from its 2015 reclassification decision. The new rules focus on three main concepts: transparency, choice, and security. Among many obligations, providers must notify customers about the types of information providers collect and how they use or share that information. Providers must obtain different levels of customer consent to use or share information depending upon the sensitivity of information and the use. The rules also impose new data security requirements, as well as notice requirements in the event of breach.

FCC Chairman Tom Wheeler and Commissioners Clyburn and Rosenworcel voted in favor of the Order, while Commissioners Pai and O'Rielly dissented.

ALSO IN THIS ISSUE

A summary of the FCC's Order follows.

The FCC Finds a Need for Broadband Privacy Rules

Section 222 of the 1996 Telecommunications Act protects certain data that telecommunications carriers collect from their customers. (¶ 21). Congress gave the FCC authority to promulgate rules under Section 222. (¶ 23). The FCC did not regulate BIAS providers under Section 222 until the *2015 Open Internet Order*, which reclassified BIAS as a telecommunications service under Title II of the Communications Act.

The FCC found that BIAS providers "sit at a privileged place in the network, the bottleneck between the customer and the rest of the Internet," allowing

continued on page 2

them to "collect an unprecedented breadth of electronic personal information." (¶ 28).

Privacy Obligations Under Section 222 Are Broadened though New Definitions

Providers and Customers. The FCC's rules apply to all carriers providing telecommunications services subject to Title II, including BIAS providers and interconnected VoIP providers. (¶ 39). For Section 222 purposes, the FCC adopted the definition in the *2015 Open Internet Order*: a BIAS provider is a person engaged in the provision of BIAS. (¶ 40). This does not include "premises operators – such as coffee shops, bookstores, airlines, private end-user networks" and other businesses that acquire BIAS from a provider to enable patrons to access the Internet. (¶ 40). Likewise, the rules "do not govern information that BIAS providers obtain by virtue of providing other non-telecommunications services, such as edge services like email, cloud services, and websites. (¶ 40).

A "customer" is "a current or former subscriber to a telecommunications service; or an applicant for a telecommunications service," which means "the duty to protect customer proprietary information . . . begins when a person applies for service and continues after a subscriber terminates his or her service." (¶¶ 41-42). Customer includes all users of the subscription, which includes household members and their guests. (¶ 44).

Customers' Confidential Information is Broadly Defined With New Categories. In terms of scope, the FCC creates multiple overlapping categories of information that need protection: "we import the statutory definition of customer proprietary network information (CPNI) into our implementing rules, and define customer proprietary information (customer PI) as including individually identifiable CPNI, personally identifiable information (PII), and content of communications." (¶ 46).

CPNI. The FCC adopts and broadly interprets the statutory definition of customer proprietary network information for all telecommunications services, including BIAS (though it noted that Section 222(h)(1)(B) focuses on telephone exchange and toll service and is not relevant to BIAS. (¶ 47).

CPNI includes information "made available to the carrier by the customer solely by virtue of the carrier-customer relationship," which includes any information falling within a CPNI category that the BIAS provider collects or accesses in connection with the provision of BIAS . . . if the provider acquires the information as a product of the relationship and not through an independent means." (¶ 48).

The FCC provides "a non-exhaustive list of the types of information that [it] considers CPNI in the BIAS context," rather than "a comprehensive list of data elements that do or do not satisfy the statutory definition of CPNI in the broadband context." The information relates to "the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier." (¶ 53). The FCC identifies the following:

- Broadband Service Plans: plans "detail subscription information, including the type of service (e.g., fixed or mobile; cable or fiber; prepaid or term contract), speed, pricing, and capacity (e.g., data caps)." They can also explain the type of information a customer subscribes, how the provider configures the network to serve the customer, the types of services the customer receives, and where the customer lives. (¶ 64).
- Geo-location: information shows "the physical or geographical location of a customer or the customer's device(s)." (¶ 65).
- MAC Addresses and Other Device Identifiers: device identifiers, such as MAC addresses, are CPNI "because they relate to the technical configuration and destination of use of a telecommunications service." (¶ 67).
- IP Addresses and Domain Name Information: source and destination IP addresses are CPNI because they "relate to the destination, technical configuration, and/or location of a telecommunications service. (¶ 68). Domain names are CPNI because they easily translate into IP addresses and relate to destination and technical configuration. (¶ 72).
- Traffic Statistics: traffic statistics relate to the amount of use, destination, and type of service. Traffic statistics related to browsing history can reveal the "destination" of communications. BIAS providers could deduce the "type" of application that a customer is using and the purpose of a communication, based on traffic patterns. (¶ 74).
- Port Information: a port is "a logical endpoint of communication with the sender or receiver's application, and consequently relates to

continued on page 7

Insurance Coverage for Breachless Cybersecurity Claims

The recent headlines regarding Johnson & Johnson's disclosure "that a person could potentially gain unauthorized access to [a certain insulin] pump through its unencrypted radio frequency communication system," described by the company as a "cybersecurity issue," reflect the fact that companies are identifying security concerns involving products in the marketplace even before a hacking incident has taken place. *See* Animas customer letter (Oct. 4, 2016), here. These types of incidents are increasingly leading to claims and regulatory investigations focused on cybersecurity issues even in the absence of any data breach or computer security breach.

The availability of insurance coverage under cyber policies for these "breachless" claims will hinge on the specific language of the policy at issue, as well as the unique facts at play. In some instances, cyber policies will not afford coverage for the costs of addressing the issue because the insured cannot show that the policy's trigger of coverage—an actual or reasonably suspected breach—is present. Insurers and insureds will need to pay careful attention to the specific facts and policy language at issue when analyzing the potential of coverage.

