Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106 (FCC 16-39)
Broadband and Other Telecommunications	)	
Services	)	

COMMENTS OF THE NATIONAL CONSUMERS LEAGUE

May 27, 2016

Executive Summary

The National Consumers League ("NCL") supports the Federal Communications Commission's ("FCC" or the "Commission") data security and data breach notification proposals. Because sensitive data cannot be separated from non-sensitive data without intrusive methods, NCL urges the Commission to consider all data that the broadband internet access service ("BIAS") providers use as deserving equal protections under the proposed Rules. NCL urges the Commission to integrate and expand on the strong consumer protection practices that are currently present in existing frameworks such as California's data security and data breach notification laws. In particular, NCL urges the Commission to implement high baseline data security protections that do not preempt stronger existing state laws. NCL also urges the Commission to adopt minimum security practices such as multi-factor authentication ("MFA"), to provide timely and transparent breach notification to consumers (e.g. information on credit freezes and providing notice about the negative consequences that will result from the breach), and to provide notification of all breaches to federal law enforcement and to the Commission.

The FCC is able to act pursuant to its Title II authority over common carriers in enacting data security and breach notification requirements on BIAS providers. The Commission's proposed rules are consistent with strong protections guaranteed under the traditional Customer Proprietary Network Information ("CPNI") rules within the telephony context and with other federal and state laws. Most importantly, the proposed rules provide a good starting point in ensuring that BIAS providers are upholding their duty to protect customers' personal information ("PI").

Data security is essential in protecting a customer's privacy, particularly when data breaches are an unavoidable threat in our modern digital economy. The

consensus among data security experts is that a breach occurring at an organization is not a question of if, but of when.[1] This is especially important given the trend towards convergence today such as Verizon's $4.4 billion purchase of AOL in 2015 and a potential bid for Yahoo this year.[2]

According to recent surveys by Pew Research, Americans have little confidence that their data will remain private and secure.[3] For instance, only 6% of respondents say they are "very confident" that landline telephone companies will be able to protect their data and only 25% say they are "somewhat confident" that the records of their activities will remain private and secure.[4] This is concerning because BIAS providers collect much larger and more sensitive data flows than traditional landline telephony providers. With the increasing scope[5] and cost of data breaches,[6] it is not enough to provide redress *ex post facto* but rather implement strong *ex ante* rules. In a world with ever increasing, highly publicized data breaches, consumers deserve confidence in the security of their data, clarity in notifications when those safeguards fail, and robust enforcement.[7]

---

[1] National Conference of State Legislatures, *Defending Against Breaches*, Mar. 1, 2015, http://www.ncsl.org/bookstore/state-legislatures-magazine/statestats-march-2015.aspx.
[2] Nick Statt, *Verizon has AOL chief Tim Armstrong looking into a Yahoo acquisition*, The Verge, Feb. 8, 2016, http://www.theverge.com/2016/2/8/10939526/verizon-yahoo-acquisition-aol-tim-armstrong.
[3] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015. Pg. 7. http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf
[4] *Id.*
[5] Experian, *Data Breach Industry Forecast*, Dec. 9, 2015, https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (*Experian Data Breach Forecast*).
[6] Elise Viebeck, *FBI: Data breaches 'increasing substantially*, The Hill, May 14, 2015, http://thehill.com/policy/cybersecurity/242110-fbi-official-data-breaches-increasing-substantially; Bill Rigby, *Cost of data breaches increasing to average of $3.8 million, study says*, May 27, 2015, http://www.reuters.com/article/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527; *See also* Privacy Rights Clearinghouse, *Chronology of Data Breaches Security Breaches 2005-Present*, https://www.privacyrights.org/data-breach (number of breaches have been going down but the records affected have increased dramatically) (last visited May 17, 2016) (*PRC Chronology of Data Breaches*).
[7] Ponemon Institute, *Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels*, PR Newswire, May 27, 2015,

NCL acknowledges the good work that the Federal Trade Commission ("FTC") has done and continues to do in consumer protection. This authority arises from Section 5 of the Federal Trade Commission Act, which allows the FTC to take action against companies engaged in unfair or deceptive practices, such as those involving the privacy and security of consumer information.[8] In particular, the FTC's Start With Security guide for businesses is a good starting point for companies looking to properly secure their data.[9]

The FCC and FTC have a proven history of collaboration. FTC Chairwoman Edith Ramirez has stated "the FTC has had numerous occasions to engage in cooperative initiatives with the FCC on privacy-related issues such as Do Not Call, pretexting, and mobile security."[10] Former FTC Commissioner Julie Brill has welcomed the FCC's enhanced presence as a "brawnier cop on the privacy beat."[11] The recent Memorandum of Understanding formalizes the collaborative efforts between the FCC and the FTC in ensuring stronger overall protection for

---

http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html.

[8] *See* FTC Chairwoman Edith Ramirez, *Prepared Statement of the Federal Trade Commission on 'Examining the Proposed FCC Privacy Rules' Before the United States Senate Committee on the Judiciary Subcommittee for Privacy Technology, and the Law*, May 11, 2016, https://www.judiciary.senate.gov/imo/media/doc/05-11-16%20Ramirez-Ohlhausen%20Joint%20Testimony.pdf.

[9] Federal Trade Commission, *Start With Security*, June 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (list of ten recommendations: start with security, control access to data sensibly, require secure passwords and authentication, store sensitive personal information securely and protect it during transmission, segment your network and monitor who's trying to get in and out, secure remote access to your network, apply sound security practices when developing new products, make sure your service providers implement reasonable security measures, put procedures in place to keep your security current and address vulnerabilities that may arise) (*FTC Start with Security*).

[10] Ramirez, *Prepared Statement of the Federal Trade Commission* at 9-11.

[11] FTC Commissioner Julie Brill, *Net Neutrality and Privacy: Challenges and Opportunities*, Nov. 19, 2015, at 1, https://www.ftc.gov/system/files/documents/public_statements/881663/151119netneutrality.pdf.

consumers.[12] However, the FCC clearly has authority under Title II to mandate data security and breach notification requirements in the BIAS space. The FCC's authority to set proactive, prescriptive rules is important in protecting consumers' data by setting out legally binding standards rather than voluntary, best practices. The FCC is the expert agency regarding BIAS and these proposed Rules will provide certainty compared with the FTC's case-by-case enforcement.

