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

In the Matter of	)	
	)	
Q Link Wireless LLC and	)	File No.: EB-TCD-22-00034450
Hello Mobile Telecom LLC	)	NAL/Acct. No.: 202332170014
	)	FRN: 0021593975; 0027619089

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: July 20, 2023 **Released: July 28, 2023**

By the Commission:

I. INTRODUCTION

1. Safeguarding the privacy of American consumers and ensuring the protection of their sensitive data have been longstanding priorities for the Federal Communications Commission (FCC or Commission). In furtherance of these important goals, we take enforcement action against two companies—Q Link Wireless LLC (Q Link) and Hello Mobile Telecom LLC (Hello Mobile) (collectively, the Companies)—that apparently relied impermissibly upon readily available biographical information and account information to authenticate online customers. In doing so, the Companies appear to have flagrantly placed the security of their customers' information at risk.

2. Telecommunications carriers maintain increasingly large amounts of sensitive customer data, including information about the types of services their customers receive and how and when they use those services. This service-related information—known as "customer proprietary network information," or CPNI—includes, among other things, customer calling records and location information. Because of the sensitivity of this data, the Communications Act of 1934, as amended (the Act), and the Commission's rules require service providers to take reasonable measures to discover and protect against unauthorized use, access and disclosure of CPNI.

3. Under the Commission's rules, a carrier's customer must be authenticated by, and provide a password to, the carrier before being allowed online access to their CPNI. However, in order to protect CPNI from unauthorized third parties who could "pretext" or impersonate a customer, the Commission's rules prohibit carriers from authenticating a customer for online access to CPNI by using readily available biographical information or account information. Carriers also cannot create backup customer authentication methods (to address lost or forgotten passwords) that prompt customers for such biographical or account information

4. Accordingly, we propose a penalty of $20,000,000 against Q Link and Hello Mobile—which have common ownership and used the same app to provide their customers with access to CPNI—for apparently violating section 64.2010(c) of the Commission's CPNI rules by using readily available biographical information and account information for customer authentication. Finally, though we do not assess separate proposed forfeitures, we also find that (1) the Companies' use of readily available biographical information and account information to control access to CPNI apparently violated section 222 of the Act and section 64.2010(a) of the Commission's CPNI rules, and (2) Q Link's use of such information for back-up authentication and password reset purposes apparently violated section 64.2010(e) of the Commission's CPNI rules.

II. BACKGROUND

A. Legal Framework

5. The Act and the Commission's rules govern and limit telecommunications carriers' use and disclosure of certain customer information. Section 222(a) of the Act imposes a duty on telecommunications carriers to "protect the confidentiality of proprietary information," including that of "customers," and section 222(c) of the Act establishes specific privacy requirements for CPNI.[1]

6. CPNI is broadly defined in the Act and includes "information that 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, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[2] It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[3] The Commission has promulgated rules implementing the privacy requirements of section 222 (the CPNI Rules),[4] and has amended those rules over time. Most relevant to this proceeding are the rules that the Commission adopted in its 2007 CPNI Order,[5] specifically section 64.2010, establishing safeguards on the disclosure of CPNI.[6]

7. The Commission's 2007 rulemaking was largely in response to concerns about the practice of "pretexting,"[7] and included the adoption of section 64.2010 of the Commission's rules. Ultimately, the Commission wanted to ensure that carriers were only granting CPNI access to the consumer to whom the CPNI belonged and not to other third party impersonators. As such, the Commission implemented requirements that carriers first authenticate customers before granting them access to CPNI. Recognizing that authentication methods could easily be bypassed if they hinged on

[1] 47 U.S.C. § 222(a), (c). The Commission has also stated that section 222 of the Act imposes on Eligible Telecommunications Carriers (ETC) a duty to protect the confidentiality of documentation provided by Lifeline customers and applicants, and the personally identifiable information contained therein. *See* 47 U.S.C. § 222(a); *Lifeline and Link Up Reform and Modernization, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order*, WC Docket Nos. 11-42 et al., *Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order*, 30 FCC Rcd 7818, 7896, para. 234 (2015) (*2015 Lifeline Order on Reconsideration*). This includes a requirement that ETCs "employ the following practices to secure any subscriber information that is stored on a computer connected to a network: firewalls and boundary protections; protective naming conventions; user authentication requirements; and usage restrictions, to protect the confidentiality of consumers' proprietary personal information…." *2015 Lifeline Order on Reconsideration*, 30 FCC Rcd at 7896, para. 235. The Commission also requires providers participating in the Emergency Broadband Benefit Program and the Affordable Connectivity Program to "[s]ecurely retai[n] all information and documentation it receives related to the eligibility determination and enrollment…" 47 CFR §§ 54.1606(b)(3), 54.1806(b)(3).

[2] 47 U.S.C. § 222(h)(1)(A).

[3] *Id.* § 222(h)(1)(B).

[4] 47 CFR §§ 64.2001-64.2011.

[5] *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*).

[6] 47 CFR § 64.2010.

[7] As used in the *2007 CPNI Order*, "pretexting" means "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records." *2007 CPNI Order*, 22 FCC Rcd at 6928 & n.1. *See also AT&T Inc.*, Notice of Apparent Liability, 35 FCC Rcd 1743, 1746, 1763, paras. 7, 59 (2020).

readily obtainable account or biographical information, the Commission placed limits on the information that carriers are permitted to use for customer authentication.[8]

8. As the Commission explained in 2007, "some carriers permit customers to establish online accounts by providing readily available biographical information,"[9] and the record showed "holes" in carriers' authentication methods, such as "authenticating a customer's identity through information the carrier readily provides to any person purporting to be the customer without authentication."[10] The Commission also observed that "biographical identifiers are widely available on websites and easily obtained by pretexters" and that "biographical information like social security number can be found on the Internet."[11] Therefore, the Commission established a framework for customer authentication and specified that, because of their inherent vulnerabilities, certain types of data could not be used for authentication or related purposes.

9. Section 64.2010(a) of the Commission's rules requires that telecommunications carriers "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" and "properly authenticate" customers before disclosing CPNI over the telephone, online, or in-store.[12] Subsections (c) and (e) articulate specific rules about online access to CPNI and establishing/resetting customer passwords—with both sections prohibiting carriers from authenticating a customer through the use of "readily available biographical information" or "account information."[13] "Readily available biographical information" means "information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth."[14] "Account information" is "information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount."[15]

10. With respect to online access to CPNI, section 64.2010(c) of the Commission's rules requires carriers to authenticate their customers "without the use of readily available biographical information, or account information."[16] Once authenticated, customers may only obtain online access to CPNI through a password "that is not prompted by the carrier asking for readily available biographical information, or account information."[17] Section 64.2010(e) of the Commission's rules sets forth requirements for password establishment and back-up authentication methods. Specifically, a carrier must authenticate a customer—without the use of "readily available biographical information, or account information"—before the customer sets a password.[18] Similarly, while a carrier may establish back-up customer authentication methods in the event of lost or forgotten passwords, "such back-up customer

[8] *2007 CPNI Order*, 22 FCC Rcd at 6936-41, paras. 13-23.