Background

In the aftermath of a data breach, a company may quickly face claims on multiple fronts, including from consumers, businesses, and regulatory authorities. A cyber breach in many circumstances will involve harm to persons or organizations whose sensitive information is in fact compromised and misused. Those claims may fall within the general scope of coverage afforded by cyber insurance policies because one of the necessary predicates to trigger coverage under many cyber insurance policies—unauthorized access to sensitive information through the failure of computer security—is present. *See, e.g.*, *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. 15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. May 31, 2016; appeal pending, 9th Cir. No. 16-16141).

In addition to these "breach" claims, however, companies and other organizations are increasingly facing "breachless" claims, such as those involving unexploited vulnerabilities. These claims, while less common, often involve a different set of issues for the purposes of evaluating potential insurance coverage. Insurers will therefore need to evaluate these claims carefully, and insureds should examine their risk management strategies, such as through insurance and contractual indemnification, to mitigate potential exposure for liability.

To illustrate, a number of private putative class actions have been filed alleging security defects in certain products. *See, e.g.*, *Cahen v. Toyota Motor Corp.*, 3:15-cv-01104-WHO (N.D. Cal.) (alleging that defendant automobile manufacturers "sold or leased vehicles that are susceptible to computer hacking and are therefore unsafe"); *Ross v. St. Jude Medical Inc.*, No. 2:16-cv-06465-DMG (C.D. Cal.) (seeking damages and alleging that a "vulnerable communication channel in an implanted … device … could result in a major privacy breach"). These claims do not allege that a vulnerability *has* been exploited, but instead complain about *potential* vulnerabilities and allege harm from the existence of a *potential* for a breach. Plaintiffs commonly allege that they did not obtain the full benefit of their bargain because these vulnerabilities were neither known nor disclosed to them at the time they purchased the products.

In addition to claims by private litigants, companies may also face claims, inquiries, or investigations from regulatory authorities even in the absence of a breach. *See, e.g.*, *In re Dwolla, Inc.*, No. 2016-CFPB-0007 (Doc. 1, filed March 2, 2016) (consent order between company and CFPB entered into regarding alleged misrepresentations with regard to a company's data security practices despite there being no evidence of that consumers actually suffered tangible harm); *see also* Joe Carlson, *FDA joins investigation into security of St. Jude medical devices*, Star Tribune (Aug. 26, 2016) (available here) (discussing security of certain medical devices and noting that the FDA "confirmed that it has joined an investigation of claims that the devices can be hacked remotely"). These matters arise from a number of different sources and involve a variety of regulatory agencies.

Coverage Implications

These "breachless" claims present important questions for cyber insurers regarding the scope of coverage afforded under their policies. Given the wide variety of forms in the marketplace, this determination will often require careful analysis of the specific language of each policy to determine whether and to what extent coverage may respond.

As with any insurance policy, a policyholder bears the initial burden of proving that a coverage grant in

continued on page 4

its insurance policy has been triggered. *See, e.g.*, *Consolidated Edison Co. of New York, Inc. v. Allstate Ins. Co.*, 774 N.E.2d 687, 690 (N.Y. 2002). Cyber policies are virtually always written on a claims-made basis, and they often include a threshold requirement of the existence of a breach (or reasonably suspected breach) that is first discovered during the policy period. If the policy trigger includes the actual or reasonably suspected breach, a cyber policy may simply not respond to the "breachless" claim. Claims involving products may also give rise to other dispositive coverage issues. For example, many cyber policies respond only to incidents affecting specified computer systems. For claims involving the security of products or systems that do not fall within those networks, there may be no coverage for that independent reason.

In addition to third-party liability coverage, cyber policies often afford first-party coverage for the insured's own costs of investigating and responding to a breach. The trigger of coverage under the first-party coverage part in many cyber policies is the existence of a known or reasonably suspected breach of a company's computer network (provided it is first discovered during the applicable policy period). This coverage is not written to cover generalized concerns regarding data security. If it were, insurers would face an endless flow of claims given the needs of many insureds to work continuously to improve the security of their systems. Instead, it is triggered only when the insured discovers indicia that sensitive data was compromised. The availability and extent of coverage may in some respects mirror the triggers for reporting and notice obligations under state breach notification laws. *See, e.g.*, Cal. Civ. Code § 1798.82(a) (requiring notification to persons whose "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person"). In this way, first-party cyber coverage may be analogous to a commercial crime policy; while a commercial crime policy may afford certain coverage for a first-party loss after a crime has taken place, it typically does not cover the expenses of investigating potential holes in a company's security procedures that may enable crime to happen in the first instance. Likewise, a cyber policy may be triggered for first-party loss in the aftermath of an actual breach of the insured's data or computer system, but it does not afford coverage for the costs to simply assess an insured's systems or detect potential ways that a vulnerability might be exploited. In sum, in the absence of an actual breach event, and where there is no likelihood that sensitive information was actually or reasonably believed to have been compromised, first-party coverage seems unlikely to be available under a cyber policy.

Third-party liability coverages under cyber policies often are written to apply only to claims involving the same events that trigger coverage in the first-party context—*i.e.*, when there has been a data breach event (including a reasonably suspected compromise of data). Were it otherwise, these policies might be swept into coverage disputes when there were allegations of inadequate data security, even if the focus of those disputes was clearly on other, uncovered events. For example, a former employee asserting a claim for wrongful termination for "blowing the whistle" on potential security vulnerabilities would involve allegations of improper data security, but it would not trigger coverage under a cyber policy. Cyber policies thus often differ from other claims-made E&O or D&O policies triggered simply by a "Claim" for a "Wrongful Act" in that, as noted above, there is an additional requirement for the existence of a breach event.