[12] *FCC-FTC Consumer Protection Memorandum of Understanding*, Nov. 16, 2015, https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf; *See also* Angelique Carson, *FCC vs. FTC isn't Batman vs. Superman*, International Association of Privacy Professionals, Oct. 1, 2015, https://iapp.org/news/a/ftc-v-ftc-isnt-batman-vs-superman/.

Table of Contents

Introduction

The National Consumers League ("NCL") respectfully submits the following comments in the above-captioned docket.

NCL is America's pioneering consumer advocacy organization, representing consumers and workers on marketplace and workplace issues since our founding in 1899.[13] NCL also hosts and maintains Fraud.org, a website dedicated to giving consumers the information they need to avoid becoming victims of telemarketing and Internet fraud. NCL issues a bi-weekly publication, *the #DataInsecurity Digest*, which delivers important consumer-focused data security news, policy, and news analysis to consumers. NCL's comments focus primarily on the data security and data breach notification provisions of the NPRM. However, NCL is also in agreement with comments filed by public interest organizations such as Public Knowledge, the Center for Democracy & Technology, and New America's Open Technology Institute regarding the privacy provisions of the NPRM.

I. BIAS Providers Must Implement and Maintain Robust Data Security Processes

The Commission's proposed rules lay out a firm framework that will ensure that customers of BIAS providers enjoy the data security protections that they deserve. BIAS providers pose a "unique and heightened risk to privacy for their subscribers" because BIAS providers collect vast amounts of customer information

[13] National Consumers League, *Mission*, http://www.nclnet.org/mission (last visited May 17, 2016).

and there is a relative lack of competition among BIAS providers.[14] Therefore, NCL views all information held by BIAS providers to be sensitive and thus require the same, strict data security protections. The FCC's proposed Rules reflect the lessons learned from its previous Consent Decrees such as the one with Cox Communications in 2015.[15] The dangers of data breaches apply to companies of all sizes, so it is important that the Commission mandate robust data security processes that ensure that BIAS providers will be proactive in their security efforts.

Because security practices are constantly evolving, NCL agrees with the FCC's proposal to "not to specify technical measures for implementing the data security requirements."[16] What constitutes reasonable data security today will not constitute reasonable security tomorrow. For example, passwords used to be the primary method in protecting access to information, but given the evolving threat landscape, there is consensus among data security professionals that passwords alone are no longer sufficient to authenticate access to users' accounts.[17] It is important that the FCC emphasize that while the Commission will not be overly prescriptive—in order to encourage innovation—it will still interpret the rules broadly in order to protect consumers. We urge that any employed authentication method should be measurable so that BIAS providers will be incentivized to continually test and update their data security.[18]

---

[14] Public Knowledge, *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World*, Feb. 2016, https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf.
[15] Cox Consent Decree, 30 FCC Rcd *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1105/DA-15-1241A1.pdf.
[16] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No.
16-106, Notice of Proposed Rulemaking, FCC 16-39, at para. 176 (rel. Apr. 1, 2016), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.docx (*Broadband Privacy NPRM*).
[17] *Broadband Privacy NPRM* at para. 197.
[18] Access, *Encrypt All The Things: A Digital Rights Campaign*, Mar. 4, 2014, https://encryptallthethings.net/docs/EATT.pdf.

II. A Multi-Stakeholder Process Is Not The Proper Avenue For Ensuring BIAS Data Security

Data security is too important of an issue to leave to a multi-stakeholder process similar to the National Telecommunications and Information Administration's ("NTIA") privacy multi-stakeholder processes.[19] Too often in multi-stakeholder processes the results are voluntary standards resulting from unequal bargaining power between powerful industry interests and other stakeholders. Effective data security requires something more than a voluntary standard. The efficacy of such talks is also questionable given the prior collapse of proceedings in multiple NTIA-led multi-stakeholder talks. For instance, the NTIA's facial recognition multi-stakeholder process led to the walkout of civil liberties and consumer advocacy groups last year.[20] In another example, mobile app transparency talks led to severe frustration on the part of consumer advocacy groups over the process' inability to produce a strong, obligatory code of conduct.[21]

Multi-stakeholder processes should not take the place of strong baseline security rules. If the NTIA were to conduct multi-stakeholder discussions, such discussions should focus on how BIAS providers can meet their obligations under the Commission's data security rules, rather than trying to replace the Commission's two-step data security proposal itself.

---

[19] *Broadband Privacy NPRM* at para. 178.
[20] Natasha Singer, *Consumer Groups Back Out of Federal Talks on Face Recognition*, The New York Times, June 16, 2015, http://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/.
[21] Angelique Carson, *Did NTIA's Multi-Stakeholder Process Work? Depends On Whom You Ask*, Sep. 3, 2013, International Association of Privacy Professionals, https://iapp.org/news/a/did-ntias-multi-stakeholder-process-work-depends-whom-you-ask/.

III. The FCC Should Examine and Integrate Strong Security Protection Frameworks From the OECD FIPPs, the PCI DSS, State Law, and the GDPR

As it considers existing regulatory and voluntary data security frameworks as models for its proposed rules, NCL urges the FCC to give added weight to frameworks that have a proven history of providing a baseline for robust data security protections. In addition to those identified by the FCC in paragraph 195 of the NPRM, the Commission should look to the Federal Trade Commission's Fair Information Practice Principles ("FIPPs"), the Payment Card Industry Data Security Standard ("PCI DSS"), the European Union's General Data Protection Regulation ("GDPR"), and strong existing state laws as a stepping stone towards crafting and refining its data security proposal.

The FTC's FIPPs are the foundation of privacy enforcement in the United States. The relevant provisions that apply to this NPRM require notice, security, and enforcement.[22] These FIPPs informed the later Organization of Economic Cooperation and Development ("OECD") *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, which require openness, security safeguards, and accountability.[23] The OECD Guidelines have formed the basis for national privacy laws, sector-specific laws, and best practices for the past three

[22] National Institute of Standards and Technology, *The Fair Information Practice Principles*, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf (*The FIPPs*).
[23] Hugo Teufel III, *Privacy Policy Guidance Memorandum*, U.S. Department of Homeland Security, Dec. 29, 2008, at 2, https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf; The Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

decades.[24] In keeping with these principles, it is important that BIAS providers implement and maintain robust security measures.

