Ransomware Payment: Legality, Logistics, and Proof of Life

Part Two: Investigation and Response | by John Reed Stark

Ransomware is a crime, has significant regulatory implications and can involve important legal responsibilities and liabilities. At a minimum, ransomware schemes run afoul of the federal computer crime statute, 18 U.S.C. § 1030, and particularly subsection (a)(7), which forbids hacking intended to extort something of value from the victim.

Above all else, the legal ramifications of any ransomware incident or failure can be calamitous for any public or private company. Even the most traditional realms of IT dominion such as exfiltration analysis, malware reverse engineering, digital forensics, logging review and most technological remediation measures are rife with legal and compliance issues and a myriad of potential conflicts.

For instance, after a cybersecurity incident such as a ransomware attack, law enforcement, regulators, vendors, partners, insurers, customers and others may:

- Request forensic images of impacted systems;
- Demand copies of *indicators of compromise*;
- Mandate that their own auditors or examiners visit sites of infiltration and conduct their own audit and investigation;
- Want to participate in remediation planning;
- Seek interviews and interactions with IT personnel;
- Require briefings from a victim company's forensic experts and data security engineers; or
- Ask to attach a recording appliance to a victim company's network in hope of capturing traces of attacker activity, should an attacker return.

These requests raise a host of legal issues, including how exactly to respond to each request and whether any response would violate the privacy of customers, be at odds with commercial agreements, result in a waiver of the attorney-client or work product privileges or have any other legal/compliance consequences.

Because so many incident response issues are critical to the very survival of a company, who else but the GC can oversee and direct investigative workflow, commanding the investigation and remediation for the C-suite, sharing with senior management the ultimate responsibility for key decisions, while having the responsibility and duty of reporting to the company's board.

First published on the Nasdaq Governance Clearinghouse

RANSOMWARE AND THE ATTORNEY-CLIENT PRIVILEGE

Attorney involvement, awareness, leadership, and direction are not the only essentials for managing the quagmire of legal issues arising during a ransomware response. GC involvement also triggers the protections afforded by the attorney-client and work product privileges, a critical component in the response to data security incidents.

The involvement and direction of counsel in the context of any investigation will presumably apply to the work product produced not only directly by the legal team members but also by the outside advisors, including the digital forensic investigators engaged by internal or external counsel.

This is standard practice in the context of any other type of investigation – a cyber incident is no different. There is nothing nefarious or extraordinary about this approach, it is a time-honored and tested standard operating procedure. The involvement of counsel establishes a single point of coordination and a designated information collection point.

Counsel as quarterback of ransomware response also enhances visibility into the facts, improves the ability to pursue appropriate leads and, most importantly, ensures the accuracy and completeness of information before it is communicated to external audiences. Otherwise, incomplete and/or inaccurate information could be released, only to have to later be corrected or even retracted.

RANSOMWARE INVESTIGATIVE TACTICS

While determining the bona fides of a ransomware strain is always challenging, an experienced digital forensic examiner can find some answers by searching for some of the more typical cyber-indicators. Ransomware malware is characteristically a type of tool, which is not only known to most professionals, but may even be readily available for purchase online. If the name and modus operandi of the ransomware is new or otherwise unknown, rather than a victim firm being "patient zero," the ransomware may turn out to be bogus.

Digital forensic experts can also research the Bitcoin payment address, the malware message, any relevant phishing emails, and any other of the ransomware characteristics in data security research forums and internal archives to analyze recent commentary about the ransomware and test its efficacy and validity.

There are also a range of digital forensics tests to initiate upon an infected file to assess a ransomware strain's actual efficacy. For instance, one simple test is to return the file name to its original form. Real ransomware changes the file extension of encrypted files. The ransomware files may not be encrypted but just renamed to provide the illusion of encryption to cajole a ransom payment. A digital forensics expert can also investigate the severity of the attack, reverse-engineer the malware that has taken control of victim data and attempt a full-fledged data recovery.

RANSOMWARE PAYMENT LOGISTICS

In cases where a particular ransomware attack cannot be fully mitigated, an experienced digital forensics firm can broker and validate a solution that minimizes the cost of recovery and prevents further extortion from the attacker.

Paying off the ransomware attackers typically entails: 1) sending the secret ransomware key file now stored on the victim's computer; 2) uploading that file (or data string) to the attackers together with a Bitcoin payment; and 3) awaiting a decryption key or a tool a victim can use to undo the encryption on the victim company files. This is a complex and challenging process.

