HUNTON
ANDREWS KURTH

BASELOAD

Current Topics in the Power and Utilities Capital Markets



February 2019

Contents

Attacks on the Grid: An Update from the Power Capital Markets

Background

The past three years have witnessed numerous reports in the press regarding both actual and potential cyberattacks on utility assets throughout the world.[1] American investigators concluded that the attack in Ukraine in December 2015 may well have been the first power blackout triggered by a cyberattack.[2]

In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities.[3] According to an article in The Wall Street Journal in July 2018, in part based on statements from federal officials, hackers working for Russia claimed "hundreds of victims" in 2017 in a giant and long-running campaign that put the hackers inside the control rooms of U.S. electric utilities where they could have caused blackouts.[4] Later that month, a senior Department of Homeland Security official tempered this assessment, asserting that while cyberattacks on the U.S. grid are constant, cyber criminals do not currently have the ability to cause large power disruptions.[5] In April 2018, a cyberattack on a shared data network forced four of the nation's natural gas pipeline operators to temporarily shut down computer communications with their customers.[6]

[1] David E. Sanger, *Utilities Cautioned About Potential for a Cyberattack After Ukraine's*, *The New York Times* (Feb. 29, 2016); Ted Koppel, *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, (Oct. 18, 2016); Nicole Periroth and David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*, *The New York Times* (March 15, 2018); Clifford Krauss, *Cyberattack Shows Vulnerability of Gas Pipeline Network*, *The New York Times* (April 4, 2018); Rebecca Smith, *Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say*, *The Wall Street Journal* (July 23, 2018); David E. Sanger, *Russian Hackers Appear to Shift Focus to U.S. Power Grid*, *The New York Times* (July 27, 2018); Latif M. Nurani, *Cybersecurity and the Electric Grid*, *Infrastructure* (Aug. 15, 2018); Peter Kelly-Detwiler, *Cybersecurity; The Hackers Are Already Through the Utilities' Doors, So What's Next?*, FORBES (Dec. 20, 2018); Rebecca Smith and Rob Barry, *America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It*, *The Wall Street Journal* (Jan. 10, 2019); Pedro Pizarro, *Planning for Cyber Incidents*, *Electric Perspectives* (Jan/Feb 2019); Alison Noon, *Utilities Brace For FERC Scrutiny Of Vendor Cybersecurity*, *Law360* (Jan. 25, 2019).

[2] *Id.*

[3] Rebecca Smith and Rob Barry, *America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It*, *The Wall Street Journal* (Jan. 10, 2019).

[4] Rebecca Smith, *Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say*, *The Wall Street Journal* (July 23, 2018).

[5] Gavin Bade, *DHS walks back utility cyber warnings as Southern CEO says no grid emergency*, *Utility Dive* (July 31, 2018).

[6] Clifford Krauss, *Cyberattack Shows Vulnerability of Gas Pipeline Network*, *The New York Times* (April 4, 2018).

In January 2019, The Wall Street Journal published an extensive report detailing the efforts by hackers to compromise the hundreds of contractors and subcontractors that work on the power grid.[7] By planting lines of code on the websites of trade publications, hackers invisibly gained computer usernames and passwords from unsuspecting visitors to such sites. That enabled the hackers to gain access to sensitive systems, according to Homeland Security officials. According to the WSJ report, approximately 60 utilities were targeted (including some outside the United States) and some experts believe the systems of two dozen or more U.S. utilities ultimately were breached.[8]

The SEC has been focused on cybersecurity for some time. In October 2011, the Division of Corporation Finance of the SEC issued disclosure guidance with respect to cybersecurity.[9] The guidance listed specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents, including: risk factors, MD&A, business description, legal proceedings and a registrant's financial statements.

In February 2018, the SEC again published interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.[10] According to the SEC's release, "[t]oday, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century."[11]

In its 2018 guidance, the SEC went into detail as to the nature and extent of a registrant's disclosure obligations with respect to cybersecurity risks and incidents:

> In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations…We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation — which often can be lengthy — would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.[12]

Further, in a December 6, 2018, speech at the School of International and Public Affairs of Columbia University, SEC Chairman Clayton again touched on the SEC's current focus on cybersecurity. He noted that "from an issuer disclosure perspective, it is important that investors are sufficiently informed about the material cybersecurity risks and incidents affecting the companies in which they invest."[13]

[7] Rebecca Smith and Rob Barry, *America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It*, *The Wall Street Journal* (Jan. 10, 2019).