[9] *Id.* at 6940, para. 20.

[10] *Id.* at 6940, para. 20 & n.73.

[11] *Id.* at 6940, para. 20 & n.74.

[12] 47 CFR § 64.2010(a).

[13] *Id.* § 64.2010(c), (e). The Commission made clear that the specific customer authentication requirements it adopted were "minimum standards" and emphasized the Commission's commitment "to taking resolute enforcement action to ensure that the goals of section 222 [were] achieved." *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[14] 47 CFR § 64.2003(m).

[15] *Id.* § 64.2003(a).

[16] *Id.* § 64.2010(c).

[17] *Id.*

[18] *Id.* § 64.2010(e).

authentication method may not prompt the customer for readily available biographical information, or account information."[19]

B. Factual Background

11. Q Link is a common carrier and mobile virtual network operator (MVNO) that offers wireless voice and data service under the Commission's Lifeline program[20] to qualifying low-income subscribers, as well as prepaid wireless services for both Lifeline and non-Lifeline subscribers.[21] Hello Mobile, an affiliate of Q Link, also is a common carrier and provides nationwide mobile wireless voice and data service to consumers as an MVNO. Both Companies are also identified as participating providers in the Commission's Affordable Connectivity Program.[22] Therefore, both Q Link and Hello Mobile are telecommunications carriers subject to the requirements of section 222 and the Commission's rules for the conduct relevant here.[23] Q Link and Hello Mobile are wholly owned by Florida-based Quadrant Holdings Group LLC (Quadrant), which in turn is wholly owned by Quadrant's Chief Executive Officer, Mr. Issa Asad.[24] In addition, Mr. Asad is listed as the CEO for both Q Link and Hello Mobile.[25]

---

[19] *Id.*

[20] The Lifeline program, administered by the Universal Service Administrative Company (USAC) on the Commission's behalf, provides qualifying low-income consumers discounts on voice and/or broadband Internet access service to help ensure that all Americans have access to affordable service. *Bridging the Digital Divide for Low-Income Consumers*, Fifth Report and Order, Memorandum Opinion and Order and Order on Reconsideration, and Further Notice of Proposed Rulemaking, 34 FCC Rcd 10886, 10887, para. 3 (2019); *see also* 47 CFR § 54.401 (describing the Lifeline program).

[21] *See* Q Link Wireless, *About Q Link Wireless*, https://qlinkwireless.com/about-q-link-wireless.aspx (last visited June 8, 2023).

[22] The Affordable Connectivity Program (ACP) provides qualifying low-income households discounted monthly broadband service and a one-time discount of up to $100 on a tablet, desktop computer, or laptop. *See Affordable Connectivity Program*, WC Docket No. 21-450, Second Report and Order, FCC 22-64, at 1-2, para. 3 (2022). *See also* 47 CFR § 54.1803 (describing ACP support amounts). A list of ACP participating providers is available at FCC, Affordable Connectivity Program Providers, https://www.fcc.gov/affordable-connectivity-program-providers (last visited June 8, 2023). Both Companies also participated in the Emergency Broadband Benefit Program, the predecessor to the ACP. Q Link is the subject of a pending Commission enforcement action that proposes a $62 million penalty against the company for apparently violating Emergency Broadband Benefit Program rules by seeking and receiving reimbursement for connected devices in excess of market value. *See Q Link Wireless, LLC*, Notice of Apparent Liability for Forfeiture, DA 23-2, 2023 WL 345342 (Jan. 17, 2023).

[23] *See* 47 U.S.C. § 222; 47 CFR § 64.2003(o) (defining *telecommunications carrier or carrier* for purposes of the rules implementing section 222); 47 U.S.C. §§ 153(51) (providing that "[a] telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services"), 332(c) (providing that a person engaged in the provision of a commercial mobile service shall be treated as a common carrier for purposes of the Act).

[24] Response to Letter of Inquiry, from John T. Nakahata, et al., HWG LLP, Counsel to Q Link Wireless LLC, to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, at 1-2, Response to Inquiry 1 (Feb. 7, 2022) (on file in EB-TCD-00032935) (App LOI Response). We note Quadrant's registration on the Commission's Form 499 Filer Database, as well as registrations in both Delaware and Florida, list the company as "Quadrant Holdings Group, LLC", while the App LOI Response list them as "Quadrant Holdings LLC," and Quadrant's website names the entity "Quadrant Holdings, LLC." We also note that Hello Mobile's registration in Florida lists the company as "Hello Mobile Telecom LLC."

[25] *See* FCC Form 499 Filer Database, Q Link Wireless LLC, https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=829223 (last visited June 8, 2023); FCC Form 499 Filer Database, Hello Mobile Telecom LLC, https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=832680 (last visited June 8, 2023).

12. The Companies provide online access to CPNI through their respective websites and the My Mobile Account app (App). Through the Q Link website (Website), Q Link customers can log in to their account to "complete an order, upload documents, view order status, check usage, refill account or recertify."[26] Q Link describes the App as a user's "on-the-go hub to monitor and enjoy every aspect of your account with Q Link," including the ability to "view a detailed report of your monthly usage" and "add more minutes and data at any time with just the click of a button."[27] As explained in more detail below in the Discussion section, some of the information that customers can access through both the Website and the App constitutes CPNI. As such, those platforms are subject to the Commission's rules governing customers' online access to their CPNI and proper customer authentication methods.

13. On April 9, 2021, the Ars Technica website published an article claiming that a security flaw in the App potentially exposed the private information of an unknown number of Q Link subscribers.[28] Consequently, the Telecommunications Consumers Division (TCD) of the Commission's Enforcement Bureau's (Bureau) opened an investigation (App Investigation). On December 3, 2021, TCD issued an initial Letter of Inquiry (App LOI) to Quadrant, directing Quadrant and the Companies to provide information and documents regarding the Companies' duty to protect CPNI and other proprietary information under section 222 of the Act and section 64.2010 of the Commission's rules.[29] TCD then issued a supplemental LOI (App SLOI) on June 10, 2022, that directed Quadrant and the Companies to provide detailed information regarding the App login, authentication, and account access features.[30] The responses to these inquiries[31] were not complete or, with regard to the response to the supplemental LOI, timely. As a result, the Bureau issued a Notice of Apparent Liability (NAL) proposing a $100,000 forfeiture against Quadrant, Q Link, and Hello Mobile for apparently violating section 503(b)(1)(B) of the Act by failing to respond to a Commission order.[32]

14. TCD's review of Quadrant and the Companies' joint responses in the App Investigation indicated that some of the Companies' customer authentication practices may violate the CPNI Rules. As described in more detail below, the Companies apparently made impermissible use of readily available

[26] Q Link Wireless, *My Q Link Login*, https://qlinkwireless.com/members/Login.aspx (last visited June 8, 2023).

[27] Q Link Wireless, *What is My Mobile Account?*, https://support.qlinkwireless.com/what-is-my-mobile-account/ (last visited June 8, 2023).