The PCI DSS is the information security standard for companies that handle credit and debit card transactions and is used to reduce fraud. Version 3.1 will expire on October 31, 2016 and the updated Version 3.2 requirements, which refine its established six control objects,[25] are best practices until February 1, 2018.[26] The noteworthy changes, which are useful standards for the FCC to examine, include a change in requirement from two-factor authentication to MFA, requiring MFA within local secure networks, requiring frequent penetration testing, requiring frequent reviews of employee adherence to the standards, and incentivizing companies to continuously implement and maintain the PCI DSS standards.[27] There have been critics of the PCI DSS who state that every company that has suffered a large hack in recent years has been PCI-compliant (Sony, Target, Anthem, etc.) and that Version 3.2, with its emphasis on compliance-driven security, will not move fast enough to address risks.[28] However, this standard is still useful in informing the Commission about the need and efficacy, based on industry experiences, of various security practices.

NCL also encourages the FCC to look at the Center for Internet Security's Critical Security Controls for Effective Cyber Defense (the "Controls") as a reference

---

[24] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, The White House, May 2014, at 17, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

[25] *Document Library*, PCI Security Standards Council, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf at 5 (build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy).

[26] Laura Johnson, *PCI DSS 3.2: What's New?*, PCI Security Standards Council, Apr. 28, 2016, http://blog.pcisecuritystandards.org/pci-dss-32-is-here.

[27] *Id.*

[28] Sean Michael Kerner, *Will PCI DSS 3.2 Make Payments More Secure?*, eWeek, May 2, 2016, http://www.eweek.com/security/will-pci-dss-3.2-make-payments-more-secure.html.

for prioritizing actions regarding the security risk management process and standards for security controls.[29] The 20 measures in the Controls define a "minimum level of information security that all organizations that collect or maintain personal information should meet."[30] The Controls can be grouped by the type of action they feature: count connections, configure securely, control users, update continuously, protect key assets, implement defenses, block access, train staff, monitor actively, and test and plan responses.[31]

At least 12 states have laws specifically addressing data security.[32] For instance, California requires that businesses "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[33] Massachusetts is stricter and requires the development, implementation, and maintenance of a "comprehensive security program" that "contains administrative, technical and physical safeguards."[34] There is also a section devoted solely to computer system security requirements.[35]

The FCC should also examine international law such as the European Union's GDPR, which will soon replace the Data Protection Directive as Europe's data protection law. The GDPR is a regulation as opposed to a mere directive, which

---

[29] Attorney General Kamala D. Harris, *California Data Breach Report*, California Department of Justice, Feb. 2016, at 30 https://oag.ca.gov/breachreport2016 (*California Data Breach Report*).
[30] *California Data Breach Report* at 31.
[31] *California Data Breach Report* at 32.
[32] Alissa M. Dolan, *Data Security and Breach Notification Legislation: Selected Legal Issues*, Congressional Research Service, Dec. 28, 2015, at 3 https://www.fas.org/sgp/crs/misc/R44326.pdf (Arkansas (ARK. CODE § 4-110-104); California (CAL. CIV. CODE § 1798.81.5); Connecticut (Conn. Pub. Acts No. 08- 167); Florida (FLA. STAT. §§ 282.318, 501.171); Indiana (IND. CODE § 24-4.9-3-3.5); Maryland (MD. CODE ANN., COM. LAW § 14-3501); Massachusetts (201 MASS. CODE REGS. § 17.00) (issued pursuant to MASS. GEN. LAWS ch. 93H); Nevada (NEV. REV. STAT. § 603A.210); Oregon (OR. REV. STAT. § 646A.622); Rhode Island (R.I. GEN. LAWS § 11- 49.2); Texas (TEX. BUS. & COM. CODE § 48.102); Utah (UTAH CODE § 13-44-201)).
[33] Cal. Civ. Code § 1798.81.5.2(b).
[34] Mass. 201 CMR 17.03(1) (also lists the minimum actions required).
[35] Mass. 201 CMR 17.04.

means that it directly imposes a uniform data security law regime on all EU members. The European Parliament approved the finalized GDPR on April 14, 2016.[36] NCL believes that the relevant provisions discussed below are appropriate frameworks for the FCC to consider. The GDPR contains data protection by design and by default in Article 25 and security of processing in Article 32, which requires companies to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk."[37] Article 35(1) requires a data protection impact assessment where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."[38]

IV. BIAS Providers Should Implement Strong Authentication Measures Such As MFA, But Only As Minimum Baseline

According to Verizon's recent *Data Breach Investigations Report* "63% of confirmed data breaches involved weak, default or stolen passwords."[39] This highlights the fundamental weakness of data security protections that rely solely on the combination of user identification and password as an authentication method. NCL recommends that BIAS providers—at a minimum—must implement safeguards

[36] European Parliament News, *Data protection reform - Parliament approves new rules fit for the digital era*, Apr. 14, 2016, http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era.
[37] Regulation 5419/16 of the European Parliament and of the Council on the General Data Protection Regulation, art. 25, 32 (*GDPR*).
[38] *GDPR*, art. 35 at 1.
[39] *2016 Data Breach Investigations Report, Verizon,* at 23, *available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ at 40 (Verizon Breach Report).*

beyond single-factor authentication based on such commonly compromised information.[40]

The Commission's proposed Rules would correctly require BIAS providers, at a minimum, to "[e]stablish and use robust customer authentication procedures to grant customers or their designees' access to customer PI." This requirement will compel all BIAS providers to implement common sense safeguards, such as multi-factor authentication, and regularly update their security practices. Absent robust regulatory incentives, breached entities have been slow to adopt more robust authentication technology despite suffering from serious data breaches. For instance, Sony took five years after it was breached, a breach affecting 77 million users, before it added two-factor authentication to its PlayStation Network.[41] This delay is unacceptable.

Static authentication methods—particularly single-factor, password-based authentication methods—are no longer sufficient as a means of authentication.[42] NCL recognizes that in the future, MFA might not be sufficient to protect consumers' data. However, MFA is a significantly stronger means of authentication than single-factor authentication. Therefore, the FCC should require mandatory MFA but should regularly review the efficacy of this measure. One way to establish this process would be to have an appropriate FCC advisory committee, such as the Technological Advisory Council, conduct regular meetings to discuss the efficacy of MFA and recommend updates to the authentication standard when MFA is no longer deemed to provide adequate protection.[43]

---

[40] *Broadband Privacy NPRM* at paras. 196-7.
[41] John Fontana, *Sony trots out 2-factor authentication 5 years after breach*, ZD Net, Apr. 20, 2016, http://www.zdnet.com/article/sony-trots-out-2-factor-authentication-5-years-after-breach.
[42] *Verizon Breach Report* at 20, 30; *California Data Breach Report* at 35.
[43] Technology Advisory Council, Federal Communications Commission (last visited May 17, 2016), https://www.fcc.gov/general/technological-advisory-council.