First off, a digital forensics firm can help a ransomware victim navigate the maze of setting up an account to handle Bitcoin, getting it funded, and figuring out how to pay other people with it. A digital forensics examiner may even be able to construct a payment scheme where rendering ransomware payments is *conditional*. By using cryptocurrency features to ensure that ransomware attackers cannot receive their payment unless they deliver a key, there can exist some added level of security and reliability upon the transaction. One ransomware response expert notes:

" … A ransomware developer could easily perform payment via a smart contract script (in a system like Ethereum) that guarantees the following property: *This payment will be delivered to the ransomware operator if and only if the ransomware author unlocks it – by posting the ransomware decryption key to the same blockchain.*"

Ransomware attackers may present the entire ransomware payment process as more akin to an ordinary business transaction than an international extortion scheme. In fact, some recent ransomware attackers purportedly even offer a victim company a discount if the victim company transmits the infection to other companies, just like referral programs of Uber or Lyft.

However, while a ransomware payment process may seem straightforward and rudimentary, the reality is far more intricate and risky. No ransomware payment process can guarantee that the ransomware attacker will provide a decryption key. The ransomware scheme may be nothing more than a social engineering ruse, more like an old fashioned Nigerian Internet scam than a malware infection – and the payment could end up being all for naught.

Indeed, ransomware attackers may no longer have the encryption key or may just opt to take a ransom payment, infect a company's system, and flee the crime scene entirely. Not only is the system of paying in untraceable Bitcoin risky, but the transaction in its entirety is so risky, it hardly seems palatable. Nonetheless, the number of victim companies that pay ransomware demands continues to grow at an alarming rate.

THE LEGALITIES OF RANSOMWARE RESPONSE

Though the FBI has hinted at the possible illegality of paying a ransomware demand, the FBI has never specifically stated that the payer could actually be charged with a crime. It would seem rather obvious that with respect to any criminal statute, actions taken under duress do not ordinarily constitute a crime. Moreover, the ransomware attacker has the criminal intent, not the victim who agrees to pay. However, there is scant specific legal authority on the subject of payment and negotiation with ransomware attackers, so the legalities of payment are worthy of some analysis.

In general, legal commentary and case law regarding ransom payments is limited. However, in a germane 2011 British case, Masefield AG v Amlin Corporate Member Ltd (The Bunga Melati Dua), relating to maritime piracy and ransom demands for safe return of the vessel and crew, the court faced a somewhat analogous scenario. Specifically, the British Court of Appeal held that there was no general public policy argument against paying ransoms, stating that:

" . . . there is no universal morality against the payment of ransom, the act not of the aggressor but of the victim of piratical threats, performed in order to save property and the liberty or life of hostages. There is no evidence before the court of such payments being illegal anywhere in the world. This is despite the realization that the payment of ransom, whatever it might achieve in terms of the rescue of hostages and property, itself encourages the incidence of piracy for the purposes of exacting more ransoms. (Perhaps it should be said that the pirates are not classified as terrorists. It may be that the position with regard to terrorists is different)."

Though addressing hostage ransoms, and not ransomware, former President Barak Obama provided a similar message in his Statement by the President on the U.S. Government's Hostage Policy Review (June 24, 2015):

"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. 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 . . . In particular, I want to point out that no family of an American hostage has ever been prosecuted for paying a ransom for the 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."

RANSOMWARE AND THE FCPA

The Foreign Corrupt Practices Act of 1977 (FCPA) prohibits payments to foreign government officials to assist in obtaining or retaining business or directing business to any person. Laws such as the FCPA reflect an alternative approach to deterring bribes, by penalizing those on the payment side of the transaction.

Specifically, the FCPA prohibits giving something of value for the purpose of "(i) influencing any act or decision of [a] foreign official in his official capacity, (ii) inducing such foreign official to do or omit any act in violation of the lawful duty of such official, or (iii) securing any improper advantage … to obtain or retain business for or with …

any person." The law provides an affirmative defense for payments that are "lawful under the written laws and regulations" of the country.

Given the FCPA threshold requirement that a payment must be made to assist in obtaining or retaining business for the individual or company or directing that business to another person, a ransomware scenario does not appear to trigger the FCPA.

However, FCPA's enforcement can provide a useful analogy when considering the legalities of paying a ransomware demand. U.S. companies often face extortionate demands from foreign police, bureaucrats, and regulators, who threaten to hold, expel or even harm employees if ransoms are not paid. And there have always been questions whether those involuntary payments can violate the FCPA. The DOJ-SEC Guidance on FCPA addresses this issue, stating:

"Does the FCPA Apply to Cases of Extortion or Duress? Situations involving extortion or duress will not give rise to FCPA liability because a payment made in response to true extortionate demands under imminent threat of physical harm cannot be said to have been made with corrupt intent or for the purpose of obtaining or retaining business."