[28] *See* Dan Goodin, *No password required: Mobile carrier exposes data for millions of accounts* (Apr. 9, 2021), https://arstechnica.com/information-technology/2021/04/no-password-required-mobile-carrier-exposes-data-for-millions-of-accounts/.

[29] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Issa Asad, CEO, Quadrant Holdings Group LLC (Dec. 3, 2021) (on file in EB-TCD-21-00032935 (erroneously captioned EB-TCD-00032200)) (App LOI). This LOI was addressed to Quadrant, but directed Quadrant, Q Link, and Hello Mobile to answer the inquiries. Quadrant and the Companies provided a single, joint response to this LOI, as well as to the supplemental LOI issued in the App Investigation.

[30] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to John T. Nakahata, Counsel to Q Link Wireless LLC (June 10, 2022) (on file in EB-TCD-00032935 (erroneously captioned EB-TCD-21-00032200)) (App SLOI). Similar to the App LOI, this SLOI directed Quadrant, Q Link, and Hello Mobile to answer the inquiries; they did so in a single, joint response.

[31] App LOI Response; Supplemental Response to Letter of Inquiry, from John T. Nakahata, et al., HWG LLP, Counsel to Q Link Wireless LLC, to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau et al. (Mar. 31, 2022) (on file in EB-TCD-21-00032935) (App LOI Supplemental Response); Response to Supplemental Letter of Inquiry, from John T. Nakahata, et al., HWG LLP, Counsel to Q Link Wireless LLC, to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau et al. (Aug. 8, 2022) (on file in EB-TCD-21-00032935) (App SLOI Response).

[32] *Quadrant Holdings LLC; Q Link Wireless LLC; Hello Mobile LLC*, Notice of Apparent Liability for Forfeiture, DA 22-825, 2022 WL 3339390 (EB Aug. 5, 2022).

biographical information and account information to authenticate online users.[33] Accordingly, TCD opened a separate investigation into the Companies' authentication practices (Authentication Investigation). On November 4, 2022, TCD issued an initial LOI (Authentication LOI)[34] in connection with the new investigation, followed by a supplemental LOI (Authentication SLOI)[35] on March 1, 2023, seeking additional and updated information. Q Link submitted responses on December 5, 2022, and March 15, 2023, respectively.[36]

15. The Companies' responses to the letters of inquiry explained what information customers can access through their accounts via the Website and the App, the methods that the Companies deployed to verify customers, and (at least for the App) some numbers related to how many customers logged in. According to the Companies, Q Link customers who successfully log in to their account via the Website can access a variety of information about their account, profile, and usage. This information includes {[[redacted]]}[37] and voice and SMS usage data.[38] Similarly, the "App allows account holders to check and 'top up' their balances, review recent voice, text, and data-usage history,"[39] and "monitor . . . every aspect of [their] account . . . ",[40] and is described as "complete account management in the palm of your hand."[41] The Website's initial login process differs from the App's initial login process. According to the Q Link Website, new customers are "directed to the National Verifier website" to verify their Lifeline eligibility; once that process is complete, they are "redirected back to Q Link's Members page to login to [their] account."[42] After this initial login, customers have the

[33] *See* App SLOI Response at 4-5, Response to Inquiry No. 1.

[34] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Issa Asad, CEO, Quadrant Holdings Group LLC (Nov. 4 2022) (on file in EB-TCD-22-00034450) (Authentication LOI). This LOI was addressed to Issa Asad as CEO of Quadrant, and directed Hello Mobile, Q Link, and Quadrant to answer the inquiries. Quadrant and the Companies submitted a single, joint response to the Authentication LOI, as well as to the supplemental LOI issued in the Authentication Investigation.

[35] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to John T. Nakahata, Counsel to Q Link Wireless LLC (Mar. 1, 2023) (on file in EB-TCD-22-00034450) (Authentication SLOI). Similar to the Authentication LOI, this SLOI directed Quadrant, Q Link, and Hello Mobile to answer the inquiries; they did so in a single, joint response.

[36] Response to Letter of Inquiry, from Patrick O'Donnell et al., HWG LLP, Counsel to Q Link Wireless LLC, to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau et al. (Dec. 5, 2023) (on file in EB-TCD-22-00034450) (Authentication LOI Response); Response to Letter of Inquiry, from Patrick O'Donnell et al., Counsel to Q Link Wireless LLC, to Shana Yates, Deputy Chief, Telecommunications Consumer Division, FCC Enforcement Bureau et al. (Mar. 15, 2023) (on file in EB-TCD-22-00034450) (Authentication SLOI Response).

[37] Material set off by double brackets {[ ]} is confidential and is redacted from the public version of this document.

[38] *See* Q Link Wireless, *How do I check my minutes or data balance?*, https://support.qlinkwireless.com/how-do-i-check-my-minutes-or-data-balance/ (last visited June 8, 2023); Authentication LOI Response at 9-11, Response to Inquiry No. 7.

[39] App LOI Response at 4-5, Responses to Inquiry No. 5(a) and 5(h).

[40] Q Link Wireless, *What is My Mobile Account?*, https://support.qlinkwireless.com/what-is-my-mobile-account/ (last visited June 8, 2023). *See also* App SLOI Response at 7-8, 11-12, Responses to Inquires No. 7 and 15 (information that authenticated customers can access via the App includes "{[[redacted]]}.").

[41] Apple App Store, *My Mobile Account App Store Preview*, https://apps.apple.com/us/app/my-mobile-account/id1408895511 (last visited June 8, 2023).

[42] *See* Q Link Wireless, *What do I need to do to complete my application using National Verifier?*, https://support.qlinkwireless.com/what-do-i-need-to-do-to-complete-my-application-using-national-verifier/ (last visited June 8, 2023).

option to create a unique password or leave in place the default password, which is the customer's {[ ]}[43] According to the Companies, an initial login to the App requires customers to enter their {[ ]}.[44] Like the Website, a customer {[ ]} after their initial login to the App.[45] As to how many customers performed an initial login to the Website or the App, the Companies {[ ]} and so did not produce any information about the number of initial Website logins.[46] However, the Companies reported a total of {[ ]} initial logins to the App between August 2022 and January 2023.[47]

16. The Companies also explained the methods it uses for authentication when a customer forgets their password. When a customer loses or forgets their password, that customer can log in via the "Forgot Your Login?" section of the Website. When a customer selects "Forgot Your Login?", the customer is logged in to their account after the customer enters their {[ ]}[48] In the alternative, a customer may reset their password by selecting the "{[ ]}" option on the Website.[49] If a customer selects "{[ ]}", the customer's password is reset after the customer enters their {[ ]}.[50] As noted above, the Companies do "{[ ]}"[51] and thus did not produce relevant data pertaining to the number of customers who have logged in to their account via the Website after forgetting their password. According to the Companies, customers cannot {[ ]} through the App.[52] Via the App, customers {[ ]} by {[ ]}[53]

[43] *See* Q Link Wireless, {[ ]} (last visited June 8, 2023) ("{[ ]}."). *See also* Authentication LOI Response at 5-6, Response to Inquiry No. 1; *see also* App LOI Supplemental Response at 5-6, Response to Inquiry 5(g).