NCL suggests that the FCC allow for the use of third-party credentials only as an alternative method of authentication to carrier-provided MFA. While allowing BIAS providers, particularly smaller ISPs, to utilize third-party credentials in this way might save time and resources, adding an additional link in the chain of trust increases the attack surface and increases the risk of a data breach.[44] Recognizing this trade-off, the security standards provided by third-party credentials providers should still be equivalent to those imposed on BIAS providers by the FCC. The BIAS providers should take responsibility for any lapses in security caused by the use of this method, which would be a proper reflection of the customer's expectation of the BIAS provider-client relationship.

V. BIAS Providers Must Conduct Risk Management Assessments in Order to Meet Evolving Security Risks

Risk management means that a BIAS provider must develop, implement, monitor, and regularly update a comprehensive information security program. This is a critical component to a strong data security program. The Commission's proposed rules would require BIAS providers to "[e]stablish and perform regular risk management assessments and promptly address any weaknesses in the provider's data security system identified by such assessments."[45] The basic process starts with assigning responsibility for information security within the organization, and continues as follows: identifying information assets and data to be secured; assessing risks to the assets and data; implementing technical, administrative, and physical controls to address identified risks; monitoring the effectiveness of controls and updating as risks, business practices, and controls evolve.[46] The frequency of

[44] *Broadband Privacy NPRM* at para. 196.
[45] 47 U.S.C § 64.7005(a)(1).
[46] *California Data Breach Report* at 29.

risk assessments should not be predicated on the sensitivity of the underlying information, because all information should be treated as equally sensitive within the BIAS context.[47] Mandating regular risk management assessments will compel BIAS providers to maintain parity with contemporary risks and vulnerabilities.

A. BIAS Providers Must Train Employees About Security Risks and Must Continually Assess Employees To Maintain Compliance

Employee training is another important component to a strong data security program.[48] The Commission's proposed rules require BIAS providers to "[t]rain employees, contractors and affiliates that handle customer PI about the BIAS provider's data security procedures."[49] Verizon's *Data Breach Investigations Report* found that the leading cause of reported data breaches were due to errors made by employees.[50] Regarding employee errors, phishing also remains a popular way to install persistent malware in order to steal user data and credentials.[51] A 2015 Druva survey found that a majority of companies (82%) have employees that do not follow established policies for data privacy.[52] This same Druva survey found that 56% of IT organizations struggled with insufficient employee awareness and understanding of data privacy policies.[53] While robust data security processes can mitigate the damage caused by a breach, it is important to emphasize that malware cannot be installed if employees do not click on malicious links, download harmful

---

[47] *Broadband Privacy NPRM* at para. 183.
[48] Daniel Solove, *Is Data Security Awareness Training Effective?*, Teach Privacy, Feb. 25, 2014, https://www.teachprivacy.com/data-security-awareness-training-effective/ (finding that data security awareness training is effective).
[49] 47 U.S.C. § 64.7005(a)(2).
[50] *Verizon Breach Report* at 40.
[51] *Verizon Breach Report* at 17; *California Data Breach Report* at 32.
[52] Druva, *The State of Data Privacy in 2015 A Survey of IT Professionals*, Apr. 2015, at 4 http://www.druva.com/resources/analyst-reports/the-state-of-data-privacy-dimensional-research-report/.
[53] *Id.* at 6.

email attachments, or fall victim to social engineering.[54] Therefore, it is vital that employees receive proper cybersecurity training to increase awareness and are regularly tested to ensure compliance with such training.[55]

B. BIAS Providers Must Designate a Senior Official Who Will Be Responsible for Information Security Measures.

It is important to have corporate accountability given the numerous costs of a breach: reputational and legal costs, downtime costs, and the negative consequences for leadership.[56]The Commission's proposed Rules require BIAS providers to "[d]esignate a senior management official with responsibility for implementing and maintaining the broadband provider's information security measures."[57] There is great value in designating a senior level information security officer, especially given the rising trend of high-profile breaches.[58] An information security officer can help a BIAS provider meet privacy and security regulations and centralize and coordinate a company's information security policy. An information security officer can also facilitate communications with customers before and after a breach.

Increasingly, CEOs have directly felt the consequences of high-profile breaches. For instance, Sony Pictures Entertainment co-chairwoman Amy Pascal[59]

---

[54] *Verizon Breach Report* at 19.
[55] *See generally* John Schroeter, *Measuring the Effectiveness of Your Security Awareness Program*, CIO, Feb. 12, 2014, http://www.cio.com/article/2378759/security0/measuring-the-effectiveness-of-your-security-awareness-program.html.
[56] *Experian Data Breach Forecast* at 6.
[57] 47 U.S.C. § 64.7005(a)(3).
[58] *See generally* Sarah K. White, *5 reasons you need to hire a Chief Privacy Officer*, CIO, Feb. 1, 2016, http://www.cio.com/article/3027929/leadership-management/5-reasons-you-need-to-hire-a-chief-privacy-officer.html.
[59] Dominic Rushe, *Amy Pascal steps down from Sony Pictures in wake of damaging email hack*, The Guardian, Feb. 5, 2015, http://www.theguardian.com/film/2015/feb/05/amy-pascal-leaving-sony-pictures-email-leak.

was fired in 2015 and Target chairman and CEO Gregg Steinhafel[60] was fired in 2014 as a direct result of data breaches. A 2014 Ponemon Institute survey found that data breaches are within the top three of incidents that affect a company's reputation (30%).[61] Executives themselves have ranked data breaches second only to poor customer service in terms of potential to damage business reputation.[62]

To be clear, data breaches do not just affect high-level officials. Breached companies, such as Target, have spent hundreds of millions of dollars dealing with the aftermath of data breaches.[63] After the Sony breach in 2014, Sony's employees were "forced to use pencil and paper and their personal email accounts in the days after the attack."[64] This breach was especially egregious given the large, public breach in 2011 of its PlayStation Network, which led to the theft of personal information about 77 million accounts and at least $171 million in cleanup costs.[65] Based on this past precedent, it is the benefit to all that BIAS providers reduce risks and fallout from data breaches.

