CYBERSPACE LAW COMMITTEE
WINTER WORKING GROUP
FORT LAUDERDALE, FLORIDA
JANUARY 29-30, 2016

Ransoming Data: Technological and Legal Implications of Payments for Data Piracy

Panelists: Ian T. Ramsey, Stites & Harbison, PLLC, Louisville, Kentucky; Edward A. Morse, Creighton University School of Law, Omaha, Nebraska

Summary

Cybercriminals are reinventing the crime of extorting money from individuals and companies. Firms and individuals facing the prospect of data losses from ransomware or disclosure of customer information face difficult choices. This program will explore legal and technological frameworks affecting this scenario, including financial regulation, sanctions regimes, and potential penalty structures that affect the payment of ransom and suggest potential changes in the legal framework that might reduce incentives for malefactors to engage in this behavior.

Contents

I. Ransom and Terrorist Financing: An Overview.

Ransom from kidnapping is a potentially significant source of terrorist financing, which has drawn attention from International authorities.[1] 1,283 kidnappings motivated by terrorism were reported in 2012; one group reported average ransom of $4.5 million/hostage in 2012, up from nearly $1 million in 2011.[2]

UN sources indicate that a "majority of kidnappings are criminal in nature rather than being motivated by terrorism."[3] While it may be understandable to pay ransom, payment may nevertheless violate the UN sanctions regime. "The Al-Qaida sanctions regime confirms that ransom should not be paid to listed groups or individuals. When a ransom is paid, the insurance sector, private companies and risk consultancies may be involved in providing the funds or facilitating payments. The kidnap and ransom insurance market, worth $250 million in 2006, doubled in size by 2011."[4]

In an apparent effort to provide a humanitarian response to families of victims, President Obama announced U.S. policy initiatives in this area on June 24, 2015. On one hand, the President confirmed that the official U.S. policy on paying ransom would not change: "I firmly believe that the United States government paying ransom to terrorists risks endangering more Americans and funding the very terrorism that we're trying to stop. And so I firmly believe that our policy ultimately puts fewer Americans at risk." [5]

On the other hand, the President also announced a significant change: "At the same time, we are clarifying that our policy does not prevent communication with hostage-takers -- by our government, the families of hostages, or third parties who help these families. And, when appropriate, our government may assist these families and private efforts in those communications -- in part, to ensure the safety of family members and to make sure that they're not defrauded. So my message to these families was simple: We're not going to abandon you. We will stand by you." [6] Moreover, the President also stated: "In particular, I want to point out that no family of an American hostage has ever been prosecuted for paying a ransom for the

[1] See Fifteenth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 22083 (2012) concerning Al-Qaida and associated individuals and entities, U.N. Security Council S/2014/41 ((January 29, 2014); http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_41.pdf [hereinafter "Fifteenth report"].
[2] Fifteenth Report, ¶ 36.
[3] Id. ¶ 38.
[4] Id. ¶ 37. see also Sixteenth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 161 (2012) concerning Al-Qaida and associated individuals and entities, U.N. Security Council S/2014/770 (October 29, 2014), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_770.pdf [hereinafter "Sixteenth report"]. Insurance and financial intermediaries play a significant role in the ransom environment, and submarkets for "outsourcing" kidnapping functions to criminal enterprises also seem to be developing. See id. ¶¶ 52-59.
[5] Statement by the President on the U.S. Government's Hostage Policy Review (June 24, 2015), https://www.whitehouse.gov/the-press-office/2015/06/24/statement-president-us-governments-hostage-policy-review
[6] Id.

return of their loved ones. The last thing that we should ever do is to add to a family's pain with threats like that."[7]

In other words, while the U.S. won't pay ransom, private parties apparently may do so – and the government will assist with communications and may act to ensure that they are not defrauded. As a practical matter, this policy is likely to enhance the economic value of hostage taking. The very rationale offered by the President to deny government ransom payments would seemingly apply to payments from private sources. Private payments thus incentivize those who intend to undertake kidnapping activities by conferring economic benefits.

Of course, the President's statement cannot change laws that penalize banks for facilitating payments, which are discussed below. Some commentators think that the policy change may have a negligible impact on the kidnapping environment because banks will not take on the risk of facilitating that payment based on the President's word alone.[8] Without a license from the Treasury's Office of Foreign Assets Controls, it would be risky to process a transfer to a designated individual, firm, or country that is subject to international sanctions.[9] But as discussed below, sanctions regimes are far from comprehensive. The list of sanctioned individuals, entities, and governments is not complete, and there may also be weak links in the regulated network of banks and financial institutions.

Technology also facilitates physical kidnapping or its close cousin, "virtual kidnapping", which involves false claims that a loved one has been kidnapped when he or she is really just off the grid for a time.[10] Access to social media and other online sources can facilitate the detection of a victim's location, as well as other valuable information for extorting payment. In this sense, technology can be a two-edged sword: it can provide advantages that accrue on both sides of the law.

Technology makes cyber extortion through ransomware possible.[11] Risk consultants have opined that "the development of new and resilient cyber extortion techniques will increase the threat to business in the coming year."[12] In some cases, data security breaches are also triggering cyber-ransom. Rather than monetizing the value of data through identity theft and financial fraud, some cybercriminals are going directly to the victims in asking for payments to avoid disclosing sensitive personal data. For example, hackers have targeted clients of Ashley Madison, which include thousands of accounts allegedly linked to corporate and government email addresses. The hackers state: "If you would like to prevent me from finding and sharing this information with your significant other send [bitcoins] to the following address…."[13]

---

[7] Id.
[8] See Samuel Rubenfeld, Easier U.S. Stance on Terrorist Ransoms Hindered by Bank Risks, Wall Street Journal Risk & Compliance Journal (June 25, 2015), available at http://blogs.wsj.com/riskandcompliance/2015/06/26/easier-u-s-stance-on-terrorist-ransoms-hindered-by-bank-risks/ .
[9] See id. The sanctions regime is discussed in part VI, below.
[10] See Control Risks, RISKMAP REPORT 2015, at 120, https://www.controlrisks.com/webcasts/studio/flipping-book/riskmap-report-2015/riskmap-report-2015.html (registration required for access).
[11] See id. at 121.
[12] Id.
[13] See Ashley Madison Hack Sparks Lawsuit, www.pymnts.com/news/2015/ashley-madison-hack-sparks-lawsuit (August 24, 2015).

While this activity does not involve direct threats to human life (but after disclosure to a significant other, who knows?), it presents security threats that resemble those in the kidnapping regime. This activity is also getting attention from law enforcement. The Wall Street Journal has also recently reported on the threat from cyber hackers, with an FBI official stating that certain ransomware is so good that, "to be honest, we often advise people just to pay the ransom."[14] This program examines the technology and the legal frameworks affecting ransom payments for data. While the act of invading another's computer system and extorting funds from them are likely the subject of criminal proscriptions in other countries, as well as violations of U.S. law, the primary focus here is upon the means of detecting and enforcing such laws, as well as the legal framework that may impact the firm or individual making a ransom payment.