Conclusion

While cyber insurance policy forms vary widely, the existence of an actual or reasonably suspected breach is fundamental to many cyber insurance policies currently in the marketplace. The "breach" is an essential element to trigger coverage. As claims and investigations that do not involve an actual or even reasonably suspected breach are becoming increasingly common, insurers and insureds must carefully examine the specific facts and policy language of a given matter to determine the existence of coverage. ■

For additional information, please contact:

Mary E. Borja
202.719.4252
MBorja@wileyrein.com

Edward R. Brown
202.719.7580
ERbrown@wileyrein.com

The Broad Coverage Implications from *Camp's Grocery* for Cyber Exposures under CGL Policies

At first glance, a recent federal district court decision appears to be simply another ruling finding no coverage for a "data breach" exposure under a Commercial General Liability (CGL) policy. See *Camp's Grocery, Inc. v. State Farm Fire & Casualty Co.,* No. 4:16-cv-0204, 2016 WL 6217161 (N.D. Ala. Oct. 25, 2016). But digging deeper, this decision has important implications for future cyber-related claims. The court found there was no third-party claim for property damage to tangible property where credit cards had to be replaced because intangible data contained on them had been compromised. In addition to finding that coverage was not triggered in the first instance, the court applied an increasingly common exclusion—which bars coverage for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"—to find that coverage was unavailable for a claim arising out of a payment card breach. Given the relative sparsity of case law on these issues, the court's decision to broadly apply the exclusion is likely to guide courts addressing data security issues in other contexts, such as the emerging risks at the intersection of physical property and cybersecurity, including exposures associated with the "Internet of Things."

Background

In *Camp's Grocery*, the policyholder, which operated a grocery store, was sued by three credit unions alleging that its computer network was hacked, which compromised confidential customer data including credit card, debit card, and check card information. As a result, the plaintiffs claimed that they suffered losses to their cardholder accounts in the form of card reissuance charges, fraud losses, lost interest and transaction fees, lost customers, diminished goodwill, and administrative expenses associated with investigating, correcting, and preventing fraud. The policyholder tendered the suit under its CGL policy, but the insurer denied coverage. In ensuing coverage litigation, the district court granted summary judgment in favor of the insurer.

First, the court rejected the policyholder's argument that first-party endorsements specific to computer programs and electronic data imposed a duty to defend or indemnify it for the credit unions' suit. The court found the policy to be unambiguous, and it refused to read the duty to defend (as described in a third-party liability coverage part) as also applying to the first-party coverage endorsements. The court determined that the insurer's discretionary right to defend "claims of owners of property" arising under the first-party coverage form did not impose a duty to defend claims involving such exposures, as the insured argued. In this way, the court's decision was similar to a recent decision applying New York law, *RVST Holdings, LLC v. Main Street America Assurance Co.*, 256 N.Y.S. 3d 712 (N.Y. App. Div. 2016), where the court also refused to conflate third-party and first-party coverages under a policy when addressing claims arising from a claim by a financial institution against a retailer following a payment card breach at the retailer's restaurants.

Second, the court addressed whether the underlying claim alleged "personal and advertising injury," which the policy defined to include "injury … arising out of one or more of the following offenses: … e. [o]ral or written publication, in any manner, that violates a person's right of privacy[.]" The court noted as a threshold matter that the policyholder abandoned its argument that that provision applied. The court went on to rule, however, that "[e]ven absent abandonment, [it] would find that the underlying action does not allege … 'personal and advertising injury' for the reasons stated in [the insurer's] brief."

Finally, the court also rejected the policyholder's argument that the plaintiffs' alleged losses in the form of "replacement customer debit and credit cards" alleged "property damage" within the meaning of the policy. The court noted that the policy expressly defined "property damage" to include "tangible property" only but not to include "electronic data." The court ruled that, even if credit and debit cards are tangible property, the plaintiffs did not focus on any acts or omissions that caused physical harm or damage to the cards but instead alleged that the policyholder's "lax computer network security allowed the intangible electronic data contained on the cards to be compromised such that the magnetically encoded card numbers could no longer be used, causing purely economic loss flowing from the need to issue replacement cards with new electronic data[,]" which was not a claim for "property damage" within the meaning of the policy. In addition, the court noted that the policy expressly excluded "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data," which it held would bar coverage in any event.

continued on page 6

The Broad Coverage Implications from Camp's Grocery *for Cyber Exposures under CGL Policies*

continued from page 5

Analysis

Camp's Grocery is important for a number of reasons.

First, the court recognized that first-party coverage pertains to losses sustained by the insured to its own property and refused to read a duty to defend into a coverage part covering direct loss. The court also properly found that certain Inland Marine endorsements did not create a duty to defend based on language stating the insured may "elect" to defend against suits arising from claims by owners of property.

Second, *Camp's Grocery* shows that "personal and advertising injury" has real limitations and cannot ordinarily be looked to as coverage for data breach liability.

Third, the decision shows that courts recognize the difference between the corruption of electronic data and damage to tangible property, even when the electronic data is stored on or in a tangible item. The decision further demonstrates that policyholders cannot circumvent a requirement for "property damage" by focusing on physical aspects of a loss, such as payment cards that are reissued, when the tangible property at issue is only made worthless because of the compromise of electronic data. The same rationale could apply to claims that computer systems or other devices are made worthless because of vulnerabilities associated with software within them.