---

[60] Tiffany Hsu, *Target CEO resigns as fallout from data breach continues*, Los Angeles Times, May 5, 2014, http://www.latimes.com/business/la-fi-target-ceo-20140506-story.html.
[61] Ponemon Institute, *The Aftermath of a Data Breach: Consumer Sentiment*, Apr. 2014, at 10 http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.
[62] Security Magazine, *Experian Study on Data Breaches Reveals Gaps in Response Plans*, Nov. 3, 2015, http://www.securitymagazine.com/articles/86760-experian-study-on-data-breaches-reveals-gaps-in-response-plans.
[63] Jonathan Stempel & Nandita Bose, *Target in $39.4 million settlement with banks over data breach*, Dec. 2, 2015, http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203.
[64] Daniel Miller & Saba Hamedy, *Cyberattack could cost Sony Pictures tens of millions of dollars*, Los Angeles Times, Dec. 5, 2014, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hacking-cost-20141205-story.html.
[65] John Gaudiosi, *Why Sony didn't learn from its 2011 hack*, Fortune, Dec. 24, 2014, http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

VI. BIAS Providers Must Compel Third Parties to Protect Shared Customer Data

Given customers' expectation concerning their relationships with their BIAS provider(s) and the high number of incidents attributable to poor vendor security, NCL urges the Commission to hold BIAS providers accountable for third party recipients' handling of customer PI. This responsibility should hold for the entire lifecycle of the data.[66] For example, high-profile breaches at companies such as at Target have been traced to security lapses by third party vendors.[67] NCL agrees with the Commission's contention that "Section 222(a) requires BIAS providers to ensure the confidentiality of customer PI when shared with third parties."[68] Verizon's *Data Breach Investigations Report* found that "97% of breaches featuring stolen credentials leveraged legitimate partner access."[69]

The Target breach exposed personal data and credit information on more than 110 million consumers. One of Target's HVC vendors, Fazio Mechanical ("Fazio"), fell victim to an email phishing attack, allowing the thieves to install malware and steal the network credentials that had previously been issued to Fazio. Allegedly, Fazio's primary method of detecting malicious software on its internal systems was the free version of Malwarebytes Anti-Malware.[70] This reflects poor security processes. Furthermore, attackers moved from Target's external billing system into an internal portion of the network occupied by point-of-sale devices.[71] The failures in the Target case show the importance of segmenting systems and

---

[66] *Broadband Privacy NPRM* at para. 211.
[67] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, Feb. 12, 2014, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
[68] B*roadband Privacy NPRM* at para. 211.
[69] *Verizon Breach Report* at 33.
[70] Krebs, *Email Attack on Vendor Set Up Breach at Target*.
[71] *Id.*

implementing strong authentication. This failure is also a result of failing to adhere to FTC best practices.[72] Target has spent over $290 million in costs related to the breach—costs that are inevitably passed along to consumers—and these costs are expected to increase.[73]

Another example of the need to better secure customer information when shared with third parties is the recent breach at Experian. Experian was the third party processor of credit checks for T-Mobile. In September 2015, Experian disclosed that it had suffered a breach of T-Mobile data, ranging from at least the dates between September 1, 2013 and September 16, 2015. This breach exposed approximately 15 million Social Security numbers ("SSNs") and other sensitive information on consumers who had applied for financing from T-Mobile.[74] This is very alarming because SSNs are a key piece of data needed to perpetrate new account identity theft. Interestingly, Experian itself has suffered previously from a hacker gaining access to sensitive information via a subsidiary.[75] As of November 2015—only one month after disclosure of the breach—Experian disclosed that it had spent at least $20 million in response to the breach.[76]

NCL encourages the FCC to mandate that BIAS providers must obtain general contractual commitments from third parties to safeguard consumers' data while leaving the specific terms to the company's discretion.[77] However, if the FCC chooses to mandate specific practices,[78] then it should require—at minimum—that third

---

[72] *FTC Start With Security* at 3.
[73] Stempel & Bose, *supra*.
[74] Brian Krebs, *Experian Breach Affects 15 Million Consumers*, Oct. 2, 2015, http://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/.
[75] Brian Krebs, *ID Theft Service Proprietor Gets 13 Years*, July 15, 2015, http://krebsonsecurity.com/2015/07/id-theft-service-proprietor-gets-13-years/.
[76] Adam Sage, *T-Mobile Data Breach Response Cost Experian $20M*, Law 360, Nov. 12, 2015, http://www.law360.com/articles/726434/t-mobile-data-breach-response-cost-experian-20m.
[77] *Broadband Privacy NPRM* at para. 212; *See* Md. Code, Com. Law § 14-3503(b)(1) (shall require by contract that the third party implement and maintain reasonable security procedures and practices).
[78] *Broadband Privacy NPRM* at para. 212.

parties be contractually required to adhere to the same data security processes as BIAS providers. Third parties should be required to notify BIAS providers after discovering a data breach involving BIAS customers' data.

VII. BIAS Providers Should Limit Data Collection, the Time Period for Retaining Customer Data, and Should Securely Dispose Of Customer Data

NCL believes that, due to the unique position of BIAS providers with regards to their ability to see all traffic traversing their networks, all information should be treated as equally sensitive for data security purposes. This would be a stronger framework than the FCC's assertion that the "more customer information that a BIAS provider maintains, and the more sensitive that information is, the stronger the data security measures a BIAS provider will need to employ to protect the confidentiality of that information."[79]

Data minimization is one of the core principles under the FIPPs.[80] Data minimization requires that companies should only collect personally identifiable information ("PII") that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill those specified purpose(s).[81] Data minimization is a common-sense way of reducing both the records affected in the event of a breach and the surface area for attack. Data minimization requirements would also be consistent with consumer expectations. According to a recent Pew Research survey, only a small number of Americans

[79] *Broadband Privacy NPRM* at para. 221.
[80] *The FIPPs.*
[81] *Id.*

(16%) believe that their cellular telephone company or their landline telephone company should be able to retain records of their activity.[82]

NCL acknowledges that preserving data can be useful in creating new services and in providing the Commission with metrics in the efficacy of its rules.[83] However, this must be balanced against the increased likelihood of a breach: the more data that a BIAS provider retains the higher the chance and the greater the damage from a breach. Security will never be perfect, so companies should ensure that they are minimizing as much risk as possible.[84]

It is also important to securely dispose of information that is no longer useful or applicable: practicing good disposal hygiene ensures that the company does not accidentally use customer data.[85] At least 31 states and Puerto Rico require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable.[86] For instance, California requires a business to take "all reasonable steps" to delete information "within its custody or control."[87] The future possibilities of big data should not blind companies to the large, present dangers of unnecessarily retaining data.