[8] *Id.*

[9] CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

[10] Release Nos. 33-10459; 34-82746, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 26, 2018).

[11] *Id.*, at 2.

[12] *Id.*, at 11-12.

[13] SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks, Chairman Jay Clayton (Dec. 6, 2018).

Power Capital Markets

In the power and utility capital markets, we have witnessed over the past several years an increased focus by all market participants on cybersecurity risks, diligence and disclosure. As suggested in the SEC's 2018 guidance, issuers in the industry are, with few exceptions, including cyber threats in their 1934 Act Risk Factors.

Further, underwriters and their counsel have had some success in adding cyber representations to underwriting agreements (including debt transactions) over the past several years. While many issuers have successfully negotiated to exclude any new cyber representation, we expect these negotiations to continue as participants in the market continue to focus on cyber risks and diligence.

Cybersecurity risks and procedures have also become a greater and greater focus of business due diligence calls held in connection with capital markets transactions. Such a diligence review may include topics such as the issuer's data assets (including any sensitive consumer data), risk management, top cybersecurity threats, resources applied to cybersecurity, compliance with applicable standards, insurance coverage and a description of past cybersecurity incidents.

We expect market practice in the power capital markets with respect to cybersecurity to continue to evolve. Given the nature of the threat to power and utility issuers and the SEC's ongoing focus on cybersecurity, deal participants should expect to devote additional time and resources on cybersecurity, including diligence and disclosure.

Hunton Andrews Kurth LLP's energy sector security team assists companies in protecting the security and resilience of their critical infrastructure facilities in the face of physical and cyber threats. Our team works with companies in the electric utility, oil, natural gas, pipeline, coal, nuclear, renewable energy and clean power, and related sectors to minimize the risks or consequences of a serious security incident. Our lawyers work seamlessly together to help clients with legal and regulatory compliance, physical and cybersecurity risk minimization, strategic engagement with key government agencies, response to physical or cyber events, insurance coverage and dispute resolution arising from law enforcement investigations, government enforcement actions and private litigation. The relevant practices include:

- ***Regulatory Compliance*** *- Complying with North American Electric Reliability Corporation (NERC) Reliability Standards, NIST security standards, and other regulations or guidance issued by federal and state agencies, including the FERC, NERC, Environmental Protection Agency (EPA), Pipeline and Hazardous Materials Safety Administration (PHMSA), Department of Transportation (DOT), National Transportation Safety Board (NTSB), Nuclear Regulatory Commission (NRC), Federal Emergency Management Agency (FEMA), Occupational Safety and Health Administration (OSHA), Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), state public utility commissions, and state attorneys general.*
- ***Statutory Compliance*** *- Complying with all federal and state information security requirements, including security breach notification laws at the federal level and in 47 states and four territories, the Pipeline Safety Act, the Payment Card Industry Data Security Standard, HIPAA, and the Gramm-Leach-Bliley Act.*
- ***Compliance with Foreign Laws*** *- Utilizing the experience of our team members in the United States, United Kingdom, Belgium and Beijing, and our network of leading local privacy and cybersecurity lawyers in more than 100 countries, we work with clients to ensure compliance with foreign legal requirements.*
- ***Risk Reduction*** *- Reducing the risks and consequences of major physical and cyber events, including assistance with the development of strategies, policies, plans and procedures that reflect industry best practices and standards, as appropriate, employee training, table top exercises, and cybersecurity penetration testing.*
- ***Strategic Engagement*** *- Strategically engaging with the federal government on information sharing and collaboration opportunities, and helping clients obtain the latest threat and vulnerability information from agencies such as the FBI, the Department of Homeland Security and the Department of Energy.*