Fourth, this decision shows that courts will apply exclusions for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data," which have become more prevalent in recent years since Insurance Services Office, Inc. published a new form endorsement for CGL coverage, in a straightforward and predictable manner. Going forward, this part of the court's ruling may have the broadest impact on future coverage litigation given that it adds to the growing body of case law applying broadly worded electronic data exclusions according to their terms. *See also Metro Brokers, Inc. v. Transp. Ins. Co.*, No. 1:12-cv-3010, 2013 WL 7117840 (N.D. Ga. Nov. 21, 2013) (applying "the extraordinarily broad exclusionary language" in an exclusion for "[a]ny 'malicious code'" and "[a]ny 'system penetration'" to bar coverage for a claim involving computer hacking through use of a key logger virus).

As the Internet of Things becomes an even bigger part of our economy, the limitation of property damage to tangible property and the widespread use of electronic data exclusions may have particular application when there are risks and claims that involve both cyber and physical aspects. ■

For more information, please contact:

Parker J. Lavin
202.719.7367
PLavin@wileyrein.com

Edward R. Brown
202.719.7580
ERbrown@wileyrein.com

Spotlight

Megan L. Brown, partner in Wiley Rein's Appellate, Cybersecurity, Data & Network Security, and Telecom, Media & Technology practices, has been recognized as one of the nation's top "Cybersecurity & Data Privacy Trailblazers" for 2016 by *The National Law Journal* (NLJ). Ms. Brown is among a select group of 50 honorees who made the list this year, and were profiled by NLJ in its October 31 issue.

This is the second consecutive year that a Wiley Rein attorney has been named to the highly competitive list. Matthew J. Gardner, of counsel in the firm's Cybersecurity and White Collar Defense & Government Investigations practices, was recognized as a NLJ Cybersecurity Trailblazer in 2015.

the 'destination' of a communication." It can show the destination, type, and technical configuration, of service. (¶ 75).

- Application Header: "contain[s] data for application-specific protocols to help request and convey application-specific content." It "communicates information between the application on the end user's device and the corresponding application at the other endpoint of the communication. The type of applications used, the URLs requested, and the email destination all convey information intended for use by the edge provider to render its service. Application headers can also reveal information about the amount of data being conveyed in the packet." (¶ 76).
- Application Usage: data that reveals customer use of an application can reveal the type of applications the customer uses and with whom she communicates. (¶ 78.)
- Application Payload: "part of the IP packet containing the substance of the communication between the customer and entity with which the customer is communicating." It can help "identify the parties to the communication . . . and thus the communication's destination." The "payload's size and substance can also indicate the amount of data the customer is using, the type of communication, and the duration of the use of the service." (¶ 79).
- Customer Premises Equipment and Other Device Information: "equipment employed on the premises of a person to originate, route, or terminate telecommunications." This includes mobile devices, smartphones, and tablets. Covered information relates to the technical configuration, type, and destination of a telecommunications service. It includes "protocols the BIAS provider uses to interface that device with its network, as well as the type of service to which the customer subscribes." (¶¶ 80-81).

Customer Proprietary Information. The FCC creates another category of protected information: "customer proprietary information," which it defines as "information that BIAS providers and other telecommunications carriers acquire in connection with their provision of service, which customers have an interest in protecting from disclosure." (¶ 85). It includes "three non-mutually-exclusive categories: (1) individually identifiable customer proprietary network information (CPNI), (2) personally identifiable information (PII), and (3) content of communications." (¶ 85).

PII is "information that is linked or reasonably linkable to an individual or device." Information is linked or reasonably linkable if it "can reasonably be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device." (¶ 89). This includes names, addresses, telephone numbers, and other information used to contact an individual. (¶ 95). It includes information on a subscriber list. (¶ 96). This definition applies to "all § 222 contexts." (¶ 100).

The content of communications is "any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication." (¶ 102).

De-identified Data. The FCC adopts the FTC's three-part test for de-identification:

1. Not reasonably linkable. Providers must determine that information is not linked or reasonably linkable to an individual or device. (¶ 111). If carriers maintain customer PI in identifiable and de-identified formats, "they must silo the data so that one dataset is not reasonably linkable to the other." (¶ 113).
2. Public Commitments. Carriers must "publicly commit to maintain and use de-identified information in a de-identified fashion and to not attempt to reidentify the data." This commitment must inform customers of their rights and the provider's practices, and promote accountability. (¶ 116).
3. Contractual Limits. Providers must contractually prohibit recipients of de-identified information from attempting to re-identify it. (¶ 117).

The FCC will use a case-by-case approach to determine whether otherwise personally identifiable customer PI has been de-identified. (¶ 121).

The FCC Mandates Meaningful Notice of Privacy Policies

The FCC rules require providers to disclose privacy practices, but are not prescriptive about format or specific content. (¶ 123).

continued on page 8

Required Privacy Disclosures. Privacy policies must accurately describe:

- The types of customer PI that collects by virtue of provision of service, and how that information is used; (¶¶ 127-129)
- Under what circumstances a carrier discloses or permits access to customer PI, including the categories of entities to which it discloses or permits and the purposes for which customer PI will be used by each category; (¶¶ 130-131), and
- How customers can exercise privacy choices. Privacy notices must:
  - Describe opt-in and opt-out rights. This includes explaining that:
    - denial of approval will not affect the provision of the telecommunications services of which they are a customer;
    - approval, denial, or withdrawal of approval is valid until the customer revokes such approval or denial, and the customer has the right to deny or withdraw access at any time. However, notice should explain that the provider may be compelled, or permitted, to disclose a customer's PI when is provided for by other laws.
  - Provide a simple, easy-to-use way to provide or withdraw consent. (¶¶ 132-134).

Timing and Placement of Notices. The FCC requires notice of privacy policies at the point of sale prior to purchase of service, and that they be clearly, conspicuously, and persistently available on carriers' websites and via apps that are used to manage service, if any. The FCC eliminated periodic notice requirements from the voice CPNI rules. (¶¶ 137-143).