VIII. BIAS Providers Should Conduct, at Minimum, Yearly Audits to Ensure Compliance with the Commission's Rules

[82] Lee Rainie, *The state of privacy in America: What we learned*, Pew Research Center, Jan. 20, 2016, http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.
[83] *Broadband Privacy NPRM* at para. 229.
[84] Swapnil Bhartiya, *Linus Torvalds: Security will never be perfect*, CIO, Aug. 20, 2015, http://www.cio.com/article/2973995/linux/linus-torvalds-security-is-never-going-to-be-perfect.html.
[85] *Verizon Breach Report* at 42.
[86] National Conference of State Legislatures, *Data Disposal Laws*, Jan. 12, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.
[87] Cal. Civ. Code §1798.81.

NCL strongly encourages the FCC to require, at a minimum, yearly security audits to be conducted by independent parties. The frequent audits are necessary to ensure compliance with the FCC's rules, as well as to encourage companies to treat security issues seriously throughout the year.

IX. Breach Notification is an Integral to Protecting Customers After a Breach and For Fixing and Resolving Weaknesses in Security

The trigger for notification to customers should not be harm-based[88] and should at least mirror the best state notices, which require notice based on a reasonable belief of acquisition by an unauthorized person.[89] If the FCC adopts a harm trigger because it finds that breach fatigue is indeed a legitimate worry, then it should make sure that the trigger is as broad as possible. However, any breach, no matter the size or scope, should always be reported to federal law enforcement and to the FCC. Notifications should be written in an organized and easily readable format.[90]

At minimum, BIAS providers should be required to report all breaches, no matter how small and regardless if the data is encrypted, to federal law enforcement and the Commission. For example, breach notification law in California states "the requirement to notify is triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person."[91] While the FCC will not be able to pursue all cases due to resource constraints, this breach notification data will be invaluable in providing much needed data to analyze the

[88] National Consumers League, *National Consumers League Statement on AdultFriendFinder.com Data Breach*, May 22, 2015, http://www.nclnet.org/adultfriendfinder_breach.
[89] *California Data Breach Report* at 4; *See also Broadband Privacy NPRM* at para. 237.
[90] *See* Cal. Civ. Code 1798.82(d)(1)(D).
[91] *California Data Breach Report* at 2.

impact and efficacy of its data security rules.[92] Breaches indicate lapses or vulnerabilities in security that companies will be forced to recognize and fix.[93] NCL believes that an ancillary benefit of these breach notification requirements is the creation of incentives for companies to share information in order to minimize the impact for themselves and for customers.

X. The FCC Should Integrate Strong Breach Notifications from State Law and the GDPR

The FCC should also examine existing legislation and determine common themes and trends in breach notification. This will also give the FCC an opportunity to determine the language that will afford customers the greatest protection.

There are many state laws that the FCC can examine: forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring entities to notify individuals of security breaches of PII.[94] At least 25 states in 2016 have introduced or are considering security breach notification bills or resolutions.[95]

The FCC should also review the GDPR, which contains multiple, consumer-protective provisions concerning breach notifications. For example, Article 33(1) requires notification of a breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it...unless the personal data breach is

---

[92] *Broadband Privacy NPRM* at para. 248.
[93] *Verizon Breach Report* at 42.
[94] National Conference of State Legislatures, *Security Breach Notification Laws*, Jan. 4, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[95] National Conference of State Legislatures, *2016 Security Breach Legislation* (last visited Apr. 29, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx.

unlikely to result in a risk to the rights and freedoms of natural persons."[96] Article 34(1) requires notification "without undue delay" when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons."[97] But there are exceptions, such as if the company has properly encrypted such data.[98] Article 33(2) requires third parties to notify the first party "without undue delay."[99] Article 30 requires companies to keep a record of all processing activities.[100]

XI. Consumers Should Receive Timely and Transparent Notifications

The number of records affected by data breaches continues to escalate.[101] Due to the upsurge of reports of data breaches in the media, data breach fatigue is a term that experts have continued to use to describe consumers' seeming indifference, particularly when data breaches only involve credit information.[102] Data breach fatigue can be defined as "the condition whereby consumers ignore or minimize the consequences of having their information compromised" as consumers continue to get inundated with notifications about the next big breach.[103] This means that consumers are less likely to take steps to protect themselves or to hold companies responsible for not protecting their information. However, there is evidence to show that customers who have been victims of a data breach do take

---

[96] *GDPR*, art. 33(1).
[97] *GDPR*, art. 34(1).
[98] *GDPR*, art. 34(3)(a) at 163.
[99] *GDPR*, art. 33(2).
[100] *GDPR*, art. 30.
[101] *See PRC Chronology of Data Breaches*.
[102] Sarah Hazack, *Home Depot and JPMorgan are doing fine. Is it a sign we're numb to data breaches?*, The Washington Post, Oct. 6, 2014, https://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/.
[103] Andrew Bolson, *If Not All Data Breaches Are Equal, Why Are All Data Breach Notifications Treated the Same?*, International Association of Privacy Professionals, Oct. 28, 2014, https://iapp.org/news/a/if-not-all-data-breaches-are-created-equal-why-are-all-data-breach-notifications-treated-the-same/.

steps to protect themselves.[104] For instance, RAND's recent survey on consumer attitudes toward data breach notifications found that 62 percent of respondents accepted offers of free credit reporting, suggesting that customers do in fact take steps to mitigate the negative consequences of a data breach.[105] A 2015 Ponemon Institute survey found that 67% of respondents believe that organizations have an obligation to compensate data breach victims, 63% believe that organizations need to provide identity theft protection, and 58% believe that organizations should provide credit monitoring services.[106] Furthermore, even if customers choose to do nothing, these notifications would still help create the foundation for agencies like the FCC to investigate and take appropriate action, and would create incentives to implement and maintain better security processes in order to avoid the costs of a breach.