Part II provides an overview of ransomware and the technology behind ransom payments. Parts III examines the financial regulatory structure and its potential to deal with identifying and preventing financial crimes, including cybercrime. Part IV addresses the sanctions regime and other laws that can potentially affect ransom payors. Finally, part V briefly concludes with some policy options and other considerations that could affect the market for ransoming data.

II. Ransomware and Ransom Payments.

A. Overview

Ransomware is malware—malicious code—introduced into desk top computers and mobile devices which encrypts data with the intent to exchange a ransom payment for the decryption key.[15] The concept is not new. The sophistication of the code has, however, metastasized into a sophisticated and lucrative criminal enterprise by taking advantages in the U.S. private and public sectors.[16]

The scheme works this way: a user opens an attachment to email or an html link within an email or simply accesses an infected website.[17] The malware is transferred to the user's system.[18] There are generally three variants of malware transferred: (1) encryption, commonly known as CrptoLocker; (2) screen lock, commonly known as WinLocker; and, (3) Master Boot

[14] See Devlin Barrett, Paying Ransoms to Hackers Stirs Debate, The Wall Street Journal, November 9, 2015, at http://www.wsj.com/articles/paying-ransoms-to-hackers-stirs-debate

[15] This should not be confused with fake-antivirus, also known as rogue security software and also scareware. It is considered a form of ransomware because it pretends to find malware on your computer. In some instances payment is requested, while other forms offer the service for free. In this scenario, the scam is the user is not really paying for anything at best and at worst the "fix" being paid for actually is a link that delivers malicious code. See www.wikipedia.org, "rogue security software." For a partial list naming over 100 type fake-antivirus programs see www.wikipedia.org, "list of rogue security software."

[16] In his remarks to the Senate Judiciary Committee on December 9, 2015, F.B.I. Director James B. Comey stated, "An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated." www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-8.

[17] First reported in 2012 and given the name "reveton" this virus was described as a drive-by malware because it was activated by simply clicking on an infected website. *See* www.fbi.gov/news/stories/2012/august/new-internet-scam.

[18] A Botnet also could already be on a user's system and under a general purpose upgrade command could allow malware to be installed without any action by the user. See www.sophos.com, Article ID:119006.

Record which interrupts normal operating systems.[19] In each case, instructions are posted on the user's screen for the payment of a ransom to obtain a key correcting the problem.

The most commonly known form of ransomware is known as Cryptolocker, which first appeared in 2013 according to an alert posted by the United States Computer Emergency Readiness Team ("US-CERT"). Other forms followed such as Xorist, CryptoBit, CryptoDefense, and CryptoWall.[20] A particularly devious variant is called BitCrypt which while encrypting files searches and steals bitcoins from the user.[21] There is a hint of professionalism in the tone of the instructions juxtaposed against the clear message that your data is forever lost unless the ransom is paid. And to make sure that language is not a barrier to payment the user can access ransom instructions in English, French, German, Russian, Italian, Spanish, Portuguese, Japanese, Chinese and Arabic.[22] In 2014, "ransomware attacks grew 113 percent, driven by more than 4,000 percent increase in crypto-ransomeware--file encryption attacks."[23] There is not a corresponding rise in prosecutions, however. Instead there appears to be a race by the United States government to regulate crypto-currency and prosecute cyber-criminal using crypto-currency.

The first civil enforcement to action against a virtual currency exchanger occurred May 2015 against Ripple Labs, Inc. and its wholly-owned subsidiary XRP II, LLC. for selling its virtual currency XRP. The $700,000 civil fine was for violating several requirements of the Bank Secrecy Act, not registering with FinCen, and failing to have adequate money laundering programs in place to protect its product from use by money launderers or terrorist financiers.[24] In 2015, the U.S. Attorney for the Southern District of New York issued a press release concerning only one criminal prosecution against Anthony R. Murgio and Yuri Lebedev for running an unlicensed internet Bitcoin exchange used by victims of CryptoWall ransomware to pay ransoms via TOR[25] (The Onion Router) to cyber-criminals.[26] At the same time, the FBI issued a press release noting that between April 2014 and June 2015, the FBI's Internet Crime

---

[19] See www.sophos.com, Article ID: 119006. For more information on Botnets go to www.fbi.gov, "Botnets 101 What They Are and How to Avoid Them," published on June 5, 2013.

[20] CryptoWall is cited using TOR, short for "The Onion Router," to direct victims of ransomware to host sites were the ransom is paid in Bitcoin. This system disguises the users identity. *See* Senate Judiciary Committee statements of Director James B. Comey, December 9, 2015. Another less publicized malware known as CTB-Locker (Curve-TOR-Bitcoin Locker) aka Critroni was reported in June 2014 by the IDG News Service in a July 21, 2014, article published in PCWorld.

[21] This variant first appeared in February 2014 and a decryption program was created shortly thereafter credited to researchers at Airbus Defence and Space. *See* www.pcworld.com, IDG News Service, Lucian Constantin, March 25, 2014. For more information on Airbus see www.cybersecurity-airbusds.com, although the company does not mention its involvement.

[22] *Id*.

[23] Symantec 2015 Internet Security Threat Report, www.symantec.com.

[24] See Press Release issued on May 5, 2015, at www.fincen.gov.

[25] TOR is a free software download that allows for anonymous, i.e., untraceable, communications. Because of this anonymity, cyber-criminals have been known to use this benefit and thus cloaked its use to be associated with criminal activity. In reality, the basis of the program is actually a United States non-profit organization www.torproject.org having its original funding roots tied to the United States government. The instructions, for example, might instruct a victim to go to a host site and follow Bitcoin payment instructions. The site and the payments arguably are then untraceable to an individual.

[26] *See* www.fbi.gov/newyork/press-releases/2015/manhattan-u.s.-attorney-annouces-charges-against-two-florida-men-for-operating-an-underground-bitcoin-exchange.

Complaint Center had received 992 CryptoWall-related complaints with victims reporting losses over $18 million.[27]

B. Bitcoin and Crypto-Currency[28] in the Ransom Scheme.

The Bitcoin first emerged in 2009 and steadily built acceptance among those more deeply involved in coding initiatives. That acceptance migrated to the criminal underworld and became prominently associated with the Silk Road, which abruptly ended when the site was seized by U.S. federal agents in October 2013.[29] The Bitcoin and other convertible crypto-currencies are, however, the keystone to current ransomware schemes.[30]

While efforts to rehabilitate crypto-currencies are evident, in that many legitimate businesses now accept bitcoin as a form of payment, the association of bitcoin with criminal enterprises is a perception. Perhaps recognizing these conflicts, the Department of Justice held a Blockchain Summit in November 2015 with representatives from the Department of Justice, FinCen, and representatives from the private sector towards building a Digital Currency Task Force.[31]

From a regulatory perspective, one of the inherent weaknesses of a crypto-currency is the lack of connection between the putative currency and those claiming ownership and a centralized, regulated system that could permit tracking.[32] The allure of cryto-currency is its decentralized system, where validation of exchanges through an official log or "block chain" is monitored to validate transactions. The business is becoming more mainstream with companies like BitFury recently attracting significant rounds of financing and a former White House communications deputy.[33]

The Bitcoin and its progeny can be made untraceable and thus well suited for criminal transactions, also explaining why perhaps BitFury has on its Board of Advisors a former Department of Justice prosecutor specializing in computer crime. From Bitcoin, according to the website coinmarketcap.com, as of December 2015, 677 "altcoins" now exist, the phrase connoting that virtually all are copies of Bitcoin.