[44] App SLOI Response at 4-5, Response to Inquiry 1. *See also* My Mobile account, *Account Login* (last visited June 8, 2023) (screenshot on file in EB-TCD-22-00034450) (login screen prompts user to enter "{[ ]}").

[45] *Id.* at 4-5, Response to Inquiry No. 1.

[46] Authentication LOI Response at 18, Response to Inquiry No. 18.

[47] Authentication SLOI Response at 6-7, Response to Inquiry No. 4.

[48] *See* Q Link Wireless, {[ ]} (last visited June 8, 2023) ("{[ ]}"). *See also* Authentication LOI Response at 7-8, Response to Inquiry No. 4.

[49] Authentication LOI Response at 7-8, Response to Inquiry No. 4.

[50] *Id.* We note that this system was described in the Companies' December 5, 2022, Authentication LOI Response. At some point after that response, the Website appears to have been changed (*see* Q Link, *My Q Link Login*, https://qlinkwireless.com/members/Login.aspx (last visited June 8, 2023)), removing prompts that the customer (if they had forgotten their login) supply {[ ]}. However, on another portion of the Website the previous "{[ ]}" still appears to be available, prompting the user to enter their {[ ]} (last visited June 8, 2023)).

[51] Authentication LOI Response at 18, Response to Inquiry No. 18.

[52] App LOI Supplemental Response at 5-6, Response to Inquiry No. 5(g).

[53] App SLOI Response at 5-6, Response to Inquiry No. 3. In their response, the Companies did not describe the information required by customer service to reset customers' passwords.

III. DISCUSSION

17. We find that the Companies apparently willfully and repeatedly violated section 64.2010 of the Commission's rules and section 222 of the Act. Three specific provisions of section 64.2010 of the Commission's rules are at issue in this investigation: section 64.2010(a) regarding "reasonable measures" to protect CPNI;[54] section 64.2010(c) regarding online access to CPNI;[55] and section 64.2010(e) regarding password establishment and resets.[56] Among the latter two provisions, two common elements exist: (1) customer authentication requirements, and (2) restrictions on the use of account information and readily available biographical information for authentication purposes. Ultimately, section 64.2010 of the Commission's rules sets baseline requirements for carriers to safeguard CPNI. The Companies' apparent failure to comply with these minimum standards has put their customers' personal information at risk of misappropriation, breach, and unauthorized access and disclosure.

A. The Companies Apparently Willfully and Repeatedly Violated Section 64.2010(a) of the Commission's Rules and Section 222 of the Act

18. We find that the Companies' methods for controlling access to CPNI apparently violate the requirement to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" set forth in section 64.2010(a) of the Commission's rules,[57] as well as section 222 of the Act (which requires carriers to protect customer information).[58] The obligation to employ "reasonable measures" to protect CPNI is an overarching responsibility that applies to each carrier and that is separate and independent from the more specific requirements in the CPNI rules regarding customer authentication. As the Commission stated when section 64.2010(a) was adopted, "[w]e fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[59]

19. Here, the Companies failed to meet that expectation because they made CPNI accessible to effectively any party who knew—or could obtain—a customer's readily available biographical information or account information – namely a customer's {[[redacted]]}[60] On the App, the customer's username was account information (their {[[redacted]]}) and the customer's password was set by default to biographical information (their {[[redacted]]}).[61] Moreover, the Companies placed consumers' CPNI at even greater risk by not requiring customers to {[[redacted]]} biographical information ({[[redacted]]}) as the password indefinitely.[62] The types of biographical and account information at issue here (namely {[[redacted]]}) are often widely known and easily obtainable, and {[[redacted]]} only exacerbates the issue. These practices plainly do not constitute reasonable data security measures and therefore violate both section 64.2010(a) of the CPNI rules and section 222 of the Act,[63] which establishes carriers' duties for protecting customer information. However, as discussed in more detail below in the Proposed Forfeiture section, we decline at this time to propose a penalty for the Companies' apparent violations of section 64.2010(a) and section 222.

---

[54] 47 CFR § 64.2010(a).

[55] *Id.* § 64.2010(c).

[56] *Id.* § 64.2010(e).

[57] *Id.* § 64.2010(a).

[58] 47 U.S.C. § 222.

[59] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[60] *See* App SLOI Response at 4-5, Response to Inquiry No. 1.

[61] *Id.*

[62] *Id.*

[63] 47 U.S.C. § 222.

Nonetheless, assessing a proposed penalty for such practices is within our authority and we may do so in future cases.

B. The Companies Apparently Willfully and Repeatedly Violated Section 64.2010(c) of the Commission's Rules

20. The Companies' practice of using customer readily available biographical information and account information (i.e., {[ ]}) as a default method to authenticate users apparently violates section 64.2010(c) of the Commission's CPNI Rules. Section 64.2010(c) of the Commission's rules provides that:

> [a] telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.[64]

21. *The Website and App Provide Online Access to CPNI*. The Q Link Website allows customers to access a variety of information about their account, profile, and usage. This information includes {[ ]} and voice and SMS usage data.[65] A number of these data elements (including, at a minimum, usage information such as {[ ]}) constitute CPNI, as they relate to the "quantity, . . . type, destination, location, and amount of use" of a telecommunications service.[66] The App provides access to customers' usage history, allowing customers to check their balances[67] and "monitor . . . every aspect of [their] account."[68] Similarly, the App also enables users to review, among other things, their {[ ]}[69] These categories of usage information also satisfy the definition of CPNI because they relate to the "quantity" or "amount of use" of a telecommunications service.[70]

22. *The App Impermissibly Relies Upon Readily Available Biographical Information and Account Information to Authenticate Customers.* According to Q Link's responses to the App SLOI, when a customer initially logs in to the App, they must enter account information—specifically, their {[ ]}—and password to access their account.[71] Unless a customer has opted to change their password, it continues to be the customer's default password, namely their {[ ]}. Upon accessing

[64] 47 CFR § 64.2010(c).

[65] *See* Q Link Wireless, *How do I check my minutes or data balance?*, https://support.qlinkwireless.com/how-do-i-check-my-minutes-or-data-balance/ (last visited June 8, 2023); Authentication LOI Response at 9-11, Response to Inquiry No. 7 (accessible information included {]}).

[66] 47 U.S.C. § 222(h)(1)(A).

[67] App LOI Response at 4-5, Responses to Inquiry No. 5(a) and 5(h).

[68] Q Link Wireless, *What is My Mobile Account?*, https://support.qlinkwireless.com/what-is-my-mobile-account/ (last visited June 8, 2023). *See also* App SLOI Response at 7-8, 11-12, Responses to Inquires No. 7 and 15 (information that authenticated customers can access via the App includes "{[ ]} which Q Link defines to include {[ ]}).

[69] App SLOI Response at 11-12, Response to Inquiry No. 15.

[70] 47 U.S.C. § 222(h)(1)(A).