Form and Format of Notices. The FCC declined to adopt a specific format for notices but:

- Notices should be clear, conspicuous, comprehensible and not misleading. (¶¶ 147-150).
- Providers should convey notice in a language that customers can understand. (¶ 151).
- So long as notices on mobile devices meet these guidelines and convey necessary information, they comply. (¶ 152).

The FCC directed the Consumer Advisory Committee ("CAC") to formulate a proposed standardized notice format within six months after its new membership is reconstituted, but no later than June 1, 2017. Providers that voluntarily adopt a format developed by the CAC and approved by the FCC bureaus will be in compliance with the requirement that notices be clear, conspicuous, comprehensible, and not misleading. (¶¶ 153-155).

Advance Notice of Material Changes to Privacy Policies. The FCC requires providers to give advance notice of material changes to privacy policies to existing customers, via email or other means of active communication agreed to by the customer. Advance notice of material changes to a privacy policy must be clear, conspicuous, comprehensible, and not misleading. The notice also must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

The notice must inform customers of (1) changes being made; and (2) customers' rights with respect to a material change as it relates to customer PI. A "material change" is what a reasonable customer would consider important to her privacy decision. The FCC recommends that providers solicit contact preferences and let customers choose preferred methods of contact. It encouraged providers to include notices of changes in billing statements. (¶¶ 156-160).

Advance notice of material change should address whether changes are retroactive. The notice need not contain the entirety of the provider's privacy policies, so long as it accurately conveys relevant changes and provides easy access to full policies. The notice must be translated into a language other than English if the provider transacts business with the customer in that language. The notice also must explain the customer's rights. Although the FCC did not specify the timeframe for advance notice, BIAS providers and other telecommunications carriers must give sufficient advance notice to allow the customers to exercise meaningful choice. (¶ 163).

Harmonizing Voice Rules. The FCC applied these rules to all providers of telecommunications services, so that notice rules are harmonized across BIAS and other telecommunications services. In harmonizing the rules, the FCC eliminated requirements it no longer found necessary, such as requiring notices be re-sent every two years and have specific email subject lines. (¶¶ 164-165).

continued on page 9

The FCC Imposes Approval Requirements for the Use and Disclosure of Categories of Customer Proprietary Information

In applying Section 222 to BIAS, the Commission adopted separate customer choice rules for sensitive and non-sensitive customer PI. (¶ 166).

- Sensitive Customer PI: Use and sharing of sensitive customer PI requires express informed consent (opt-in) from customers. Sensitive customer PI includes, at a minimum, precise geo-location, health, financial and children's information; Social Security numbers; content; and web browsing and application usage and their functional equivalents. For voice, sensitive customer PI includes call detail information. (¶ 167).
- Non-Sensitive Customer PI: Providers must provide customers the ability to opt out of the use or sharing of non-sensitive customer information. Providers must also provide customers with a persistent, easy-to-use mechanism to adjust their choice. (¶ 167).
- Material Retroactive Changes: Material retroactive changes to privacy, use, or sharing policies require opt-in approval from customers regardless of whether the previously collected consumer information is sensitive or non-sensitive PI. (¶ 195).

Because carriers must use and share customer PI to provide service, to bill and collect payment, and for other purposes, the FCC adopted limitations and exceptions to the customer choice rules.

No additional customer consent is required for a BIAS or telecommunications provider to use and share customer PI to provide the telecommunications service and services that are part of, necessary to, or used in the provision of telecommunications service. Consent to use customer PI in these circumstances can be implied in the service relationship. (¶ 203).

- The FCC clarified that the provision of telecommunication service includes limited first-party marketing of improved service within the scope of service to which the customer subscribes. (The FCC provides "guidance" that this includes communications services commonly bundled, customer premises equipment, services formerly known as "adjunct-to-basic" services, services for inside wiring, technical support, reasonable network management, and research to improve or protect the network). (¶ 204).

Carriers may also infer approval to use and share *non-sensitive* customer PI to market *other* communications services commonly marketed with the telecommunications service to which the customer already subscribes (*e.g.*, offering fixed or mobile voice and video service to an existing broadband Internet subscriber). (¶ 205). Notably, the FCC changes the rights of wireless carriers to market other services; "our rules no longer permit CMRS providers to use or share customer PI to market all information services without customer approval." (¶ 207).

Likewise, the FCC recognizes the need for "reasonable network management" (¶ 208), and the statutory rights of carriers to engage in certain activities. No additional consent is needed for a BIAS or telecommunications provider to:

- Initiate, render, bill, and collect for service;
- Protect rights and property of the carrier, or protect users of services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;
- Provide inbound services, including customer support, referral, or new services, within the scope of the customer's request; and
- Provide certain customer PI in emergency situations, including call location information of commercial mobile service users to certain specified emergency services in response to a user's call for emergency services, a user's legal guardian or immediate family in an emergency situation involving the risk of death or serious physical harm, and providers of information or database management services solely for the purpose of assisting in the delivery of emergency services in the case of an emergency. (¶¶ 210-220).

The FCC adopted requirements for soliciting customer opt-in and opt-out consent. Providers must solicit customers' privacy choices at the point of sale. (¶ 222). Additionally, a carrier making material changes to its privacy policy must solicit customers' choices before implementing changes. (¶ 223). The FCC declined to require particular forms or methods for the solicitation. (¶¶ 224-225). Solicitations of consent must clearly and conspicuously inform customers of (1) the types of customer PI that the carrier is seeking to use or share; (2) how those types of customer PI will be used or shared; and (3) the categories of entities with which information is shared. A solicitation must provide a means to easily access

continued on page 10

the carrier's privacy policy, as well as a way for customers to exercise their choice. (¶ 226).