---

[27] *See* www.fbi.gov/sandiego/press-releases/2015/fbi-warns-public-of-cryptowall-ransomware-schemes.

[28] We use the phrase crypto-currency here to denote its reference to a math-based virtual currency protected by cryptography. Virtual currency is a more generalized term describing the digital representation of value versus a fiat currency of coin and paper or e-money which is a digital representation of a fiat currency.

[29] A version 3 of Silk Road continues today and many other sites known as dark markets have proliferated since the seizure.

[30] *See* FIN-2013-G001, "Application of FinCen's Regulations to Persons Administering, Exchanging, or Using Virtual Currency," March 18, 2013. The Guidance was later applied in FIN-2015-R001, "Application of FinCen's Regulations to Persons Issuing Physical or Digital Certificates of Ownership of Precious Metals," August 14, 2015.

[31] See www.coindesk.com, November 10, 2015, article by Pete Rizzo.

[32] The inability to track the currency also raises global money laundering and terrorism concerns. The United States is a member of the Financial Action Task Force, www.fatf-gafi.org, a policy-making body focused on these issues. Of note for this article is FATF's June 2014 publication "Virtual Currencies: Key Definitions and Potential AML/CFT Risks found at www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.

[33] www.bitfury.com, Press, "Former Whitehouse Communicator Jamie Smith Joins BitFury as Global Chief Communications Officer," December 4, 2015 .

Bitcoin's association with criminal enterprises appeared to have given it enough notoriety moving its acceptance to more traditional transactional channels. Even the subsequent arrest and collapse of Bitcoin exchanges—websites where federally accepted and regulated currency is exchanged for crypto-currency—did not seem to slow the pace. So, when Mt. Gox shut down and filed for bankruptcy in February 2013 because of the alleged theft of Bitcoins valued at $430 million, the valuation of BitCoin plunged and then recovered. Likewise, several breaks in the block chain, where the issued numbers appear to have dramatically changed, have occurred effecting valuation and similarly been corrected.

Even so, the Internal Revenue Service in its Virtual Currency Guide IR-2014-36 published on March 25, 2014, declared that a virtual currency is property and thus when used is a taxable event. See also Notice 2014-21, 2014-16 IRB 938 (March 26, 2014). This was likely prompted by several criminal prosecutions around the United States concerning Bitcoins ending with the August 2013, United States District Court Memorandum Opinion in the case styled *Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*, Case No. 4:13-cv-00416, which found that Bitcoin was money and thus subject to the jurisdiction of the SEC for misrepresentations to investors that Shavers had defrauded.

Objectively there is a direct relationship between the rise of crypto-currencies and the increase of ransomware attacks. This makes logical sense in the sequence of events compared to a generic kidnapping scenario where the exchange of money arguably places criminals in their most vulnerable position. The virtual kidnapping of ransomware allows for anonymity from beginning to end of the event. And, because an individual life is not directly concerned, the investment of law enforcement resources committed to solving these crimes are balanced accordingly.

C. Law Enforcement Agencies.

To the general public, a maze of regulatory authorities have investigative authority when impacted by ransomware. The most logical first responder would be local law enforcement. A larger city having a financial budget supporting a cyber-crime unit would be helpful, but that only covers a small fraction of U.S. businesses and individuals. More significantly, the crimes associated with ransomware are more akin to federal prosecution as the criminal acts are generally interstate and most likely international.[34] Federal authorities thus may be better suited, as they are likely to provide access to a globally collaborative law enforcement network.

The Federal Bureau of Investigations has a dedicated and effective Cyber Task Force which utilizes an on-line cyber-crimes reporting form via the Internet Crime Complaint Center, commonly known as (IC3). The Department of Homeland Security has the National Cybersecurity and Communications Integration Center (shares information with federal, state, local law enforcement and private sector), but also collects reports of phishing, malware, and

[34] A list of charges against the FBI's 10 Most Wanted for Cyber-Crimes includes: Money Laundering, RICO, Wire Fraud, Computer Fraud and Abuse Act, Identity Theft and Assumption Deterrence Act, Aggravated Identity Theft, Conspiracy, Conspiracy to Commit Bank Fraud, Computer Intrusion, Fraud In Connection with a Computer, Conspiracy to Commit Computer Hacking, Computer Hacking, Identification Document Fraud Conspiracy, Accessing a Computer without Authorization for the Purpose of Commercial Advantage and Private Financial Gain, Damaging Computers through the Transmission of Code and Commands, Economic Espionage, Theft of Trade Secrets.

unauthorized access. Separate from these is the U.S. Immigration and Customs Enforcement Cyber Crimes Center (C3)[35], primarily dedicated to drug and child related offenses. Internationally there is the Europol Cyber Crime Center (EC3), INTERPOL, and U.K. National Cyber Crime Agency.

Closely associated with the FBI is the National Cyber Investigative Joint Task Force[36] in partnership with the Department of Defense Cyber Crime Center (DC3)[37], the aforementioned Cyber Task Forces, iGuardian[38] (relating to minors), InfraGuard[39] (private – FBI collaboration to share information), National Cyber-Forensics & Training Alliance[40] (collaboration between FBI Cyber Division's Cyber Initiative and Resource Fusion Unit, private sector, Carnegie Mellon Computer Emergency Response Team, and FBI Internet Crime Complaint Center), and the Cyber Action Team, which deploys experts to assist with cyber intrusions around the world.

The Secret Service has its Electronic Crimes Task Force[41] and finally the Department of Justice has designated a Computer Crime and Intellectual Property Section[42] to handle prosecutions. Perhaps further complicating this question for the general public is the role of the Federal Trade Commission taking the lead on identity theft education and reporting.[43]

III. Financial Regulation and the Detection of Criminal Activity.

Traditional financial channels continue to play an important role in many cybercrimes. For obvious reasons, those engaged in data ransom would presumably prefer that the true identity of the payee is not known to the payor, which might lead to the use of crypto-currencies. But some criminal enterprises choose traditional financial channels, despite the fact that they may generate scrutiny from government regulators and law enforcement officials, which criminals would rather avoid. Despite the regulatory net, there are still holes that cybercriminals (and other criminals) use to elude law enforcement. Using crypto-currency is only one such means of evasion. The discussion below provides a selective treatment of some significant regulatory requirements and their potential effects in deterring criminal enterprises, which provides important context for understanding the fiscal environment for the cybercriminal.

