



ADVOCATE

NAVIGATE

EVALUATE

Alexicon *insider*

DECEMBER 21, 2016

SPECIAL BULLETIN

Broadband Privacy Rules *Effective Dates Announced*

The Broadband Privacy Rules adopted earlier this year ([link to FCC order](#)) now have several effective dates. In general, the FCC’s Broadband Privacy Order is effective January 3, 2017, but most of the major rules either require further PRA approval or have delayed effective dates.

Please note: All small providers (those with less than 100,000 connections) have an extra 12 months to implement and comply with the notice and customer approval rules (the most onerous rules).

Overall Effective Date:	January 3, 2017
New Data Security Requirements:	March 2, 2017
Data Breach Notifications:	Later of PRA approval or June 2, 2017
Notice & Customer Approval:	Later of PRA approval or December 4, 2017
“Take-it-or-leave-it” Prohibition	January 3, 2017

Thus, the earliest effective date of the notice and customer approval rules for small carriers is December 4, 2018.

Data Security Requirements

Eff. 3/2/17

The FCC adopted new data breach requirements for broadband internet access service (BIAS) providers that will also be applied to other telecommunications carriers. All providers must adopt reasonable security measures that take into account four factors:

- (1) Nature and scope of activities
- (2) Sensitivity of data collected
- (3) Size (of the provider)
- (4) Technical feasibility.

While the FCC does not mandate any specific measures, it does provide some guidance on how companies can meet the reasonableness standard (see further



Alexicon

Questions? Comments?

Contact Chris Barron

chris@alexicon.net



ADVOCATE

NAVIGATE

EVALUATE

Alexicon *insider*

DECEMBER 21, 2016

below). It is important to note that the FCC’s approach does not entail strict liability in the event of a data security breach, so long as the carrier has implemented reasonable measures.

For small carriers, the size factor should, in most cases, significantly inform the reasonable security measures adopted. In general, small BIAS providers do not collect and maintain, for example, web browsing information (a form of customer proprietary information) for many reasons, and thus would not, all things being equal, need to adopt measures of larger providers that do collect such information. In addition, small providers typically have limited data operations, and thus should take this into account when deciding on appropriate security measures.

The FCC offers the following to assist carriers in implementing reasonable data security measures:

- ⇒ **Engagement with industry best practices and risk management tools**
- In particular, see the National Institute for Standards and Technology Cybersecurity Framework ([NIST CSF](#)) and the Federal Trade Commission’s 2015 Security Guide for Business ([here](#)).
- ⇒ **Strong accountability and oversight**
- ⇒ **Robust customer authentication**
- ⇒ **Other practices**, such as implementing a “data minimization” policy.

Data Breach Notification Requirements

Earliest eff. 6/2/17

The FCC also adopted a set of rules governing circumstances in which carriers find customer proprietary information (PI) has been breached. The rules (47 CFR § 64.2006) will generally require customer notification within 30 days of a known breach, as well as notification of the FCC, the FBI, and the U.S. Secret Service for breaches that affect more than 5,000 customers. We will provide a more detailed summary of these rules once the effective date is known and draws nearer.

Customer Proprietary Information

- Individually identifiable CPNI
- Personally Identifiable information
- Content of Communications

“Take-It-Or-Leave-It” Prohibition

Eff. 1/3/17

The new broadband privacy rules prohibit the condition of BIAS offers on waived privacy rights, also known as “take-it-or-leave-it”. In addition, if a provider offers a financial incentive (i.e., lower monthly rates) in exchange for a customer’s approval to use the customer’s PI, then a notice must be provided that covers specific information (47 CFR § 64.2011).





ADVOCATE

NAVIGATE

EVALUATE

Alexicon *insider*

DECEMBER 21, 2016

Conclusion / Next Steps

Although the most onerous of the FCC's broadband privacy rules—those related to customer notice and approval—are not effective for small carriers until the end of 2018, there are portions of the rules that all carriers should prepare to implement. We will issue further updates once the effective date of the notice and approval rules draws nearer.

- ⇒ All carriers should ensure procedures are in place to comply with the “take-it-or-leave-it” prohibition rules
- ⇒ All carriers should take steps to ensure reasonable data security measures are in place. For small carriers, these measures should reflect the context in which any customer data may be used and, most importantly, the size of the provider.
- ⇒ Companies should become familiar with the data breach notification requirements (future Special Bulletin will cover in more detail).
- ⇒ Companies should review and become familiar with the customer notice and approval rules, as these have the potential to cause the most effort in ensuring compliance (think the early CPNI days).

Please let us know if you have any questions.



Alexicon

Questions? Comments?

Contact Chris Barron

chris@alexicon.net