Likewise, customer choice mechanisms must be simple, comprehensible and non-misleading, and at no additional cost. Carriers must make the mechanism persistently available through their websites, on apps, and on any functional equivalent, or by a 24-hour toll-free number if the carrier lacks a website. The FCC declined to require a particular format, except to specify that it should be clear and conspicuous, comprehensive, and non-misleading. (¶ 228). The Commission encourages, but does not require, carriers to make available a customer-facing dashboard to provide the customer choice mechanism. (¶ 230).

Providers must "promptly" implement a customer's choice. Although rules do not define promptly, the standard takes into account the size of the company, the type and amount of customer PI used, and the particular use or sharing involved. (¶ 231). Customer choices must stay in effect and not be changed without affirmative consent (in the case of sensitive customer PI and previously collected non-sensitive PI), or opportunity to object (for non-sensitive customer PI to be collected in the future). (¶ 232).

To reduce burdens, the FCC eliminated compliance, recordkeeping, and annual certification requirements in Section 64.2009 of the FCC's rules. (¶ 234).

The FCC Mandates "Reasonable" Data Security Measures For Internet and Voice

The FCC mandates data security for BIAS providers and other telecommunications carriers: "[a] telecommunications carrier must take reasonable measures to protect customer PI from unauthorized use, disclosure, or access." 47 C.F.R § 64.2005(a). The carrier "may employ any lawful security measures that allow it to implement the requirement," 47 C.F.R § 64.2005(c). The FCC eschewed the "strict liability proposal originally offered, choosing to more

continued on page 11

Post-Election Review: Health Care Privacy and Security under a New Administration

Kirk J. Nahra, Speaker

Tuesday, December 6, 2016 | 1:00 PM to 2:30 PM ET

This session will explore the current state of health care privacy and data security, with an eye towards exploring new developments that are anticipated with a new administration and a new Congress. We will update the audience on the key developments from 2016, covering enforcement, litigation, and important industry updates. Then we will turn to the future – how the new administration will affect these developments and what we can expect looking forward into 2017 and beyond, for legislation, new regulations, overall enforcement topics and other issues of importance for the health care industry.

REGISTER HERE

Educational Objectives:

From this presentation, you will:

- Have an understanding of the key enforcement priorities today and going forward;
- Know the most significant new legislative proposals and regulations that will affect the industry in 2017;
- Be able to analyze where enforcement and audit developments will focus your company's compliance attention;
- Be able to evaluate how overall privacy regulation will be changing in the future
- Understand the most important privacy and data security developments for the year ahead for your company.

Who would benefit most from attending this program?

This session will be important for lawyers, compliance personnel, the privacy and data security industry and virtually anyone in the health care industry (including service providers to the industry) who work in any way with personal data or big data analytics.

directly focus on the reasonableness of the providers' data security practices." (¶ 236).

Reasonableness is Based on Context. Security "must appropriately take into account each of the following factors: (1) The nature and scope of the telecommunications carrier's activities; (2) The sensitivity of the data it collects; (3) The size of the telecommunications carrier; and (4) Technical feasibility." 47 C.F.R § 64.2005(b). These factors afford "flexibility." (¶ 242).

- The rule covers both sensitive and non-sensitive information, but providers need not have "the same, strict data security protections" for all information. (¶ 244).
- With respect to "technical feasibility" the FCC declines to expressly add cost consideration, but states that "our rule gives providers broad flexibility to consider costs when determining what security measures to implement over time." (¶ 244).

FCC Provides Guidance but No Safe Harbor. "[T]he presence and implementation of such practices will be factors [the FCC] will consider" in assessing compliance, but "these practices do not constitute a 'safe harbor.'" (¶ 246). The FCC provides guidance on practices that indicate compliance. "A provider that fails to keep current with industry best practices and other relevant guidance . . . runs the risk of both a preventable data breach and that it will be found out of compliance with our data security rule." (¶ 245).

- Industry Best Practices and Risk Management. FCC urges use of "up-to-date and relevant industry best practices, including available guidance on how to manage security risks responsibly" such as the NIST Cybersecurity Framework, CSRIC reports and best practices. (¶ 250).
- Strong Accountability and Oversight. The FCC expects a "written comprehensive data security program," the designation of senior management responsibility for data security as well as an official responsible for privacy practices, with "effective interaction with Boards of Directors." The FCC suggests "training employees and contractors on the proper handling of customer PI," and controls over third parties. The FCC also "remind[s] providers that they are directly accountable for the acts and omissions of their agents . . . for the entirety of the data lifecycle." (¶ 251-251).
- Robust Customer Authentication. The FCC urges providers to "consider stronger alternatives to relying on rudimentary forms of authentication," to use heightened authentication when appropriate, and to "notify customers of account changes and attempted account changes." (¶ 253).
- The FCC encourages data minimization and consideration of encryption. (¶ 254). The FCC urges "engagement in established information sharing practices." (¶ 254).

Voice Rules are Replaced. The FCC "replace[s] the data security rules that currently govern voice services with the more flexible standard we are adopting for BIAS," noting that some practices "may or may not be relevant in the context of providing voice services." (¶ 259).

The Rules do not Limit Other Lawful Activity. The FCC states that the rules do not limit "cyber threat information sharing that is lawfully conducted pursuant to the Cybersecurity Information Sharing Act of 2015 (CISA)." FCC encourages provider activity to "improve Internet security" and "protect their customers against" malware, phishing attacks and other threats. (¶ 246).