A. Domestic payments: BSA and AML.

As a practical matter, payments to domestic payees through regulated financial channels will present significant risks of detection for the cybercriminal.

1. Customer identification and due diligence requirements imposed by the Bank Secrecy Act will generally require robust identification of accounts and payees in the domestic context. See, e.g., 31 CFR § 1020.220 (illustrating Customer Identification Programs for banks and similar financial institutions).

[35] www.ice.gov/cyber-crimes.
[36] www.fbi.gov/about-us/investigative/cyber/ncijtf.
[37] www.defense.gov.
[38] www.ice.gov/cyber-crimes/iguardian.
[39] www.infraguard.org.
[40] www.ncfta.net.
[41] www.secretservice.gov/investigation.
[42] www.justice.gov/criminal-ccips.
[43] www.consumer.ftv.gov and www.identitytheft.gov.

2. U.S. persons and non-U.S. persons both require some form of identification from an official source to open accounts.

3. Entities present special challenges, particularly when state laws permit formation without disclosing the identity of actual owners. However, BSA/AML requirements generally require some information gathering about the principals and the location of operations. Moreover, FinCEN's notice of proposed rulemaking would enhance these requirements, along with other due diligence activities designed to identify problematic customers. See Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45153 (Aug. 4, 2014).
    a. These include beneficial ownership disclosure, and enhanced and ongoing monitoring requirements to identify and support suspicious transactions.
    b. These requirements essentially deputize banks and other financial services providers to engage in risk assessment, thereby smoking out suspicious customers. See generally Schroeder, Hodge, and Morse, Electronic Payments: Winnowing the Network and Avoiding the Shadows, ABA Cyberspace Law Winter Working Group (Jan. 23, 2015), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567806 .

4. Of course, ongoing monitoring requirements may mean that payments from your legitimate firm could trigger government scrutiny, too. Information sharing may also affect prospects for detection. See, e.g., 31 CFR § 1020.520, .540 See also Federal Financial Institutions Examination Council, Bank Secrecy Act Anti Money Laundering Examination Manual, Appendix F: Money Laundering and Terrorist Financing "Red Flags", available at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_106.htm
    a. FinCEN publishes a technical bulletin providing an annual review of aggregated SAR reports. See FINCEN, SAR Stats (October 2015), available at https://www.fincen.gov/news_room/rp/sar_by_number.html (click on "SAR Stats Issue 2 – October 2105).
    b. SAR filings have dramatically increased over time, with more than 1.7 million filed in 2014. Fraud remains a significant problem that triggers SAR filings. See id. (One would not expect 1.7 million SARS to involve no criminal activity; nor would one expect all criminal activity to be caught.)

5. So what about payments in cash? CTR requirements can also present scrutiny if there are withdrawals or deposits totaling over $10,000. Evading these by "structuring" (i.e., breaking down the transaction into multiple smaller ones) or "smurfing" (using branches or multiple locations to send funds, thereby avoiding the total) can sometimes avoid detection. Such activities are crimes, however, carrying severe penalties, including forfeiture. See Timothy J. Ford,

Note, Due Process for Cash Civil Forfeiture in Structuring Cases, 114 MICH. L. REV. 455 (2015).

a. Note also that Form 8300 imposes reporting requirements on a broader set of businesses, which may not be subject to filing a SAR under BSA requirements. See generally Jack Manhire, When do you report cash payments over $10,000?, 40 CAYMAN FINANCIAL REVIEW 48 (2015), available at http://ssrn.com/abstract=2654511
b. Civil penalties for failure to file Form 8300 include fines of up to $25K/occurrence, with a cap at $500K for small businesses and a cap of $1.5M for larger ones. Criminal penalties are higher, and may include 5 years prison.
c. Note also that firms may have an obligation to inform the person involved that they are filing Form 8300. Do you have the right information to do this? In contrast, a SAR must be kept secret from the customer, apart from information sharing with appropriate government agencies and other financial institutions.

6. Cybercriminals may try to avoid using these domestic finance channels because of the enhanced reporting and detection risks. But if they do use them, forming new entities, using friendly existing entities, and targeting institutions with weak compliance programs, are likely strategies. The domestic financial system remains a tool used by legitimate and criminal enterprises, despite these measures. No detection efforts are perfect; there are always weak links in the system.

B. Foreign Payments.

Payments to foreign destinations from U.S. payors will also face scrutiny under similar rules. However, to a considerable extent, transfers to foreign banks that extend to foreign customers will, as a practical matter, depend significantly upon the efforts of those foreign financial institutions. Herein lies a weak link to be exploited.

1. U.S. persons (including entities and "green card" holders) with foreign accounts face considerable pressure from FATCA, which requires Form 8938, and the BSA requirement for filing the FBAR (Form TD F-90-22.1) annual filing. Large penalties for failure to file reinforce this information disclosure regime.
a. The sheer ubiquity of this kind of disclosure makes it an unlikely tool to detect the use of a foreign account in making payments to a cybercriminal.
b. Foreign banks are increasingly cooperating and disclosing information on U.S. account holders despite confidentiality requirements.
c. Even though foreign depositors are generally exempt from U.S. income taxes on their interest, domestic banks are being tapped to collect and report that information to the U.S., which provides information to trade. See, e.g., Florida Banker's Assn' v. Treasury, 799 F.3d 1065 (D.C. Cir. 2015) (rebuffing bank challenge to these reporting requirements).

2. Cross-border electronic funds transactions receive extra scrutiny from FinCEN. See RIN 1506-AB01, Cross-Border Electronic Transmittals of Funds, 75 Fed. Reg. 60377 (Sept. 30, 2010) (proposed regulations).

3. The USA Patriot Act (Pub. L. No. 107-56) also amended the Bank Secrecy Act by adding new requirements for AML, enhanced due diligence (EDD), and other measures of cooperation targeting international fund transfers. See Generally 12 USC §§ 1829b, 1951-59, and 31 USC §§ 5311-14, 5316-32). Some significant provisions include:
    a. Section 311 of the Act (31 USC 5318A) permits the Treasury Department to impose Special Measures against foreign jurisdictions, financial institutions, or types of transactions in order to deal with money laundering concerns. See, e.g., RIN 1506-AB27, Imposition of Special Measure Against FBME Bank Ltd., 80 Fed. Reg. 45047 (July 29, 2015).
        1. Based on deficient AML programs (determined by audits by KPMG and EY), this foreign bank allowed significant financial services to criminal and terrorist organizations.
        2. According to FinCen, "The exclusion from the U.S. financial system of banks that, like FBME, serve as conduits for money laundering and other financial crimes will make it more difficult for terrorists, sanctions evaders, and money launderers to assess the substantial resources of the U.S. financial system." 80 Fed. Reg. at 45061.
    b. Section 312 of the Patriot Act also requires special due diligence for correspondent and private banking accounts.
    c. Failure to comply with BSA provisions, as amended, can result in large penalties for banks. See, e.g., In re: HSBC Bank USA, Assessment of Civil Money Penalty, No. 2012-02 (Dec. 10, 2012) ($500M penalty for failing to maintain adequate due diligence policies, procedures and controls for foreign correspondent accounts).
    d. But of course, this rule is only as effective as the screening mechanisms from other intermediary institutions. If other institutions connect with an excluded bank, obvious compliance challenges are presented.