[71] App SLOI Response at 4-5, Response to Inquiry No. 1.

their accounts, customers are {[[redacted]]}[72] Thus, any customer that does not change their password from the default, is required to use biographical information (their {[[redacted]]}) as a password to log in.[73]

23. A customer's {[[redacted]]} qualifies as "readily available biographical information" as it "is information drawn from the customer's life history."[74] Both the CPNI Rules and the 2007 CPNI Order identify a customer's {[[redacted]]} as an example of readily available biographical information.[75] Because a person's {[[redacted]]} is part of their {[[redacted]]} and is information easily associated with their life history, it constitutes readily available biographical information. Likewise, the {[[redacted]]} associated with a customer's account is "account information" pursuant to the CPNI Rules.[76]

24. By requiring some customers (specifically, those who did not choose to reset their password from the default) to enter account information and readily available biographical information (in the form of their {[[redacted]]}) to initially log in to the App, the Companies have failed to "authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI."[77] Further, by establishing a login process in which customers' default passwords—which many, if not most, customers will not change—consist of readily available biographical information—the Companies have failed to grant online access to CPNI "only . . . through a password . . . that is not prompted by the carrier asking for readily available biographical information, or account information."[78] Accordingly, the Companies apparently violated section 64.2010(c) of the Commission's rules in connection with their authentication process for the App—a violation that was repeated each time a customer was permitted to log in using their default password.

[72] App SLOI Response at 4-5, Response to Inquiry No. 1. In one of the Companies' prior responses, they claimed that {[[redacted]]} suggesting that in some instances an initial login to the App might not require use of a default password. App LOI Supplemental Response at 5-6, Response to Inquiry No. 5(g).

[73] Many consumers do not set secure passwords on their accounts unless a company requires them to do so. Given that 80% of hacking-related breaches are linked in some way to passwords, it is imperative that companies require secure passwords. *See* Aimee O'Driscoll, *25+ Password statistics (that may change your password habits)*, comparitech (Mar. 24, 2023), https://www.comparitech.com/blog/information-security/password-statistics/. In fact, a survey of 2500 consumers revealed that "35 percent of people never change their passwords; they only do it if they're prompted." Angela Moscaritolo, *35 Percent of People Never Change Their Passwords*, PCMag (updated July 20, 2018), https://www.pcmag.com/news/35-percent-of-people-never-change-their-passwords. Other surveys show that up to 44% of consumers worldwide only "rarely" reset passwords and that 15% of owners with "internet of things" devices do not change their default passwords. *See* Statista, *Frequency of resetting passwords worldwide in 2022* (Mar. 31, 2023), https://www.statista.com/statistics/1303484/frequency-of-password-resets-worldwide; Catalin Cimpanu, *15% All IoT device Owners Don't Change Default Passwords*, Bleeping Computer (June 19, 2017), https://www.bleepingcomputer.com/news/security/15-percent-of-all-iot-device-owners-dont-change-default-passwords/.

[74] 47 CFR § 64.2003(m).

[75] *See id.* § 64.2003(m); *2007 CPNI Order* at 6937, para. 15 n.55.

[76] 47 CFR § 64.2003(a).

[77] *Id.* § 64.2010(c). As discussed earlier, the Companies employ a different process for the Website, where customers are authenticated through {[[redacted]]}.

[78] *Id.*

C. Q Link's Password Reset Method on the Website Apparently Violated Section 64.2010(e) of the Commission's Rules

25. The method through which Q Link customers can access their accounts on the Website, and reset their passwords, in the case of lost or forgotten login credentials apparently violates section 64.2010(e) of the CPNI Rules. Namely, the rule provides in relevant part:

> Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information.[79]

26. A customer who claims to have forgotten their password can access their account on the Website by using a combination of certain readily available biographical information—their {[ ]}[80] They can also reset their password by using a combination of their {[ ]}.[81] As discussed above, a customer's {[ ]} constitute readily available biographical information; the CPNI Rules also identify a customer's {[ ]} as readily available biographical information.[82] The use of such information plainly violates the requirement that any back-up authentication method used by a carrier in the event of a lost or forgotten password "not prompt the customer for readily available biographical information, or account information."[83] Therefore, Q Link apparently violated section 64.2010(e) of the Commission's rules with respect to the alternative account access and password reset processes for the Website.

D. Proposed Forfeiture

27. Section 503(b)(1)(B) of the Act authorizes the Commission to impose a forfeiture against any entity that "willfully or repeatedly fail[s] to comply with any of the provisions of [the Act] or of any rule, regulation, or order issued by the Commission under [the Act]."[84] Here, section 503(b)(2)(B) of the Act authorizes us to assess a forfeiture against common carriers of up to $237,268 for each day of a continuing violation, up to a statutory maximum of $2,372,677 for a single act or failure to act.[85] In exercising our forfeiture authority, we must consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[86] In addition, the Commission has established

---

[79] *Id.* § 64.2010(e).

[80] *See* Q Link Wireless, {[ ]} (last visited June 8, 2023) ("{[ ]}."); *see also* Authentication LOI Response at 7-8, Response to Inquiry No. 4.

[81] Authentication LOI Response at 7-8, Response to Inquiry No. 4. But note, this system appears to have been changed since the Companies submitted their Authentication LOI Response in December 2022. *See infra* note 50.

[82] 47 CFR § 64.2003(m).

[83] *Id.* § 64.2010(e).

[84] 47 U.S.C. § 503(b)(1)(B).

[85] *Id.* § 503(b)(2)(B) (authorizing a forfeiture of up to $100,000 against a common carrier, which amount is subject to adjustment for inflation); *see* 47 CFR § 1.80(b)(11), Table 5 to paragraph (b)(11)(ii) (stating the current statutory maximum forfeiture amounts, including the adjusted amount for section 503(b)(2)(B)); *see also* 47 CFR § 1.80(b)(2); *Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 22-1356, 2022 WL 18023008 (EB Dec. 23, 2022); *Annual Adjustment of Civil Monetary Penalties to Reflect Inflation*, 88 Fed. Reg. 783 (Jan. 5, 2023) (setting January 15, 2023 as the effective date for the increases).

[86] 47 U.S.C. § 503(b)(2)(E).

forfeiture guidelines that contain base penalties for certain violations and identify criteria that we consider when determining the appropriate penalty in any given case.[87] Under these guidelines, we may adjust a base forfeiture upward based on seven listed criteria—including for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator—or downward based on four listed criteria.[88]

28. The Commission's forfeiture guidelines do not establish a base forfeiture for violations of section 222 of the Act or the accompanying CPNI Rules. Nor has the Commission previously calculated forfeitures for violations of section 64.2010(c) or section 64.2010(e). Thus, we look to the forfeitures established or issued in analogous cases for guidance.