A recent RAND survey found that 44 percent of respondents who recalled receiving a breach notification were already aware of the breach.[107] The same survey found that of the 68 percent of consumers who estimated some financial loss from a breach, the median loss was $500.[108] This is not an insignificant number. 63 percent of respondents stated that they would want companies to notify them immediately after a breach.[109] Customers deserve to know as quickly as possible so that they may take steps to mitigate the damage caused by a breach of their

---

[104] Michael Bruemmer, *Dispelling the Dangerous Myth of Data Breach Fatigue*, Security Magazine, Apr. 1, 2016, http://www.securitymagazine.com/articles/87014-dispelling-the-dangerous-myth-of-data-breach-fatigue.
[105] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, & Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, RAND Corporation, 2016, at xi, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf (*RAND Report*).
[106] Ponemon Institute, *The Aftermath of a Data Breach: Consumer Sentiment*, Apr. 2014, at 2, http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf (*Ponemon Aftermath of a Data Breach*).
[107] *RAND Report* at xi.
[108] *Id.* at xii.
[109] *Id.*

information. For instance, a bad actor could use phishing schemes to obtain more information on customers who have been victims of a breach.[110]

BIAS providers should also provide prominently displayed fraud alerts in their breach notices.[111] "When an individual has an alert on his report, a business must verify his identity before it issues credit."[112] Placing a fraud alert requires minimal effort and should be integrated in the remedial measures offered by BIAS providers in the event of a breach.[113] Initial fraud alerts must be renewed every 90 days. Extended fraud alerts may be used by victims of identity fraud to protect their credit for up to seven years.[114]

The breach notification should include a list of potential harms, as well as a list of steps that victims of the breach can take to limit the consequences of the breach. According to a 2014 Ponemon Institute survey, the most requested piece of information desired in a notification an explanation of the risks or harms that the consumer will experience as a result of the breach (67%).[115] California, in particular, has language in §§ 1798.82(d)(3)(A)-(B) suggesting that breached companies include in their breach notifications. Specifically, California law requires that "information about what [the business] has done to protect individuals whose information has been breached…[and to provide] [a]dvice on steps that the person whose information has been breached may take to protect himself" are included in the notification NCL urges the FCC to make this type of language a requirement in its

---

[110] Mike Litt & Edmund Mierzwinski, *Why You Should Get Security Freezes Before Your Information is Stolen*, U.S. PIRG Education Fund, Oct. 2015, at 4 http://uspirg.org/sites/pirg/files/reports/USPIRGFREEZE_0.pdf (*PIRG Security Freeze*).
[111] *California Data Breach Report* at 3, 37.
[112] Federal Trade Commission, *Place a Fraud Alert*, Aug. 2012, https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.
[113] *California Data Breach Report* at 37.
[114] Federal Trade Commission, *Credit Freeze FAQs*, Mar. 2014, https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.
[115] *Ponemon Aftermath of a Data Breach* at 4.

Rules in order to more effectively educate consumers. NCL also asks that the FCC encourage companies to offer identity theft prevention and mitigation services.[116]

In addition to a choice between written and electronic notifications required in 47 U.S.C. § 64.7006(a)(1), BIAS providers should be required to post and maintain substitute breach notifications in a clearly marked section of their websites.[117]

A. BIAS Providers Must Provide Information About Credit Freezes

NCL encourages the FCC to insert specific language in the proposed Rules concerning the information that is required in a customer notification.[118] While the proposed rules include providing information about credit monitoring, which only detects new account fraud, the Rules do not include information about credit freezes—which do more to prevent identity fraud. Many groups, like the U.S. Public Interest Research Group, recommend credit freezes because it is the only option available to consumers to prevent identity fraud before it happens.[119] A security freeze prevents a consumer reporting agency from releasing a credit report or any information from the report without authorization from the consumer.[120] Because different states have different requirements about credit freezes, NCL asks the FCC to require BIAS providers to provide information about credit freezes as specific to the state of each affected customer.

---

[116] *California Data Breach Report* at 3, 37.
[117] *See California Data Breach Report* at 7.
[118] 47 U.S.C. § 64.7006(a)(2)(v).
[119] *PIRG Security Freeze* at 1.
[120] National Conference of State Legislatures, *Consumer Report Security Freeze State Laws*, Mar. 31, 2016, http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx.

While credit freezes are effective in preventing the opening of new lines of credit, it also adds additional costs to the customer.[121] The lifting of a credit freeze often requires payment of a small fee and a short time delay,[122] which is an inconvenience and may prove to be an obstacle to low-income consumers.[123] It is important to acknowledge the limitations of credit monitoring, that these services do not prevent fraudsters from applying for and opening new lines of credit in your name (which a credit freeze does prevent). Credit monitoring services are not meant to prevent identity theft, but to assist the customer after the fact in cleaning up a compromised credit report.[124] Finally, it is important to note that neither credit monitoring nor security freezes can detect or prevent unauthorized use of a customer's existing credit accounts.[125]

XII. BIAS Providers Must Provide Notification to Customers Within Ten Days After Discovery of a Breach

Under the Commission's proposed Rules, BIAS providers are required to "notify affected customers of covered breaches of customer PI no later than 10 days after the discovery of the breach."[126] Most state breach laws have the same notification timing provisions as California's, which states that notification must be given "in the most expedient time possible, without unreasonable delay."[127] However, NCL recommends that the FCC keep its proposed time period of 10 days.

---

[121] *PIRG Security Freeze* at 15 (a security freeze costs between $3-10 and a $2-12 fee for unfreezing for each of the three big national credit bureaus).
[122] *Id.* (unfrozen within 15 minutes to up to three days).
[123] *California Data Breach Report* at 37.
[124] Om Malik, *Why Companies Won't Learn From the T-Mobile/Experian Hack*, The New Yorker, Oct. 6, 2015, http://www.newyorker.com/business/currency/why-companies-wont-learn-from-the-t-mobileexperian-hack.
[125] *PIRG Security Freeze* at 15-16 (in addition to tax refund fraud, medical fraud, reputational harm, or physical harm).
[126] 47 U.S.C. § 64.7006(a).
[127] *California Data Breach Report* at 4.

Because breaches are often not discovered immediately, it is vital that consumers be notified as quickly as possible in order to mitigate the later use of their data in identity fraud.