This notion, that under FCPA an individual is not guilty of a criminal offense when forced to do so by duress or extortion, is confirmed in *United States v. Kozeny*, 582 F.Supp.2d 535, 540 (S.D.N.Y. 2008). Specifically, in the Kozeny decision, the United States District Court for the Southern District of New York ruled that extortion or duress under the threat of imminent physical harm would excuse the conduct (essentially negating a corrupt intent), stating:

" . . . while the FCPA would apply to a situation in which a "payment [is] demanded on the part of a government official as a price for gaining entry into a market or to obtain a contract," it would not apply to one in which payment is made to an official "to keep an oil rig from being dynamited," an example of "true extortion." The reason is that in the former situation, the bribe payer cannot argue that he lacked the intent to bribe the official because he made the "conscious decision" to pay the official. In other words, in the first example, the payer could have turned his back and walked away—in the latter example, he could not."

Whether the "economic duress" of a typical ransomware attack would rise to the level of "true extortion" as described in the Kozeny decision remains untested and might be viewed as insufficient to excuse conduct from sanctions under the FCPA.

The FCPA could also potentially apply in ransomware scenarios where the cyber-criminal has a known connection to a foreign government. While the concealed identity of cyber-criminals involved in ransomware attacks likely prevents a payer from knowing that a payment violates the FCPA, the issue could still arise when a digital forensic expert identifies a ransomware attacker's modus operandi to be that of a state sponsored organization (e.g. from Russia, North Korea or Iran).

FOREIGN SANCTIONS AND RANSOMWARE

Like the FCPA, international sanctions regimes are also designed to prevent payments to certain designated payees, institutions, and countries who are enemies of the U.S, such as terrorists and terrorist organizations. In the United States, the Treasury's Office of Foreign Asset Controls (OFAC) supervises these programs, such as the Trading with the Enemy Act and the International Emergency Economic Powers Act (IEEPA).

Under these Acts, ransom payments (whether directly or indirectly through an intermediary) to Foreign Terrorist Organizations (FTOs) or Specially Designated Global Terrorists (SDGTs) identified by 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 IEEPA.

For example, in a February 2017 cyber-attack against the British National Health System, the attackers appeared to be ISIS and in particular, the "Tunisian Falange Team," which posted graphics and pictures aimed at the war in Syria. Whether a similar attack against a U.S. hospital, with a similar evidentiary trail indicating terrorist attribution, would trigger the limitations imposed by the OFAC is unclear and untested. However, any digital forensic findings indicating terrorist attribution or involvement is certainly worthy of consideration when contemplating a ransomware payment under such circumstances.

RANSOMWARE AND CONSPIRACY

Whether a payer of a ransomware demand can be held to have entered into a conspiracy with the ransomware attacker seems unlikely and contrary to the public interest. A conspiracy is an agreement with another that a criminal course of conduct is to be pursued. Ransomware payments do not appear to be the kind of agreements contemplated by conspiracy statutes, but instead are forced arrangements dictated by a ransomware attacker.

However, non-victim participants in the Bitcoin payment scheme to pay a ransomware attacker might still find themselves facing criminal penalties. Anthony Murgio, who pled guilty to operating as a money transmitter without a license in 2015, was also charged with violating Title 18 U.S.C., Section 1030(a)(7) and sentenced to 5 ½ years in prison. Federal prosecutors alleged that Murgio and his co-conspirators benefitted from transactions providing victims with Bitcoin to pay off ransomware demands. The indictment states:

"As part of the unlawful Coin.mx scheme, Anthony P. Murgio, the defendant, and his co-conspirators knowingly processed and profited from numerous Bitcoin transactions conducted on behalf of victims of ransomware schemes… By knowingly permitting ransomware victims to exchange currency for Bitcoins through Coin.mx, Murgio and his co-conspirators facilitated the transfer of ransom proceeds to the malware operators while generating revenue for Coin.mx."

Unlike a ransomware payer, Murgio was allegedly a part of the payment process and clearly facilitated the ransomware transactions with *unclean hands* – possessing the kind of nefarious intent required for money laundering criminal liability. Crypto-currency sellers or exchange operators may be caught up in legal trouble if they have avoided or neglected reporting requirements or have not registered as a money transmission business (like Murgio), or, if they were complicit with the ransomware attackers.