29. *Prior Commission Cases*. The Commission has a history of investigations and enforcement actions aimed at consumer protection generally, and the privacy of customer information specifically. In 2014, the Commission issued a Notice of Apparent Liability against TerraCom, Inc. and YourTel America, Inc., for apparently violating section 222(a) of the Act.[89] In *TerraCom*, the carriers' failure to reasonably secure their computer systems exposed the sensitive personal information of individual Lifeline program applicants. The Commission found that "[e]ach unprotected document [containing customer information] constitutes a continuing violation."[90] The Commission noted that even assuming each affected customer only had one unprotected document, it would still amount to 305,065 violations.[91] The Commission noted that it had used a $29,000 base forfeiture per violation in prior CPNI cases, but after considering the large number of apparent violations (over 300,000) and the massive forfeiture amount that would result by multiplying these numbers, it instead proposed a penalty of $8,500,000 for the section 222 violations in that case as "sufficient to protect the interests of consumers and to deter future violations of the Act."[92] The Commission noted:

> In determining the proper forfeiture . . . we are guided by the principle that the protection of consumer [proprietary information] is a fundamental obligation of all telecommunications carriers. Consumers are increasingly concerned about their privacy and the security of the sensitive, personal data that they must entrust to service providers of all stripes. Given the increasing concern about the security of personal data, we must take aggressive, substantial steps to ensure that carriers implement necessary and adequate measures to protect consumers' [proprietary information].[93]

In other contexts involving consumer protections under the Act and the Commission's rules, the Commission has applied a base forfeiture of $40,000 for a single act.[94] Such a base forfeiture (whether in a privacy context or more generally in a consumer protection context) appropriately deters wrongful conduct and – where consumer data is concerned – reflects the increased risk consumers face when their

[87] 47 CFR § 1.80(b)(10), Note 2 to paragraph (b)(10) (*Guidelines for Assessing Forfeitures*). Table 1 to paragraph (b)(10) lists base forfeiture amounts for section 503 forfeitures and Table 3 to paragraph (b)(10) lists the upward and downward adjustment criteria for section 503 forfeitures.

[88] 47 CFR § 1.80(b)(10), Table 3 to paragraph (b)(10).

[89] *TerraCom, Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture*, 29 FCC Rcd 13325 (2014) (*TerraCom*).

[90] *Id.* at 13343, para. 50.

[91] *Id.* at 13343, para. 50.

[92] *Id.* at 13343, para. 52.

[93] *Id.* at 13341-42, para. 46.

[94] *See, e.g.*, *Advantage Telecommunications Corp*., Forfeiture Order, 32 FCC Rcd 3723 (2017); *Preferred Long Distance, Inc*., Forfeiture Order, 30 FCC Rcd 13711 (2015).

information is not secured in a timely manner. When applied in cases involving the CPNI rules, the $40,000 base forfeiture also provides consistency with other consumer protection and privacy cases involving serious risk of harm to consumers.

30. *Applying Commission Precedent and the Statutory Factors to the Companies*. In this case, we find that each time the Companies used readily available biographical information or account information either to authenticate a customer or carry out a password reset—whether on the Website or via the App—constitutes a separate violation of section 64.2010 of the Commission's rules for which a forfeiture may be assessed. We further find that, as in other consumer protection and privacy cases, a $40,000 base forfeiture for violations of section 64.2010 of the Commission's rules is appropriate. The record shows that at least {[[redacted]]} unique customers initially logged in to the App during the period within the statute of limitations of this case.[95] As discussed earlier, each such login in which a customer used their default password constituted a violation of section 64.2010(c) of the Commission's rules because it involved authentication using readily available biographical information or account information (i.e., the customer's {[[redacted]]}). Likewise, each time a customer was permitted to use readily available biographical information to reset their password on the Website constitutes a separate apparent violation of 64.2010(e) of the Commission's rules.

31. To the extent that customers modified their passwords after establishing their accounts via the Website, yet before initially logging in to the App, the App logins would not necessarily have constituted violations of section 64.2010(c) of the Commission's rules. The record, however, does not reflect how many such customers there may have been because the Companies do not track information related to how many customers maintained their default passwords, nor how many selected a new password.[96] Similarly, the Companies were not able to respond to requests for information about the number of customers that reset their passwords on the Website.[97]

32. Accordingly, we conservatively find that there were at least 500 apparent violations of section 64.2010(c)[98] of the Commission's rules during the relevant time period—which, at a $40,000 base forfeiture, results in a proposed penalty of $20,000,000. This tally of apparent violations is amply grounded in the record and falls well under the maximum number that the Commission could reasonably identify, given that it represents less than {[[redacted]]}% of the {[[redacted]]} App logins that occurred here.[99]

33. As discussed earlier, we also find that the Companies' use of readily available biographical information and account information to control online access to CPNI is apparently a patently insecure practice inconsistent with section 222 of the Act and the "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" requirement of section 64.2010(a) of the Commission's rules.[100] Notwithstanding this failure to employ "reasonable measures" to protect CPNI, given that the other apparent violations of section 64.2010 for which we are proposing a forfeiture in this case more than justify the proposed penalty, we decline at this time to propose an

[95] Authentication SLOI Response at 6-7, Response to Inquiry No. 4 (reporting a total of {[[redacted]]} initial logins to the App between August 2022 and January 2023).

[96] Authentication LOI Response at 19, Response to Inquiry No. 21.

[97] *Id.* at 18, Response to Inquiry No. 18 (stating that the they do "not count or maintain records of website logins").

[98] Given the apparent violations related to the App upon which we base the proposed forfeiture, as well as the Companies' lack of records pertaining to Website authentication, we have declined to estimate the number of additional Website-related violations arising under 64.2010(e). Nonetheless, we underscore that the Companies' failure to keep such records does not absolve them of responsibility for those apparent violations nor prevent the Commission from making such an estimation in the future (whether related to violations of 64.2010(e) or to other violations where any company has failed to maintain records). Poor recordkeeping is no shield to liability.

[99] This finding is further supported by the statistics related to consumer password practices (suggesting significant numbers of people do not change their passwords). *See supra* note 73.

[100] 47 U.S.C. § 222; 47 CFR § 64.2010(a).

additional penalty under section 64.2010(a) of the Commission's rules or section 222 of the Act. Nevertheless, the Commission has the authority to and may impose a penalty for such a practice in future cases.

34. In determining the appropriate forfeiture amount in the instant case, we have considered the factors enumerated in section 503(b)(2)(E) of the Act, including the "the nature, circumstances, extent, and gravity of the violation, and with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other factors as justice may require."[101] Several factors lead us to believe that a substantial forfeiture—as reflected in the proposed amount of $20,000,000—is warranted for the Companies' apparent violations of section 64.2010 of the Commission's rules.

35. The current matter deals with violations of the Commission's rules regarding customer authentication. Here, the Commission has unambiguous rules requiring that customers be authenticated before accessing their CPNI online.[102] These rules are explicit that authentication may not hinge on a customer's account information or readily available biographical information.[103] The Companies in this matter apparently failed to comply with these explicit requirements, and as a result, placed the CPNI of their customers at risk.