4. So what about carrying cash outside of the U.S.? Yikes! The "Report of International Transportation of Currency or Monetary Instruments" (CMIR) must be completed for physical transportation of more than $10K into our outside the United States.
    a. Note: FinCen requires disclosure of "monetary instruments". What about prepaid cards? See Stephen T. Middlebrook, What's in Your Wallet? Could it be the Department of Homeland Security? BUSINESS LAW TODAY, November 2013, http://www.americanbar.org/publications/blt/2013/11/03_middlebrook.html

b. Middlebrook assesses the money laundering risk from such cards to be low, citing a 2013 Federal Reserve Bank of Atlanta study. See id. But he also suggests means to avoid detection by clever criminals.
c. The Government has indicated that FinCEN was still studying the issue of categorization of prepaid access cards as monetary instruments. See 79 Fed. Reg. 76456-01, 76608 (December 2014).
d. Here, too, large civil and/or criminal penalties may apply for failure to disclose, including prison of up to 10 years and seizure of funds.

5. UIGEA.

It should be noted that other statutory schemes may impact financial system transfers to online casinos located abroad, which could be targets for money transfers abroad. See e.g., Regulation GG: Prohibition on Funding of Unlawful Internet Gambling, 12 CFR 233, Compliance Guide to Small Entities, available at http://www.federalreserve.gov/bankinforeg/regggcg.htm

C. Bitcoin and the Cryptocurrency Option.

Although Bitcoin may present a means of avoiding the above regulatory regime, it will be difficult to do so as a practical matter due to increasing regulation of bitcoin exchanges as money transmitters. For excellent analysis, see Stephen T. Middlebrook and Sarah Jane Hughes, Regulating Cryptocurrencies in the United States: Current Issues and Future Directions, 40 William Mitchell L. Rev. 813 (2014). If one needs to convert currency to bitcoin, or vice versa, the regulatory environment continues to present a challenge for the cybercriminal. Conversion options outside the reach of U.S. regulators will be important. And as discussed below, the payor may also face scrutiny when it converts cash to bitcoin for the purposes of making these payments.

IV. Other Laws Impacting Payors.

A. Sanctions Regimes.

International sanctions regimes are also designed to prevent transfers to designated payees, institutions, and countries. In the United States, the Treasury's Office of Foreign Asset Controls (OFAC) supervises these programs.

1. Sanctions are rooted in laws designed to prevent support for individuals, organizations, or countries designated as enemies of the Government. These include the Trading with the Enemy Act and the International Emergency Economic Powers Act. Sanctions include asset freezes as well as preventing transfers to designees. For an historical discussion in the context of post-WWII sanctions, see Joseph Bishop, Judicial Construction of the Trading with the Enemy Act, 62 HARV. L. REV. 721 (1949).

2. OFAC has a webpage that lists designated parties and other sanctions. It contains a searchable database. See https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

3. Ransom payments to designated entities are illegal. See Samuel Cutler, Could the Administrations New Hostage Policy Leave Banks Vulnerable? , http://sanctionlaw.com/could-the-administrations-new-hostage-policy-leave-banks-vulnerable/ . Cutler explains:

   "It's important to begin from the fact that ransom payments to FTOs or Specially Designated Global Terrorists ("SDGTs") identified by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") are illegal under U.S. law. Monetary contributions to FTOs are considered material support under 18 U.S.C. 2339B, while transfers to SDGTs are violations of economic sanctions imposed pursuant to the International Emergency Economic Powers Act ("IEEPA").

   Furthermore, as the Financial Action Task Force ("FATF") notes in discussion of ransom payments to the Islamic State in Iraq and the Levant ("ISIL"), "[U.N. Security Council] Resolution 2161 applies to both direct payments and indirect payments through multiple intermediaries, of ransoms to groups or individuals on the Al-Qaida Sanctions List. These restrictions apply not only to the ultimate payer of the ransom, but also to the parties that may mediate such transfers, including insurance companies, consultancies, and any other financial facilitators."

4. OFAC includes guidance on its website in the form of Q&A advice that clearly shows that one cannot legally use intermediaries to avoid sanctions; you are still violating the law. (But that does not mean that people aren't trying.)

5. Severe consequences may follow for violating sanction restrictions.
   a. For example, see OFAC, Narcotics Sanctions Program (July 18, 2014) (noting criminal fines of up to $1M for individuals, $10M for corporations, and imprisonment of up to 10 years in prison; corporate officers may face 30 years imprisonment and fines of $5M), available at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/drugs.pdf

   b. For Civil Penalties and Enforcement Information by year, see https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx This includes a settlement of more than $329M by Credit Agricola Corporate And Investment Bank, which could have faced penalties of over $1.4B. See https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151020_cacib.pdf (10/20/2015).

   c. On the criminal front, the largest criminal penalty and forfeiture against a financial institution for sanctions violations occurred in May 2015. BNP Paribas, S.A. was sentenced to a five-year probation term

and ordered to forfeit over $8.8 billion plus pay a $140 million fine. See Department of Justice Office of Public Affairs, BNP Paribas Sentenced for Conspiring to Violate the International Emergency Economic Powers Act and Trading with the Enemy Act (May 1, 2015), available at http://www.justice.gov/opa/pr/bnp-paribas-sentenced-conspiring-violate-international-emergency-economic-powers-act-and (reporting that this is the "first time a financial institution has been convicted and sentenced for violations of U.S. economic sanctions").

6. Executive Order 13694, 80 Fed. Reg. 18077 (April 1, 2015), seeks to expand the sanctions regime to block property of persons engaging in "significant malicious cyber-enabled activities".
    b. This EO is issued under the International Emergency Economic Powers Act, the National Emergencies Act, and the Immigration and Nationality Act of 1953. See id.
    c. The President has declared "a national emergency to deal with this threat" from cyber-enabled activities. Id.
    d. The blocking extends to assets of those who "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity [proscribed by the order] or any person whose property and interests are blocked pursuant to this order." See § 1(a)(ii)(B).
        1. The Secretary of the Treasury, in consultation with the Attorney General and Secretary of State, make this determination. See id. § 1(a)(ii).
        2. Does this mean one who pays ransom to a designated person would be subject to blocking, too?
        3. Donations are prohibited, too. See id § 2.
        4. Prohibitions under section 1 include "the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order." Id. § 3(a).
        5. Conspiracies to evade or avoid are "prohibited". Id. § 5.
    e. But this still depends upon an updated list: if your cybercriminal is not on the list, then can you pay without consequences?