The FCC Imposes Detailed Breach Notification Requirements

To protect the confidentiality of customer PI, providers, including vendors and contractors, must notify the FCC and federal law enforcement regarding unauthorized or improper access, use, or disclosure of customer PI and sensitive PII if the access, use, or disclosure meets the FCC's harm-based framework. (¶¶ 261, 274). Under the framework, providers must disclose a breach if it determines that it is reasonably likely that customers will be harmed as a result of the breach. (¶¶ 261, 263). The FCC clarified that "harm" is not limited to financial harm, but also includes physical and emotional harm. (¶ 266). The FCC "establish[ed] a rebuttable presumption" that breach of sensitive PI requires customer notification. Providers must disclose information about the breach regardless if the data is encrypted and regardless of the source of the breach. (¶¶ 269, 271).

The FCC finds that its harm-based trigger will allow providers to focus only on breaches that adversely affect its customers, and will prevent notice-fatigue. (¶ 263). Providers have the burden to detect breaches and make a "reasonable determination" as to harm. (¶ 265).

continued on page 12

Providers must notify the FCC of all breaches that meet the harm-based trigger, and if 5,000 or more customers are likely to be harmed, providers must also notify the FBI and the Secret Service. (¶276). The FCC will take enforcement action against providers that do not comply. (¶276).

In terms of timing, for breaches affecting 5,000 or more customers, providers must notify the Commission, the FBI, and the Secret Service within seven business days of "reasonably determining that a breach has occurred," but at least three business days before notifying customers. (¶ 278). Federal law enforcement has discretion to delay notification to the public "to avoid interference with an ongoing criminal or national security investigation," which aligns with several states' law enforcement delay provisions. Federal law enforcement will delay notification only in "exceptional circumstances." (¶281).

For breaches of fewer than 5,000 customers, providers must notify the FCC without unreasonable delay and in any event no later than thirty calendar days after learning of a breach. (¶ 279). The Commission's 30-day customer notification time frame will allow carriers to conduct a thorough and complete investigation. (¶ 285). The FCC believes this time frame will lessen compliance burdens on small carriers, while providing customers an opportunity to engage in "time-sensitive mitigation activities." (¶ 286). To facilitate reporting, the Commission intends to create a centralized portal to the Commission and federal law enforcement. (¶ 282).

Providers' breach notifications to customers must include the following:

- The date, estimated date, or estimated date range of the breach;
- A description of the customer PI that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed;
- Information to contact the telecommunications carrier to inquire about the breach of security and the customer PI that the carrier maintains about the customer;
- Information about how to contact the FCC and relevant state regulatory agencies; and
- If the breach creates a risk of financial harm, information about national credit-reporting agencies and the steps customers can take to guard against identity theft. (¶ 288).

Notification should occur in writing to the customers' mailing or email addresses or by electronic means if the customers have agreed to that method. (¶ 291). Providers must keep records of the date the breach occurred and the date that customers were notified. (¶ 292). Providers must keep written copies of all notifications. (¶ 292). Record keeping requirements only apply to breaches that must be reported to the Commission. (¶ 292).

The FCC Regulates Other Practices That It Finds Raise Concerns

The FCC prohibited "take-it-or-leave-it" offers in which BIAS providers offer broadband service contingent on customers surrendering privacy rights. (¶ 294). BIAS providers are prohibited from terminating service or refusing to provide service due to a customer's refusal to waive privacy rights. (¶ 295).

The FCC adopted heightened disclosure and affirmative consent requirements for BIAS providers that offer financial incentives (such as lower monthly rates) in exchange for consent to use, disclose, and/or permit access to confidential information.[1] (¶ 294). Providers must "provide a clear and conspicuous notice of the terms of any financial incentive program that is explained in a way that is comprehensible and not misleading." The explanation "must include information about what customer PI the provider will collect, how it will be used, with what types of entities it will be shared and for what purposes," and the notice "must be provided both at the time the program is offered and at the time a customer elects to participate in the program." Providers must "make financial incentive notices easily accessible and separate from any other privacy notifications and translate such notices into a language other than English if they transact business with customers in that language." And, if a BIAS provider markets a service plan that involves an exchange of personal information for reduced pricing or other benefits, it must also provide at least as prominent information to customers about the equivalent plan without exchanging personal information." (¶ 301).

BIAS providers must "obtain customer opt-in consent for participation in any financial incentive program that requires a customer to give consent to use of customer PI," and once approval is obtained, they

continued on page 13

[1] The heightened disclosure and consent requirements apply only to financial incentive practices offered by BIAS providers. (¶ 298 n.868)

"must provide a simple and easy-to-use mechanism that enables customers to change their participation in such programs at any time." The mechanism "must be clear and conspicuous and in language that is comprehensible and not misleading," and must be "persistently available on or through the carrier's website; the carrier's application, if it provides one for account management purposes; and any functional equivalent of either." (¶ 302).

Although the FCC noted that this provides "flexibility to experiment," it cautioned that it will monitor such practices – "particularly if allegations arise that service prices are inflated such that customers are essentially compelled to choose between protecting their personal information and very high prices." The FCC will take action on a case-by-case basis if incentive practices are "unjust, unreasonable, unreasonably discriminatory, or contrary to Section 222." (¶ 303).

The FCC Addressed Other Contested Issues.

*Dispute Resolution***.** Carriers may not require customers to waive rights to file informal complaints through the appropriate channels. (¶ 304). Furthermore, the FCC announced that, in February 2017, it will "initiate a rulemaking on the use of mandatory arbitration requirements in consumer contracts for broadband and other communications services." (¶ 305). The FCC anticipates the lessons and conclusions drawn in the Consumer Financial Protection Bureau's rulemaking will be "informative and useful." (¶ 305).