- ***Response to Cyber Incidents*** *- Providing comprehensive "breach coach" assistance in managing the full panoply of activities associated with a significant cybersecurity incident/data breach, including: (i) directing a privileged internal forensic investigation; (ii) liaising with law enforcement and federal and state regulatory agencies such as the FBI, US Secret Service, Department of Justice, FTC and state attorneys general; (iii) analyzing breach notification requirements; (iv) managing notifications to affected individuals, state and federal regulators and consumer reporting agencies; (v) negotiating with payment card services; (vi) establishing relationships with credit bureaus; (vii) managing public relations; (viii) training call center agents; (ix) handling regulatory investigations and enforcement actions; (x) managing legislative inquiries; (xi) preparing executives for hearings; (xii) assisting with investor relations; preparing for litigations and advising on information retention obligations; and (xiii) handling resulting lawsuits (including class actions) and other legal actions brought by regulators, customers, business partners and other parties in federal and state court, before regulatory agencies and in alternative dispute resolution proceedings.*
- ***Response to Physical Incidents*** *- Providing comprehensive assistance with responding to significant physical events, including engaging with federal and state regulatory agencies, minimizing litigation consequences, preparing for congressional inquiries and hearings, and advising on public relations and other issues.*
- ***Dispute Resolution*** *- Assisting with dispute resolution regarding physical and cyber events, including investigations by the FBI, US Secret Service and other law enforcement agencies; enforcement actions by the EPA, PHMSA, FERC, OSHA, FTC, Department of Justice and state attorneys general; and individual and class action litigation regarding liability, insurance coverage, contractual obligations and other issues in federal and state court, alternative dispute resolution proceedings and before regulatory agencies.*
- ***Limiting Liability*** *- Reducing the potential legal liability associated with a terrorist attack by obtaining a certification or designation for a physical or cybersecurity system under the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act.*
- ***Insurance Counseling and Recovery*** *- Assisting with insurance coverage for physical and cybersecurity incidents, including the development of insurance programs that address a company's cyber or physical risk profile, and the recovery of insurance proceeds in the event of an incident.*
- ***Policy Advocacy*** *- Advising on executive branch and congressional activity relating to physical and cybersecurity, including policies and programs, pending legislation, hearings, inquiries and investigations.*

Hunton Andrews Kurth LLP's energy sector security team is led by cybersecurity partner ***Paul Tiao****, and energy partner* ***Kevin Jones****, and includes lawyers from a wide range of practice groups within the firm.*

QRP Deals Come to Power Capital Markets

"Qualified replacement property" (QRP) transactions pursuant to Section 1042 of the Internal Revenue Code (IRC) have been relatively common in the capital markets. Recently, the Procter & Gamble Company issued QRP debt in November 2015 and August 2017. United Parcel Service, Inc. has been particularly active in the space, issuing QRP debt in December 2014, September 2015, October 2015, December 2015, March 2016, June 2016, August 2016, March 2017 and November 2017. But for the first time, these deals have recently started to receive attention from utility issuers. Over the last year, Florida Power & Light Company conducted multiple securities offerings whereby such securities being issued are used as QRP by certain taxpayers to avoid or defer tax on the gain from sales of "qualified securities."[1] [2]

Section 1042(a) of the IRC permits a taxpayer, upon a timely election, to defer or eliminate capital gains taxes on the sale of "qualified securities" to an "eligible worker-owned cooperative" (EWOC) or an "employee stock ownership plan" (ESOP).[3] Pursuant to IRC Section 1042(c), "qualified securities" are securities issued by a closely held domestic C corporation (i.e., with no stock outstanding that is "readily tradeable" on an established securities market) that have been held by the taxpayer for a minimum of three years before the sale of the securities to an EWOC or an ESOP.[4] The taxpayer must purchase "qualified replacement property" as early as three months before the sale but no later than twelve months from the consummation of the sale.[5]

For purposes of Section 1042 of the IRC, QRP means any security issued by a domestic operating corporation that (i) uses more than fifty percent of its assets in the active conduct of a trade or business, (ii) does not have passive income in excess of twenty-five percent of its gross receipts in the taxable year prior to the purchase, and (iii) is not the corporation which issued the qualified securities that such security is replacing or a member of the same controlled group of corporations, as defined in Section 1563(a)(1) of the IRC, as such corporation.[6] QRP includes both equity and debt securities of a corporation that meets the threshold tests.[7]