B. Tax Laws.

Information reporting, limits on deductibility, withholding rules all potentially affect the tax treatment of ransom.

1. IRC § 162(a) provides a broadly-based provision allowing for the deduction of ordinary and necessary expenses connected to a trade or business. If deductible, payments are thus made with pretax dollars, reducing the ultimate economic cost to the taxpayer.

2. IRC § 162(f) denies a deduction for "any fine or similar penalty paid to a government for the violation of any law." Thus, fines have to be paid with after-tax dollars, raising the economic cost to the taxpayer.

3. IRC § 162(c)(1) addresses the matter of bribes, kickbacks, and other payments made directly or indirectly to an official or employee of any government agency or instrumentality if those payments are illegal, including payments made unlawful under the Foreign Corrupt Practices Act (see below).
   a. Often the identity of the payee of ransom may not be known.
   b. Query whether evidence of government sponsorship of terrorism/ransom activities would be sufficient to trigger this limitation.

4. IRC § 162(c)(2) similarly restricts the deduction of payments to those who are not government officials or employees "if the payment constitutes an illegal bribe, illegal kickback, or other illegal payment under any law of the United States [or State] … which subjects the payor to a criminal penalty or the loss of license or privilege to engage in a trade or business."
   a. Violations of the sanctions regimes would appear to fall within this category, to the extent that sanctions violations impose criminal penalties.
   b. Query whether local licensing rules could affect such a deduction.

5. Significantly, deduction disallowance under IRC §§ 162(c)(1),(2) must be proven by the IRS. The burden of proof to show that the sanctions regime has been violated, or that a payment violates other U.S. law, here works in favor of the taxpayer.

6. But in addition to these substantive provisions, other provisions may also affect the tax consequences of these payments. For example, information reporting requirements are imposed on payments for independent contractors providing services when the aggregate payment is $600 or more. See IRC § 6041A(a). In order to comply, the recipient must furnish the name, address, and identification number. See IRC § 6041A(f).
   a. Good luck with getting that information from the kidnapper.
   b. IRC § 6722 provides a penalty of $250/incident for the failure to furnish such statements or furnishing incomplete or incorrect statements.
   c. IRC § 6721 imposes a penalty of $250/incident for the failure to file correct information returns with the IRS.
   d. IRC § 6724 excuses such penalties where failure is "due to reasonable cause and not to willful neglect." Query whether this context meets the criteria for relief?
   e. While Federal tax law does not disallow deductions for amounts that are not reported, see Robert Wood, Can Failing to Issue Forms 1099 Preclude Settlement Deduction, Tax Notes, March 19, 2012 at 1565 (answering no). But note: you still have to prove that you made the payment.
   f. States, including California, may take the position that they may deny deductions for amounts not timely reported on Form 1099. See

https://www.ftb.ca.gov/professionals/taxnews/2014/June/07.shtml (last visited December 9, 2015).

7. And what about foreign payees? Payors may be subject to withholding requirements on payments to non-U.S. Persons *if* the payment constitute gross income from sources within the U.S. See IRC § 1441; 1442.
   a. It is unclear whether ransomware will involve activities sufficient to connect the payee to the United States.
   b. Treaty provisions may also apply.
   c. *De minimis* exclusion rules could apply, but not likely. See IRC § 861(a)(3).
   d. Tax risk here: if you are subject to withholding and fail to withhold, you may be liable for the unpaid withholding tax. See IRC § 1461. Consider it another cost associated with ransom!

C. Civil Liability under the Alien Tort Statute?

The Alien Tort Statute of 1789 (ATS) presents another consideration. The ATS states: "The district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States." Suppose A makes a payment to F for the purpose of ransoming its data. A knows that F is connected to a foreign government engaged in crimes against humanity. B, a foreign national, is injured by terrorist activities carried on by F. Could A become liable in tort to B on account of this payment?

1. This jurisdictional statute permits a cause of action for private claims based on treaties and customary international law. See *Kiobel v. Royal Dutch Petroleum Co.*, 133 S.Ct. 1659, 1663 (2013). In *Kiobel*, the Court held that claims for violations of the law of nations occurring outside the United States, and which occurred within the sovereign territory of other nations, were outside the scope of the ATS.
   a. The Court also explained that the ATS may address claims involving piracy on the high seas, which is outside the territorial sovereignty of the United States but not within the sovereignty of another nation. See id. at 1667-69.
   b. Pirates are *sui generis*, as they are considered "fair game wherever found, by any nation, because they generally did not operate within any jurisdiction."
   c. Query: Are data thieves similar to pirates? Should their actions be considered akin to being on the high seas, given the practical challenges of reaching them via the Internet?

2. Case law restricts the ATS to violations of treaties or customary international law which affect relationships between states or between an individual and a foreign state, rather than matters that occur purely between individuals. See, e.g., *Mastafa v. Chevron Corp.*, 770 F.3d 170, 180 (2nd Cir. 2014). For example, neither stealing nor murder between individuals would be included. Id. at 180-81. However, genocide or crimes against humanity could qualify.

3. Not only must the tort meet the hurdle of a violation of customary international law, but it also must "touch and concern the territory of the United States … with sufficient force to displace [a] presumption against extraterritorial application." See *Kiobel v. Royal Dutch Petroleum Co.* 133 S.Ct. 1659, 1669 (2013).
   a. *Mastafa,* supra, involved a clam against a U.S. oil company and a French bank involving actions in support of Saddam Hussein, which did indeed constitute violations of the law of nations. See 770 F.3d at 180.
   b. But merely having a HQ in the U.S. and presumably making decisions there does not satisfy the touch and concern standard. See id. at 188. While some courts may consider citizenship or residency as a factor, the Second Circuit rejects this in favor of focusing on conduct in the U.S. See id. at 188-89; see also Doe v. Drummond, 782 F.3d 576, 586-92 (11th Cir. 2015) (surveying various circuits on "touch and concern" analysis.
   c. Conduct deemed sufficient in *Mastafa* included originating and executing financial transactions in the United States that were connected to the regime, as well as purchasing and financing sales of Iraqi oil in the United States. 770 F.3d at 189-91.

4. The plaintiffs in *Mastafa* raised aiding and abetting, as well as conspiracy or joint criminal enterprise theories. According to the Second Circuit, it is an open question whether conspiracy liability satisfies the customary international law standard. The court merely assumes these theories could satisfy the standard for purposes of analysis. See id. at 181. Instead, it focuses on a standard for aiding and abetting that would satisfy the "touch and concern" requirement. (The Eleventh Circuit sees this differently, recognizing an aiding and abetting theory independently of whether this may be part of international law. See Doe v. Drummond, 782 F.3d 576, 597-98 (11th Cir. 2015)).