States with strict breach notification laws use the language of "without unreasonable delay."[128] However, the California Attorney General's Office has found that, in California, the average time from discovery of a breach to notification of those affected was 40 days, and in 75 percent of breaches notifications were made to those affected in 50 days or less.[129] It is important to note that this timing is from the date from discovery of the breach, not from the date that the breach actually occurred. Companies need to be forced to improve the time lag between actual breach, the date of discovery of the breach, and the notification to customers as any delay in notification will cause further grief to customers.

XIII. BIAS Providers Must Notify Law Enforcement and the Commission of All Breaches In Order to Show Compliance with and to Provide Data for the Efficacy of the Commission's Rules

NCL strongly agrees with the Commission's proposed breach notification Rules.[130] 47 U.S.C § 64.7006(b) requires BIAS providers to notify the FCC within seven days after discovering a breach of customer PI. 47 U.S.C § 64.7006(c) requires notification, within seven days after discovery of the breach, to the Federal Bureau of Investigation and the U.S. Secret Service if the breach affects more than 5,000 customers. NCL urges the FCC to adopt a lower threshold for notification here, such

[128] Cal. Civ. Code § 1798.82(a); Mass. Gen. Laws ch. 93H, § 3(a); 815 Ill. Comp. Stat. § 530/10(a).
[129] *California Data Breach Report* at 25.
[130] 47 U.S.C. §§ 64.7006(a)(2)(3), (b), (c).

as the threshold set by California of 500 or more people affected as a result of a single breach.[131]

Unlike the context of customer notification, here the Commission should not avoid robust data breach notification requirements because of concerns about data breach fatigue. According to Verizon's *Data Breach Investigations Report*, "[t]he time to compromise is almost always days or less, if not minutes or less."[132] The seven-day time period is also less restrictive than the GDPR, which requires notification to the relevant supervisory authority within 72 hours, unless there is no substantial risk of harm.[133] The notifications to federal law enforcement and the FCC will serve as early warning indicators and will hopefully lead to quick action and provide metrics regarding data breaches.

NCL agrees with the Commission's proposed Rules, which allows federal law enforcement to delay notifications to customers if it would "interfere with a criminal or national security investigation."[134] This language strikes the appropriate balance between customers' need to know and the ability of federal law enforcement to properly investigate the origins of the breach.

NCL agrees with the Commission's proposed Rules, which requires that BIAS providers "maintain a record of any breaches of security discovered and notifications made…[and] shall retain such records for a minimum of 2 years."[135] The retention of this data will serve a vital purpose in ensuring that enforcement agencies have the necessary information to conduct their jobs: the FCC will have data to ensure compliance and efficacy of its rules, and the FBI and the Secret Service will have data to measure trends in data breaches. The retention of this data

[131] Cal. Civ. Code § 1798.82(f).
[132] *Verizon Breach Report* at 11.
[133] *GDPR* at 53, para. 85.
[134] 47 U.S.C. § 64.7006(a)(3).
[135] 47 U.S.C. § 64.7006(d).

will not be overly burdensome, as BIAS providers should be retaining this sort of data for their own internal metrics and compliance with FCC-mandated security safeguards.

XIV. BIAS Providers Have An Obligation to Require Third Parties to Immediately Notify BIAS Providers As Soon As a Breach is Discovered

NCL believes the FCC should mandate that BIAS providers contractually require third parties with which they share customer PI to immediately notify the BIAS providers as soon as a breach is discovered.[136] All notifications that come to the attention of consumers should flow directly from the BIAS providers, as this falls within the relationship between BIAS providers and their customers. The duties owed to customers, within the context of the BIAS provider-customer relationship, cannot be waived through the sharing of customer data, so customers have a right of assurance that their data will be protected.

XV. NCL Continues to Advocate for Strong, National Breach Notification Standards Without Preempting Existing State Laws

NCL agrees with the Commission's approach in 47 U.S.C § 64.7007 that the Commission "shall determine whether a state law is preempted on a case-by-case basis, without the presumption that more restrictive state laws are preempted." This approach will ensure that States will be able to continue to innovate[137] in

[136] *Broadband Privacy NPRM* at para. 255.
[137] National Conference of State Legislatures, *Cybersecurity Legislation 2016*, Apr. 11, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-

protecting consumers' data, set a high bar for consumer protection, and help to clarify the baseline that BIAS providers must adhere to.[138] It is NCL's hope that the robust and comprehensive data security and breach notification rules set out by the FCC will also serve as a model for other states and agencies. NCL, in its 2015 Congressional Data Security Agenda, espoused the need for the creation of a strong national breach notification standard that continues to protect strong state laws such as California's.[139] A national bill should be required to set a high floor rather than a low ceiling.[140]

Conclusion

The FCC, as the expert agency, has a mandate to protect consumers' data in the context of BIAS providers. This mandate is especially important given the ability of ISPs to collect vast amounts of information concerning their customers. Just because the FCC is unable to regulate the entire Internet ecosystem does not mean that it should not act to regulate BIAS providers. Enacting strict rules will serve as a model to increase the security of consumers overall. By choosing to collect more and more information on customers, BIAS providers have an obligation, under their relationships with their customers, to properly protect customer data, and to notify customers when that data is improperly disclosed. As the California Attorney General's Office rightly puts it, "[companies] are also stewards of the data they collect and maintain. People entrust businesses and other organizations with their

---

legislation-2016.aspx (for example, cybersecurity legislation has been introduced in at least 25 states in 2016).

[138] *See California Data Breach Report* at 5; *See also* Andrea Peterson, *Why this national data breach notification bill has privacy advocates worried*, The Washington Post, Apr. 15, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/04/15/why-this-national-data-breach-notification-bill-has-privacy-advocates-worried/.

[139] National Consumers League, *2015 Congressional Data Security Agenda: A To-Do List for the 114th Congress*, Dec. 2014, *available at* http://www.slideshare.net/nationalconsumersleague/national-consumers-leagues-2015-cybersecurity-policy-agenda

[140] National Consumers League, *NCL statement on introduction of Data Security and Breach Notification Act of 2015*, Mar. 13, 2015, http://www.nclnet.org/statement_on_data_security_and_breach_notification_act_of_2015.

data on the understanding that the organizations have a both an ethical and a legal obligation to protect it from unauthorized access."[141] The Commission's rules will refine this obligation in the context of BIAS providers.

Respectfully submitted,

/S/

John D. Breyault
Vice President of Public Policy, Telecommunications and Fraud
National Consumers League

[141] *California Data Breach Report* at 28.