Privacy and Data Security Exemption for Enterprise Voice Customers. The Commission revisited and broadened the existing exemption from Section 222 rules for enterprise voice customers, (¶ 306), which was previously limited (¶ 307). The new exemption will apply to "a carrier that contracts with an enterprise customer for telecommunications services other than BIAS . . . if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach; and provides a mechanism of the customer to communicate with the carrier about privacy and data security concerns." (¶ 306).

Implementation Times Vary.

The FCC emphasized that until new rules become effective, Section 222 continues to apply to all telecommunications services, including BIAS, and rules remain in place for voice. (¶¶ 310, 316). The FCC adopted the following timetable:

- Notice and Choice Rules: Effective the later of: (1) the date of Paperwork Reporting Act approval (with an eight week grace period for carriers to comply); or (2) twelve months after Federal Register publication of Order summary. (¶ 312).
- Data Breach Rule: Effective the later of: (1) the date of Paperwork Reporting Act approval (with an eight week grace period for carriers to comply); or (2) six months after Federal Register publication of Order summary. (¶ 313).
- Data Security Requirements: Effective 90 days after Federal Register publication of Order summary. (¶ 314).
- Prohibition on Conditioning Broadband Service on Waiving Privacy: Effective 30 days after Federal Register publication of Order summary. (¶ 314).

Small BIAS providers (100,000 or fewer broadband connections) and small voice providers (100,000 or fewer subscriber lines) will have an additional 12 months to implement the notice and customer approval rules. (¶¶ 320-23).

The FCC will grandfather any consumer consent for BIAS that was obtained prior to the effective date of the rules as long as the consent is consistent with the new requirements. (¶ 317). Consumer consent for other telecommunications services subject to the legacy rules (including opt-out and opt-in consent) remains valid within its original scope for the time it would have remained valid under the legacy rules. (¶ 319).

Preemption of State Law

The FCC adopted the proposal in the *NPRM* and announced its "intent to preempt state privacy laws, including data security and data breach laws, *only* to the extent that they are inconsistent with any rules adopted by the Commission. (¶ 324) (emphasis in original). The FCC clarified that states will "maintain broad authority for privacy regulation and enforcement." (¶ 324). The FCC agreed that it should not "undermine or override state law providing greater privacy protections that federal law." (¶ 327). Accordingly, the FCC rejected the notion that it should "preempt state data breach law entirely." (¶ 328). The FCC concluded by noting that it is clarifying that the same preemption standard applies across all aspects of Section 222, by adopting "a new preemption

continued on page 14

section that will clearly apply to all of [its] new rules for the privacy of customer proprietary information. (¶ 330). This standard applies to both BIAS and voice. (¶ 331).

Legal Authority

The FCC primarily grounded its new privacy and security rules in Section 222 of the Communications Act. (¶¶ 333-367). Because the FCC reclassified broadband providers as telecommunications carriers, the FCC rejected arguments that Section 222 could not be applied to broadband internet access service. (¶¶ 334-342). It also relied upon Section 201(b), Section 202(a), Title III, and Section 706 as additional sources of authority for the rules. (¶¶ 368-372). After clarifying its authority to apply the rules to providers of interconnected VoIP services (¶¶ 373-374), the FCC rejected First Amendment challenges to the rules, explaining that the rules are narrowly tailored to further the government's substantial interest in protecting the privacy of customers of telecommunications services. (¶¶ 375-392).

The Commission concluded that its sensitivity-based choice framework is supported by the U.S. Constitution and meets the three-part *Central Hudson* test. (¶ 375). The Commission dismissed the First Amendment concerns raised in the comments and emphasized that its rules do not amount to compelled speech or prior restraint and do not deny carriers their right of editorial control. ■

Several members of Wiley Rein's Telecom, Media and Technology, Privacy, and Cybersecurity practices contributed to this summary and work on aspects of FCC and FTC privacy and security regulation and enforcement. Clients should feel free to contact them for additional insights.

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

C. B'anca Glenn
202.719.3753
cglenn@wileyrein.com

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

John T. Lin
202.719.3570
jlin@wileyrein.com

Bennett L. Ross
202.719.7524
bross@wileyrein.com

Madi Lottenbach
202.719.4193
mlottenbach@wileyrein.com

Brett A. Shumate
202.719.7168
bshumate@wileyrein.com

Ari Meltzer
202.719.7467
ameltzer@wileyrein.com

Joshua S. Turner
202.719.4807
jturner@wileyrein.com

Katy M. Ross
202.719.7410
kmross@wileyrein.com

Daniel P. Brooks
202.719.4183
dbrooks@wileyrein.com

Dwayne D. Sam
202.719.3409
dsam@wileyrein.com

SPEECHES & EVENTS

Post-Election Review: Health Care Privacy and Security Under a New Administration
Kirk J. Nahra, Speaker
Bloomberg BNA
December 6, 2016 | Online Webinar

Managing Big Data in an Evolving Legal Environment
Kirk J. Nahra, Speaker
AHLA's Institute for Health Plan Counsel
December 9, 2016 | Chicago, IL

Acclimating to Changing Regulatory, Legislative & Enforcement Activities and Breach Notification Requirements
Kirk J. Nahra, Moderator
ACI's 21st National Advanced Global Legal and Compliance Forum on Cyber Security and Data Privacy & Protection
January 30, 2017 | Washington, DC

Navigating the HIPAA Enforcement Landscape
Kirk J. Nahra, Speaker
The 26th National HIPAA Summit
March 29-31, 2017 | Washington, DC

Contributing Authors

Mary E.Borja	202.719.4252	mborja@wileyrein.com
Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Scott D. Delacourt	202.719.7459	sdelacourt@wileyrein.com
Parker J. Lavin	202.719.7367	plavin@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Brett A. Shumate	202.719.7168	bshumate@wileyrein.com
Joshua S. Turner	202.719.4807	jturner@wileyrein.com