5. According to the Second Circuit in *Mastafa*, an aiding and abetting theory requires not merely knowing of alleged abuses, but sharing a purpose in achieving them. Basing its analysis on prior cases, including *Presbyterian Church of Sudan v. Talisman Energy, Inc.*, 582 F.3d 244 (2d Cir. 2009), the court explained:

> The relevant inquiry at all times is whether plaintiffs' complaint "supports an inference that [defendants] acted with the 'purpose' to advance the Government's human rights abuses," *Presbyterian Church,* 582 F.3d at 260, *not* whether defendants merely *knew* that those abuses were occurring and that defendants' business was enabling such acts. Plaintiffs' allegations that defendants *intentionally* flouted the sanctions regime for profit, or that they *knew* their actions were in violation of United Nations Security Council resolutions, or "international law," or U.S. policy are irrelevant to the *mens rea* inquiry; rather, our analysis necessarily focuses on allegations that defendants *intended* to aid and abet violations of

customary international law carried out by the Saddam Hussein regime—a contention that is unsupported by the facts alleged in the complaint.

Mastafa, supra, 770 F.3d at 193. See also *Drummond, supra* (following a similar approach on the matter of aiding and abetting).

6. In other words, liability under this provision is highly unlikely for the typical ransom payor.

D. Foreign Corrupt Practices Act?

The Foreign Corrupt Practices Act of 1977 ("FCPA"), as amended, 15 U.S.C. Sections 78dd-1 *et seq*, prohibits payments to foreign government officials to assist in obtaining or retaining business or directing business to any person.[44] The anti-bribery provisions[45] of the FCPA applies to all U.S. persons or companies, companies with securities listed in the United States, and to foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the United States.[46] The FCPA prohibits the use of mails or any "means or instrumentality of interstate commerce" in furtherance of any offer, payment, promise to pay, or authorization of payment.[47]

The civil or criminal enforcement[48] of the FCPA is shared between the Department of Justice, Fraud Section of the Criminal Division, FCPA Unit and the Securities and Exchange Commission, Enforcement Division. The FCPA Unit also partners regularly with the FBI and its International Corruption Unit. The Department of Homeland Security, the Internal Revenue Service Criminal Investigation, and the Department of Treasury Office of Foreign Asset Control also investigate FCPA violations.

The core principle to criminalize bribery in international commercial transactions was accomplished with member and non-member countries of the Organisation for Economic Co-operation ("OECD") in the Convention on Combating Bribery of Foreign Officials in International Business Transactions (the "Anti-Bribery Convention"). All of

[44] The publication "A Resource Guide to the U.S. Foreign Corrupt Practices Act" is an excellent resource and is the result of extensive research by the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission. A copy can be found at www.justice.gov.
[45] The FCPA also has accounting provisions for companies whose securities are listed in the United States requiring corporations to make and keep books and records that fairly and accurately reflect transactions and devise and maintain an adequate system of control.
[46] 15 U.S.C. sec. 78dd-1(a)[issuer of securities], 15 U.S.C. sec. 78dd-2(a)[domestic concern], 15 U.S.C. sec. 78dd-3(a)[foreign individual or company].
[47] The phrase "interstate commerce" has specific importance to a ransomware payment and the application of the FCPA because it is defined in specific part to means "communication among the several States, or between any foreign country and any State…include[ing]…a telephone or other interstate means of communication." 15 U.S.C. sec. 78dd-2(h)(5) and 15 U.S.C. sec. 78dd-3(f)(5).
[48] A FCPA violation generally is not the only criminal act. The Travel Act, 18 U.S.C. sec. 1952, prohibits using the mail or any facility in interstate commerce with the intent to distribute proceeds of any unlawful activity or to promote, manage, establish, or carry on any unlawful activity. *Id*. Mail and wire fraud are likely implicated too.

the signatories are also members of the OECD's Working Group on Bribery, which monitors the implementation of the Convention.[49]

The criminal penalties for violating the FCPA's anti-bribery provision are significant, up to a $2 million for companies and $100,000 and 5-years of imprisonment for individuals.[50] The civil penalties are only slightly less allowing for $10,000 fines for companies and individuals.[51] Given the substantial penalties, it would seem reasonable that a company or individual making a ransom payment to recover data lost in a ransomware scheme would be immune.

Unfortunately, this currently is not true. In *United States v. Kozeny*, 582 F.Supp.2d 535, 540 (S.D.N.Y. 2008), the United States District Court for the Southern District of New York ruled that only extortion or duress under the threat of imminent physical harm would excuses the conduct.[52] The facts of this FCPA case involve a detailed discussion of Azerbaijan law and the general legal principle that an individual is not guilty of a criminal offense when forced to do so by duress or extortion. The defendant Frederic Bourke, Jr. argued for a jury instruction arguably following the Azerbaijan Criminal Code Economic where extortion was an exception to criminal prosecution. The court firmly rejected this argument and noted that economic coercion—an exact description of ransomware—is not considered immunized conduct.[53]

Some key additional requirements are listed below.

1. There must be a connection between the payor and payee involving a foreign government, public international organization, and any conceivable agent or agency of either.[54]

2. The Act requires knowledge, which is defined to include direct knowledge where the person is aware that conduct is occurring, indirect knowledge where the circumstances exist or there is an awareness that the result is substantially certain to occur, or a firm belief that circumstances exist or that such result is substantially certain to occur.[55]

3. An exception exists for payments to a foreign official to expedite or secure the performance of a routine governmental action[56], while affirmative

[49] www.oecd.org, generally. The OECD on December 2, 2014, launched the Foreign Bribery Report. Of interest is the Reports discussion of sanctions per country. The United States is listed as sanctioning 128 separate foreign bribery schemes since becoming a signatory in February 1999, while the next closest is Germany with 26.
[50] 15 U.S.C. sec. 78dd-2(g)(1)(A) and 15 U.S.C. sec. 78dd-3(e)(1)(A).
[51] 15 U.S.C. sec. 78dd-2(g)(1)(B) and 15 U.S.C. sec. 78dd-3(e)(1)(B).
[52] *See United States v. Gonzales*, 407 F.3d 118, 122 (2nd Cir. 2005)(actions taken under duress do not ordinarily constitute a crime).
[53] S. Rep. No. 95-114, at 10 and 11.
[54] 15 U.S.C. sec. 78dd-1(a)[issuer of securities], 15 U.S.C. sec. 78dd-2(a)[domestic concern], 15 U.S.C. sec. 78dd-3(a)[foreign individual or company].
[55] 15 U.S.C. sec. 78dd-1(f)(2), 15 U.S.C. sec. 78dd-2(h)(3), 15 U.S.C. sec. 78dd-3(f)(3).
[56] 15 U.S.C. sec. 78dd-1(b), 15 U.S.C. sec. 78dd-2(b), 15 U.S.C. sec. 78dd-3(b).