The taxpayer's basis in the QRP is determined at the time of purchase, but the basis is reduced by the capital gain on the "qualified securities" that has been deferred.[8] Taxpayers can further eliminate tax on the initial gain by setting up lifetime gifts, which do not require recognition of the deferred gain under Section 1042 of the IRC.[9]

The securities of operating utilities will often qualify as QRP under Section 1042(c)(4) of the IRC. In 2018, Florida Power & Light Company completed two floating rate note securities offerings which met the criteria as QRP.[10] In the Florida Power & Light Company offerings, the floating rate notes each had fifty year tenors and a floating interest rate set at three-month LIBOR ***minus*** thirty basis points.[11] The structure of these offerings, similar to the other recent offerings in this space, also provided both the holder and issuer certain flexibility for repayment. The issuer is permitted to redeem the notes at descending prices beginning in year 30. Holders are permitted to require repayment of their notes at ascending prices beginning on the first year after issuance. The issuer is also permitted to shorten the maturity of the notes upon the occurrence of certain "tax events."[12]

It remains to be seen whether other utilities will conduct similar offerings. But given the pricing characteristics, it appears likely that others in the industry will take advantage of this structure.

[1] Florida Power & Light Company, Form 424(b)(2), dated June 12, 2018, *available at* https://www.sec.gov/Archives/edgar/data/37634/000114420418034044/tv496404-424b2.htm.

[2] Florida Power & Light Company, Form 424(b)(2), dated November 8, 2018, *available at* https://www.sec.gov/Archives/edgar/data/37634/000114420418058626/tv506592-424b2.htm.

[3] 26 U.S.C. § 1042(a) and (b).

[4] *Id.* at § 1042(c).

[5] *Id.* at § 1042(c)(3).

[6] *Id.* at § 1042(c)(4).

[7] Rev. Rul. 2000-18, Internal Revenue Service (2000).

[8] 26 U.S.C. § 1042(d), See also Rev. Rul. 2000-18.

[9] 26 U.S.C. § 1042(e)(3).

[10] Florida Power & Light Company, Form 424(b)(2), dated June 12, 2018 and Florida Power & Light Company, Form 424(b)(2), dated November 8, 2018.

[11] *Id.*

[12] *Id.*

Underwriting Agreements and Other QFCs: Preventing Another Lehman

In 2017, the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC) adopted rules (QFC Rules) to improve the resilience of global systemically important banking organizations (GSIBs).[1] The QFC Rules generally require U.S. GSIBs and their subsidiaries worldwide, as well as the U.S. subsidiaries, branches and agencies of foreign GSIBs, to include new language in certain of their qualified financial contracts (QFCs) to mitigate the risk of destabilizing closeouts of those QFCs.

The new regulations require covered GSIBs to include this new language in order to limit the ability of its QFC counterparties to terminate its QFCs or exercise default rights in the event that the GSIB or one of its affiliates becomes subject to a resolution proceeding. It is envisioned that the Dodd-Frank Act provisions that require this new language will avoid instability in the financial system like that caused by the Lehman Brothers insolvency.

When the Lehman Brothers parent filed for bankruptcy, counterparties with Lehman's operating subsidiaries exercised their cross-default rights. This led to rapid sales of collateral that secured the terminated QFCs in order to generate liquidity, among other undesirable results.

The exercise of rights by a non-defaulting party to a QFC generally is not subject to the automatic stay under the U.S. bankruptcy and insolvency laws. This is due to special "safe harbor" provisions. However, the new language required by the QFC Rules limits the ability to cross-default to the bankruptcy or insolvency of affiliates and contains certain exceptions to the safe harbor provisions which otherwise would apply to covered GSIBs.

Covered GSIB customers contemplating the issuance of securities should know about the QFC rules and also about the new language they require in certain underwriting agreements.[2] This new language does not need to be included in most underwriting agreements with a covered GSIB if both:

> (1) the agreement (a) is governed by the laws of the United States or any state and (b) does not explicitly exclude the applicability of Title II of the Dodd-Frank Act[3] or the Federal Deposit Insurance Act[4] (or a broader set of laws that includes these laws); and
>
> (2) each party to the underwriting agreement other than the covered GSIB is (a) an individual domiciled in the United States; (b) a company incorporated in or organized under the laws of the United States or any state of the United States; (c) a company which has its principal place of business in the United States; or (d) a U.S. branch or U.S. agency of a foreign banking organization.[5]