The distinction seems clear: if a Bitcoin seller actively aided and abetted a ransomware attacker, knowingly profiting from the scheme, the Bitcoin seller could be criminally liable. However, if a digital forensics firm made Bitcoin available to a client and provided technical advice as to how to pay in Bitcoin, then, like Thomas Clayton in *Proof of Life*, criminally liability seems unlikely and wholly inappropriate.

RANSOMWARE AND AML

Anti-money laundering (AML) regulations have evolved into a complex array of compliance obligations for any financial organization, especially embryonic virtual currency companies such as Bitcoin, who have become useful, convenient and effective tools for ransomware attackers. Along those lines, The U.S. Department of Justice (DOJ), together with FinCEN have become increasingly active in policing ransomware, leveraging AML statutes and regulations as their preferred statutory weaponry. For instance, in addition to being charged for violating computer crime Title 18 U.S.C., Section 1030(a)(7), Anthony Murgio, a ford Bitcoin exchange operator, also pled guilty to operating as a money transmitter without a license in 2015, and was sentenced to 5 ½ years in prison. Federal prosecutors alleged that Murgio and his co-conspirators benefitted from transactions providing victims with Bitcoin to pay off ransomware demands. The indictment states:

"As part of the unlawful Coin.mx scheme, Anthony P. Murgio, the defendant, and his co-conspirators knowingly processed and profited from numerous Bitcoin transactions conducted on behalf of victims of ransomware schemes…By knowingly permitting ransomware victims to exchange currency for Bitcoins through Coin.mx, Murgio and his co-conspirators facilitated the transfer of ransom proceeds to the malware operators while generating revenue for Coin.mx."

Not just a part of the ransomware payment process, Murgio allegedly facilitated the ransomware transactions with *unclean hands* – possessing the kind of nefarious intent required for money laundering criminal liability, which is probably why the Murgio prosecution also addresses AML liability in a ransomware scheme. Specifically, the issues relate to the failure of Murgio and his cohorts to:

- Register with the Financial Crimes Enforcement Network (FinCEN) (see FinCEN, MSB and Ransomware discussion below);
- Maintain an effective AML program;
- Comply with AML record-keeping requirements; and
- File with FinCEN *Suspicious Activity Reports* (SARs) regarding customers who needed Bitcoin to pay ransomware demands.

The Murgio indictment also alleges that Murgio and another defendant had undue influence on a federally insured credit union that handled the exchange's banking operations for a period of time, and that they tried to "trick" major financial institutions about the nature of their business.

The Murgio defendants allegedly exchanged at least $1.8 million Bitcoins for cash for certain customers who claimed they were ransomware attack victims needing Bitcoins to "pay off" ransomware attackers. The U.S. Department of Justice (DOJ) stated in their announcement of the prosecutions:

"Through Coin.mx, MURGIO, LEBEDEV, and their co-conspirators enabled their customers to exchange cash for Bitcoins, charging a fee for their service. In doing so, they knowingly exchanged cash for people whom they believed may be engaging in criminal activity. MURGIO and his co-conspirators have also knowingly exchanged cash for Bitcoins for victims of "ransomware" attacks, that is, cyberattacks in which criminals (here, distributors of the ransomware known as "Cryptowall") electronically block access to a victim's computer system until a sum of "ransom" money, typically in Bitcoins, is paid to them. In doing so, MURGIO, and his co-conspirators knowingly enabled the criminals responsible for those attacks to receive the proceeds of their crimes, yet, in violation of federal anti-money laundering laws, MURGIO never filed any suspicious activity reports regarding any of the transactions."

FINCEN, MSBs AND RANSOMWARE SCHEMES

Money Services Businesses (MSBs) have been required to register with FinCEN since 1999, when the MSB regulations first went into effect. MSBs have historically been recognized by FinCEN to include: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks, money orders, or stored value; (4) sellers or redeemers of traveler's checks, money orders, or stored value; and (5) money transmitters.

An entity acting as an MSB that fails to register (by filing a Registration of Money Services Business ("RMSB"), and renewing the registration every two years per 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380), is subject to civil money penalties and possible criminal prosecution.

The registration of the MSB serves as a first step in establishing the compliance framework for applicable FinCEN regulations designed to help mitigate the risks of criminal abuse of MSBs for money laundering and terrorist financing as the MSB seeks to provide financial services to customers for legitimate purposes. There is no cost for registration, which is a simple procedure explained in detail on FinCEN's website at https://www.fincen.gov/money-services-business-msb-registration.