36. We further note that, as a Lifeline provider and provider in the Affordable Connectivity Program, Q Link markets and offers its services primarily to low-income consumers. As the Commission observed in *TerraCom*, this is "an already vulnerable population"[104]—the Companies' approximately {[[redacted]]} subscribers[105] should not be subject to weaker privacy protections than other Americans, or forced to choose between safeguarding their personal data and obtaining access to vital communications services.[106]

37. The proposed forfeiture also is well within applicable statutory limits. As noted, section 503(b)(2)(B) of the Act authorizes us to assess a forfeiture against the Companies of up to $237,268 for each violation or each day of a continuing violation, up to a statutory maximum of $2,372,677 for a single act or failure to act.[107] Although we have conservatively grounded the proposed forfeiture in a finding of at least 500 apparent violations, the record reflects at least {[[redacted]]} initial logins to the App between August 2022 and January 2023—each of which is a presumptive violation of section 64.2010(c) of the Commission's rules.[108] As such, the proposed forfeiture is well under the limits established by section 503(b)(2)(B) of the Act.

---

[101] 47 U.S.C. § 503(b)(2)(e).

[102] 47 CFR § 64.2010.

[103] *Id.* § 64.2010(c), (e).

[104] *TerraCom*, 29 FCC Rcd at 13343, para. 51.

[105] Authentication LOI Response at 16, Response to Inquiry No. 16 (noting that for each month between August and October 2022, Q Link had in excess of {[[redacted]]} subscribers and Hello Mobile had in excess of {[[redacted]]} subscribers).

[106] Some scholars have found that low-income Americans are especially vulnerable to identity theft and other harms associated with data breaches. *See* Greene, Sara S., "Stealing (Identity) From the Poor," (2021). *Minnesota Law Review*. 3295. https://scholarship.law.umn.edu/mlr/3295.

[107] *See* 47 U.S.C. § 503(b)(2)(B); 47 CFR § 1.80(b)(2). These amounts reflect the inflationary adjustments to the forfeitures specified in section 503(b) of the Act. See *Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 21-1631, 2021 WL 6135287 (EB Dec. 22, 2021).

[108] In quantifying apparent violations, we have looked to the information the Companies produced regarding how many of the Companies' customers actually obtained online access to CPNI or reset their passwords through methods that did not meet the requirements of sections 64.2010(c) and (e) of the Commission's rules. We note, however, that the Companies' reliance on readily available biographical information and account information for

(continued…)

38. Therefore, after applying the Commission's *Guidelines for Assessing Forfeitures*, section 1.80 of the Commission's rules, and the statutory factors in section 503(b)(2)(E), we propose a total forfeiture of $20,000,000 for which the Companies are apparently liable.[109]

E. We Propose to Hold the Companies Jointly and Severally Liable for the Apparent Violations.

39. We propose to hold Q Link and Hello Mobile jointly and severally liable for the apparent violations. "Related companies operating in common enterprise or as a single business entity may be held jointly liable for wrongful conduct."[110] Courts have identified several factors to determine the existence of a single business entity or a common enterprise, including whether the companies: (1) operate under common control, (2) share office space, (3) share employees, (4) commingle funds, and (5) coordinate advertising.[111] Companies that operate as a common enterprise can be held jointly and severally liable for each other's actions.[112] The Commission has taken a similar approach in previous enforcement actions.[113]

40. Here, the business operations of Q Link and Hello Mobile significantly overlap such that we find that they apparently operate as a common enterprise. Both Companies are wholly owned by Quadrant Holdings Group, LLC,[114] and Issa Asad holds management roles in both companies' operations.[115] Hello Mobile apparently only has one employee, presumably, Mr. Asad, and states that it

---

customer authentication jeopardized the security of all of their customers' CPNI (to the extent that information was vulnerable to effectively any third party who knew a customer's {[ ]}). Thus, in future cases involving authentication practices under section 64.2010, we may look more expansively when calculating violations and setting a forfeiture, and take into account the full universe of customers whose data was placed at risk.

[109] Any entity that is a "Small Business Concern" as defined in the Small Business Act (Pub. L. 85-536, as amended) may avail itself of rights set forth in that Act, including rights set forth in 15 U.S.C. § 657, "Oversight of Regulatory Enforcement," in addition to other rights set forth herein.

[110] *Thomas Dorsher; Charitel Inc; Ontel Inc; Scammerblaster Inc*, Notice of Apparent Liability for Forfeiture, FCC 22-57 at 15, 2022 WL 2805894 *11, para. 33 (July 14, 2022) (citing *Continental Cas. Co. v. Symons*, 817 F.3d 979, 993-94 (7th Cir. 2016); *Sunshine Art Studios, Inc. v. FTC*, 481 F.2d 1171, 1175 (1st Cir. 1973); *Delaware Watch Co. v. FTC*, 332 F.2d 745, 746-47 (2d Cir. 1964); *FTC v. PayDay Financial LLC*, 989 F.Supp.2d 799, 809 (D.S.D. 2013)).

[111] *See FTC v. On Point Capital Partners LLC*, 17 F.4th 1066, 1081-82 (11th Cir. 2021) (adopting the test previously adopted by the Sixth Circuit in *FTC v. E.M.A. Nationwide, Inc*., 767 F.3d 611, 636-37 (6th Cir. 2014)); *FTC v. Lanier Law, LLC*, 715 Fed. Appx. 970, 979-80 (11th Cir. 2017)); *CFTC v. Trade Exch. Network Ltd*., 117 F. Supp.2d 29, 38-39 (D.D.C. 2015) (adopting the test in *FTC v. E.M.A. Nationwide*).

[112] *See On Point*, 17 F.4th at 1081; *FTC v. E.M.A. Nationwide*, 767 F.3d at 637.

[113] *See Sumco Panama SA, et al.*, Notice of Apparent Liability for Forfeiture, FCC 22-99, 2022 WL 17958841 at *24-28, paras. 82-96 (rel. Dec. 23, 2022); *ScammerBlaster Notice of Apparent Liability for Forfeiture*, FCC 22-57 at 15-17, paras. 33-34 (holding related companies liable as a single business entity); *see also Rising Eagle Forfeiture Order*, 36 FCC Rcd at 6254, para. 55 (holding related companies liable due to the misconduct of their common directors).

[114] App LOI Response at 1-2, Response to Inquiry No. 1.

[115] *Id.* at 2, Response to Inquiry No. 1 (stating that Issa Asad is "Q Link's only Manager and corporate officer as defined in the Company's Operating Agreement."); Florida Department of State Division of Corporations, *Detail by Entity Name*, Hello Mobile Telecom LLC, https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResultDetail?inquirytype=EntityName&directionType=Initial&searchNameOrder=HELLOMOBILETELECOM%20M180000067631&aggregateId=forl-m18000006763-3feb2ac1-686c-4c69-a18d-56a57ee7147d&searchTerm=hello%20%20mobile&listNameOrder=HELLOMOBILEMEDIA%20L150000294100 (last visited June 8, 2023) (identifying Issa Asad as a Manager). In addition, Mr. Asad is listed as the CEO of both Q Link and Hello Mobile in the FCC's Form 499 Filer Database; *see* https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=829223 and https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=832680 (last visited June 8, 2023).

has no officers or directors.[116] The Companies also share resources, including office space[117] and the My Mobile Account App.[118] Moreover, the two telecommunications Companies appear to engage in some coordinated advertising with regards to promotional material for the App.[119] Taken as a whole, these factors indicate that Q Link and Hello Mobile are functionally a single business entity, and the Commission proposes to hold them jointly and severally liable for the proposed forfeiture.