Nonetheless, since January 1, 2019, many covered GSIBs, when acting as underwriters, have been including the new language in their underwriting agreements even where unnecessary. In addition, they have been doing so regardless of whether a customer already has agreed to the new language by adhering online to the ISDA 2018 U.S. Resolution Stay Protocol (Protocol) published by the International Swaps and Derivatives Association Inc. (ISDA)[6] (along with all other parties to the customer's underwriting agreement).[7] A list of adhering parties, which is extensive but may not include all parties to any particular underwriting agreement, is available at https://www.isda.org/protocol/isda-2018-us-resolution-stay-protocol/adhering-parties.

Online adherence generally is preferable for customers even where the new language is included in their underwriting agreements and other QFCs with covered GSIBs because a customer receives certain creditor protections for adhering online which are not available by simply including the new language in a QFC (adhering online and including the new language in a QFC will not negate those protections).

[1] 12 C.F.R. §§ 252.81 *et seq.* (Federal Reserve), pt. 47 (OCC), pt. 382 (FDIC).

[2] *See also* SIFMA, Application of the U.S. QFC Stay Rules to Underwriting and Similar Agreements (Dec. 13, 2018), *available at* https://www.sifma.org/wp-content/uploads/2018/12/Application-of-QFC-Stay-Rules-to-Underwriting-Agreements.pdf.

[3] *See* 12 U.S.C. §§ 5381 *et seq.*

[4] *See* 12 U.S.C. §§ 1811 *et seq.*

[5] *See* 12 U.S.C. §§ 252.83(a) (Federal Reserve), 47.4(a) (OCC), 382.3(a) (FDIC).

[6] *See* ISDA, *ISDA 2018 U.S. Resolution Stay Protocol (Open from August 22, 2018), available at* https://www.isda.org/protocol/isda-2018-us-resolution-stay-protocol/.

[7] Adhering online to the Protocol rather than including the new language in an underwriting agreement or other QFC constitutes an agreement to the new language only if all parties to the QFC have adhered to the Protocol.

Covered GSIBs often request new language or adherence from customers with which they anticipate transacting before actually engaging in the related transactions even though the QFC Rules may not require compliance by those customers until January 1, 2020. Fortunately, earlier online Protocol adherence will not be effective as to those customers until such later date regardless of the earlier adherence.

The QFC Rules are here for good and already apply to most of the U.S. law-governed underwriting agreements that U.S. customers make with covered GSIBs, regardless of whether the new language required by the QFC Rules is included in those underwriting agreements or the U.S. customers adhere online to the Protocol. Inclusion of the new language and/or online customer Protocol adherence will result in the application of the QFC Rules to the balance of underwriting agreements with covered GSIBs.

Consequently, covered GSIB customers should develop an understanding of the QFC Rules.

For questions regarding the QFC Rules, please contact Joseph B. Buonanno (jbuonanno@HuntonAK.com), a partner in the Charlotte office of Hunton Andrews Kurth LLP and head the firm's derivatives group.

Steven C. Friend, Editor
+1 212 309 1065
sfriend@HuntonAK.com

BASELOAD is prepared from time to time to provide general information about selected power and utilities capital markets developments and issues for attorneys at Hunton Andrews Kurth LLP, and is provided to clients and friends of Hunton Andrews Kurth LLP. It is not intended to provide legal advice or legal opinions and must not be relied on as such. If you have questions related to any of the articles in this issue, please contact any of the below members of the Power and Utilities Capital Markets group at Hunton Andrews Kurth LLP:

Bud Ellis
+1 212 309 1064
ellisb@HuntonAK.com

Kevin C. Felz
+1 212 309 1053
kfelz@HuntonAK.com

Michael F. Fitzpatrick, Jr.
+1 212 309 1071
mfitzpatrick@HuntonAK.com

Steven C. Friend
+1 212 309 1065
sfriend@HuntonAK.com

S. Christina Kwon
+1 212 309 1089
ckwon@HuntonAK.com

Peter K. O'Brien
+1 212 309 1024
pobrien@HuntonAK.com

HUNTON
ANDREWS KURTH

19091-2.19