defenses include lawful payments under the written laws of the payor's government or public international organization or reasonable, bona fide expenditures such as travel or lodging directly related to promotion, demonstration, explanation of services or the execution or performance of a contract with a foreign official.[57]

4. A ransomware scenario would not usually appear to trigger the FCPA given the threshold requirement that the payment must be made to assist in obtaining or retaining business for the individual or company or directing that business to another person. The related enforcement actions seem to support this observation.[58]

5. Query, however, whether FCPA violation could occur in unusual situations. For example, suppose a hacker demands a ransom payment with a quid pro quo: "if you don't pay then I will tell the foreign contracting officer to cancel your contract"? There is at least some hint the hacker has a relationship with the foreign official. Moreover, the payment of the ransom appears to insure retention of the contract. The scenario falls outside the affirmative defenses provided; it is arguably a "knowing" payment unless facts exist to show a reasonable basis for disbelief concerning a relationship between the hacker and foreign official.

V. Altering the Legal Regime: Policy Options

Ransom crimes are likely to continue as long as they are profitable. Profitability requires a market for ransom payments and the continued means to carry out the crime. As discussed above, technology can provide constraints on the efficacy of both human and data ransoming efforts, but it also facilitates those efforts. Data security regulation, disclosure laws, and threats of liability can help nudge firms toward investing in greater security, making the cybercriminal's task more difficult.

Once crimes have occurred, territorial jurisdiction constrains governmental efforts to catch the perpetrators. International coordination of law enforcement efforts can help make crime less profitable by raising the prospects for detection and punishment, thereby increasing the relative costs. AML regimes present some steps in this direction, making it more costly and difficult to get payments into the hands of the perpetrators. But as noted, these efforts fall short of a comprehensive approach. They are also costly. And unfortunately, intergovernmental cooperation with some countries is just not going to happen.

The U.S. government's policy against paying ransom for hostages presumably reflects an attempt to constrain the size of the market for ransom payments. But the federal government can

[57] 15 U.S.C. sec. 78dd-1(c), 15 U.S.C. sec. 78dd-2(c), 15 U.S.C. sec. 78dd-3(c).
[58] A few of the enforcement actions concluded in 2015 are: U.S. v. Mikerin, United Stated District Court Maryland, Docket No. 8:14-cr-529 (Russian official plead to conspiracy to commit money laundering for arranging corrupt payments to Russian official) and U.S. v. McClung, United States District Court New Jersey, Docket No. 3:15-cr-537(employee of Berger Group Holdings plead to violations of FCPA for bribing Vietnamese government official for business).

afford to take this approach. After all, it has other policy tools to address kidnappers – including military force. The moral calculus for what one should do in a particular case may also change when the victim is one of your family members or close associates.[59] Ransoms for data may implicate slightly different ethical considerations, as loss of life is not implicated. However, if data may be lost, or worse, customer data may be disclosed or exploited as a consequence of failing to ransom that data, severe economic costs are presented as a tradeoff. Moreover, some business entities may find that they owe a fiduciary obligation to avoid costs that could affect their customers through data losses and/or disclosures.

Paying ransoms presents a classic collective action problem. The fact that one firm will deem it more expeditious to pay the ransom than to suffer the consequences (assuming that the cybercriminal will follow through after all) translates into a particular gain from trade. The payment may produce a short-term advantage for the firm (i.e., freedom from encryption, loss, or data disclosure), but it potentially enhances the long-term prospects for external threats against other firms. The future threat may not materialize if the firm invests in technology and continues to make that investment to keep ahead of the cybercriminals. In fact, the threat is likely the greatest for firms that invest less in protection. It is costly to stay ahead – an arms race between the cybercriminals and firms trying to stay ahead of them will likely benefit the security industry.

Demands for bribes by government officials present an analogous problem. In a particular case, it may be preferable to pay the bribe and obtain the gain from trade that accompanies the transaction. However, without a collective effort to refuse (an anti-bribery cartel, so to speak), firms that pay bribes will not only gain an advantage over others, but will also likely stimulate more demand for bribes in the marketplace.

Laws such as the FCPA reflect an alternative approach to this problem, in that they seek to address the collective action problem for bribes through attacking those on the payment side. Not only does this provide a catalyst for changing corporate culture, as compliance efforts become key to avoiding violations and attendant penalties, but it also overcomes jurisdictional problems that would otherwise be presented by focusing on the payee side. Interjurisdictional cooperation could help by taking aim at corrupt officials, the payor side's unwillingness to breach the FCPA likely constrains the demand from those officials, or channels it toward those countries and firms with weak compliance efforts.

Could adding new laws that impose legal sanctions on ransom payors reduce cyber ransom crimes? Currently, firms can choose to pay ransoms when their investments in protective technology (and data backups) fail to prevent the attack, with only limited constraints from sanctions regimes directed at particular actors. Adding new legal penalties on payment, in a manner similar to the FCPA, would make the option of paying ransom more costly, thus nudging firms toward choosing greater security and, in the process, making data ransom crimes more costly for cybercriminals.

However, the prospects of achieving real gains from a new legal regime require further analysis. Such an approach may simply change the locus of cybercrime by driving

[59] "Ransoming the captive" has traditionally been recognized as a corporeal work of mercy in Catholic theology. See http://www.traditionalcatholicpriest.com/2014/03/08/traditional-catholic-7-corporal-works-of-mercy/

cybercriminals toward the weaker targets (as in the case of payment card industry movement to EMV technology driving fraud online and away from brick-and-mortar stores). Moreover, defining the parameters for sanctions, both in terms of covered entities (e.g., large corporations vs. small firms vs. individuals) and covered payments (e.g., winnowing out legitimate services from ransom payments) present interesting problems that deserve further consideration.

EM/IR
121415

Ian Ramsey is his firm's Chief Information Security Officer and Co-chairs his Firm's Privacy and Data Security practice group. He is a Certified Information Privacy Professional (CIPP/US) and an experienced trial attorney. He regularly assists clients in data breach incidents and coordinates with law enforcement on such matters. He also speaks frequently on matters relating to his practice, including most recently a CLE program at the Business Law Section meeting in Chicago, "Cybersecurity Damages: An Overview of Economic Harm Resulting from Data Security Breaches" (September 17, 2015).

Ed Morse is a professor of law and holds the McGrath North Mullin & Kratz Endowed Chair in Business Law at Creighton University School of Law in Omaha, Nebraska. He is also a research scholar in Creighton's Institute for Economic Inquiry. He has written several articles on payment systems and security issues, as well as on other aspects of Internet regulation. He co-chairs the Electronic Payments and Financial Services subcommittee and is the editor of "Electronic Payments in the 21st Century", a book project sponsored by the Cyberspace Law Committee which has been approved for development for the ABA.