IV. CONCLUSION

41. We have determined that the Companies apparently willfully and repeatedly violated sections 64.2010(a), (c) and (e) of the Commission's rules. As such, the Companies are apparently jointly and severally liable for a forfeiture of $20,000,000.

V. ORDERING CLAUSES

42. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act[120] and section 1.80 of the Commission's rules,[121] Q Link Wireless LLC and Hello Mobile Telecom LLC are hereby **NOTIFIED** of their **APPARENT JOINT AND SEVERAL LIABILITY FOR A FORFEITURE** in the amount of Twenty Million Dollars ($20,000,000) for willful and repeated violations of section 222 of the Act, 47 U.S.C. § 222, and sections 64.2010(a), (c) and (e) of the Commission's rules, 47 CFR § 64.2010(a), (c), (e).

43. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,[122] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, Q Link Wireless LLC and Hello Mobile Telecom LLC **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture consistent with paragraph 46 below.

---

[116] App LOI Response at 1, Response to Inquiry 1.

[117] Quadrant Holdings Group LLC, Q Link Wireless LCC, and Hello Mobile Telecom LLC each have registered with the Florida Department of State and each list the same principal address – 499 East Sheridan Street, Suite 400, Dania Beach, Florida 33004. *See* Florida Department of State Division of Corporations, *Detail by Entity Name*, Quadrant Holdings Group LLC, https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResultDetail?inquirytype=EntityName&directionType=Initial&searchNameOrder=QUADRANTHOLDINGSGROUP%20M120000013480&aggregateId=forl-m12000001348-500f9edb-37d5-4327-b1bb-f06a868ff282&searchTerm=quadrant%20holdings%20group&listNameOrder=QUADRANTHOLDINGSGROUP%20M120000013480 (last visited June 8, 2023); Florida Department of State Division of Corporations, *Detail by Entity Name*, Q Link Wireless LLC, https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResultDetail?inquirytype=EntityName&directionType=Initial&searchNameOrder=QLINKWIRELESS%20M110000051580&aggregateId=forl-m11000005158-aada382b-d2f1-40ba-a7fe-f862b6a21801&searchTerm=q%20link%20wireless&listNameOrder=QLINKWIRELESS%20M110000051580 (last visited June 8, 2023); Florida Department of State Division of Corporations, *Detail by Entity Name*, Hello Mobile Telecom LLC, https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResultDetail?inquirytype=EntityName&directionType=Initial&searchNameOrder=HELLOMOBILETELECOM%20M180000067631&aggregateId=forl-m18000006763-3feb2ac1-686c-4c69-a18d-56a57ee7147d&searchTerm=hello%20%20mobile&listNameOrder=HELLOMOBILEMEDIA%20L150000294100 (last visited June 8, 2023).

[118] App LOI Supplemental Response at 4-8, Response to Inquiry 5. We note that the Companies apparently keep records of the 30-day average number of unique App users. However, such records apparently do not identify how many App users are Q Link customers versus Hello Mobile Customers (the Companies estimate that 97% of its subscriber base is made up of Q Link customers). This overlap in record keeping further suggests that the Companies operate as a single enterprise.

[119] *See*, My Mobile Account, *Convenient App to Manage Your Great Service*, https://mymobileaccount.com/ (last visited June 8, 2023).

[120] 47 U.S.C. § 503(b).

[121] 47 CFR § 1.80.

[122] *Id.* § 1.80.

44. In order for Q Link Wireless LLC and Hello Mobile Telecom LLC to pay the proposed forfeiture, Q Link Wireless LLC and Hello Mobile Telecom LLC shall notify Shana Yates at Shana.Yates@fcc.gov, Michael Epshteyn at Michael.Epshteyn@fcc.gov, and Lauren Merk at Lauren.Merk@fcc.gov of their intent to pay, whereupon an invoice will be posted in the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do. Upon payment, Q Link Wireless LLC and Hello Mobile Telecom LLC shall send electronic notification of payment to Shana Yates at Shana.Yates@fcc.gov, Michael Epshteyn at Michael.Epshteyn@fcc.gov, and Lauren Merk at Lauren.Merk@fcc.gov on the date said payment is made. Payment of the forfeiture must be made by credit card using CORES at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts forfeiture payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[123]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[124] or printed CORES form[125] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[126] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which

[123] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #1).

[124] FCC Form 159 is accessible at https://www fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[125] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps fcc.gov/cores/userLogin.do.

[126] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

45. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 45 L Street, NE, Washington, D.C. 20554.[127] Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

46. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to sections 1.16 and 1.80(g)(3) of the Commission's rules.[128] The written statement must be mailed to the Office of the Secretary, Federal Communications Commission, 45 L Street, NE, Washington, D.C. 20554, ATTN: Enforcement Bureau – Consumer Protection Division, and must include the NAL/Account Number referenced in the caption. The statement must also be emailed to Shana Yates at Shana.Yates@fcc.gov, Michael Epshteyn at Michael.Epshteyn@fcc.gov, and Lauren Merk at Lauren.Merk@fcc.gov.

47. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits the following documentation: (1) federal tax returns for the past three years; (2) financial statements for the past three years prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status.[129] Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation. Inability to pay, however, is only one of several factors that the Commission will consider in determining the appropriate forfeiture, and we retain the discretion to decline reducing or canceling the forfeiture if other prongs of 47 U.S.C. § 503(b)(2)(E) support that result.[130]

48. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by first class mail and certified mail, return receipt requested, to Issa Asad, Chief Executive Officer, Q Link Wireless LLC, 499 East Sheridan Street, Suite 400, Dania, FL 33004; Issa Assad, Chief Executive Officer, Hello Mobile Telecom LLC, 499 East Sheridan Street, Suite 400, Dania, FL 33004; and to John Nakahata, Esq., Counsel for Q Link Wireless LLC and Hello Mobile Telecom LLC, HWG LLP, 1919 M Street NW, Suite 800, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[127] *See* 47 CFR § 1.1914.

[128] 47 CFR §§ 1.16, 1.80(g)(3).

[129] 47 U.S.C. § 503(b)(2)(E).

[130] *See, e.g., Ocean Adrian Hinson, Surry County, North Carolina*, Forfeiture Order, 34 FCC Rcd 7619, 7621, para. 9 & n.21 (2019); *Vearl Pennington and Michael Williamson*, Forfeiture Order, 34 FCC Rcd 770, paras. 18–21 (2019); *Fabrice Polynice, Harold Sido and Veronise Sido, North Miami, Florida*, Forfeiture Order, 33 FCC Rcd 6852, 6860–62, paras. 21–25 (2018); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, 33 FCC Rcd 4663, 4678-79, paras. 44-45 (2018); *Purple Communications, Inc.*, Forfeiture Order, 30 FCC Rcd 14892, 14903-904, paras. 32-33 (2015); *TV Max, Inc., et al.*, Forfeiture Order, 29 FCC Rcd 8648, 8661, para. 25 (2014).