In 2013, FinCEN expanded its MSB definition to include virtual currency exchanges like Bitcoin. Specifically FinCEN issued guidance providing that any virtual currency "exchanger" (i.e., a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency) is a money transmitter (i.e., a person engaged in the business of accepting and transmitting currency, funds or other value that substitutes for currency) under the Bank Secrecy Act (BSA) and its implementing regulations (31 C.F.R. § 1010.100(ff)(5)) and, therefore, required to register with FinCEN as an MSB within 180 days of beginning operations.

The BSA and its implementing regulations require an MSB to develop, implement and maintain an effective written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.

MSB EXPANSION

Recently, FinCEN has begun to expand its definition of an MSB even further, to include not only virtual currency exchanges but also the enablers/financial intermediaries of ransomware schemes. In other words, FinCEN now seeks to penalize the range of financial participants and intermediaries of ransomware schemes, targeting the enablers of ransomware schemes, such as criminally complicit payment facilitators and go-betweens.

For instance, in a July 2017 AML ransomware-related enforcement action, FinCEN, in a joint prosecution by the U.S. Attorney's Office for the Northern District of California, assessed a $110 million civil money penalty against BTC-e a/k/a Canton Business Corporation (BTC-e) for willfully violating U.S. AML laws. Russian national Alexander Vinnik, one of the operators of BTC-e, was also arrested in Greece, and FinCEN assessed a $12 million penalty against him for his role in the violations.

BTC-e is an Internet-based, foreign-located money transmitter that exchanges fiat currency as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. By volume, BTC-e is one of the largest virtual currency exchanges in the world.

According to FinCEN, BTC-e facilitated transactions involving computer hacking, identity theft, tax refund fraud schemes, public corruption, drug trafficking – and ransomware.

Although BTC-e's operation and domicile were outside of the U.S., that did not stop FinCEN or DOJ from its enforcement actions. FinCEN asserted jurisdiction because BTC-e conducts business as an MSB in substantial part within the United States (including $296 million of U.S. customer transactions through U.S servers.)

In announcing the AML fines and prosecutions, Jamal El-Hindi, Acting Director for FinCEN, stated:

"We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. anti-money laundering law. This action should be a strong deterrent to anyone who thinks that they can facilitate ransomware, dark net drug sales, or conduct other illicit activity using encrypted virtual currency. Treasury's FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual currency exchangers and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards."

KEY RANSOMWARE AML TAKEAWAYS

Some key ransomware-related takeaways from the FinCEN/DOJ fines, prosecutions and overall regulatory and enforcement posture towards the alleged "criminal design" of crypto-currency exchanges, are as follows:

- FinCEN and DOJ are expanding AML statutes and regulations to attack ransomware perpetrators as AML criminal enterprises in the same way that DOJ expanded the Racketeers Influenced and Corrupt Organizations Act (RICO) to attack street gangs, gang cartels, corrupt police departments, duplicitous Wall Street bankers and even crooked political campaigns. In so doing, FinCEN and DOJ are turning the tides on ransomware attackers and enablers who exploit the Bitcoin ecosystem to anonymize (i.e. launder) the payments received by their victims. By becoming increasingly sophisticated at coopting the Bitcoin network to establish an AML jurisdictional nexus, FinCEN and DOJ have laid the groundwork to link and prosecute both the masterminds and the foot soldiers of ransomware schemes;
- FinCEN is actively mining BSA data to develop leads on cyber threats including ransomware, and coordinating with an alphabet soup of criminal investigative agencies by sharing critical analytics and by providing tactical and strategic intelligence reports associated with these threats;
- U.S. Regulators and prosecutors will take action against persons or entities in a ransomware scheme under the auspices that they are MSBs who fail to keep BSA/AML controls or know their customers – or even for avoiding or neglecting reporting requirements or not properly registering as money transmission businesses (like Murgio);
- When an offshore person or entity intentionally and maliciously participates and profits within the financial machinations of a ransomware scheme (such as the alleged money laundering by BTC-e and its senior management), a company or person's location overseas is not necessarily a defense to AML charges;
- Companies beset by a ransomware demand should carefully review FinCEN's guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies and obtain compliance advice and counsel when necessary. While legitimate businesses might need to conduct Bitcoin transactions with shady characters, such as unlocking vital systems infected by a ransomware virus, their actions could nonetheless raise AML red flags by facilitating such transactions; and
- The digital forensic firms and other professional service experts that a ransomware victim may engage to help facilitate a ransomware payment or interact with the ransomware perpetrators obviously lack the criminal intent of culprits like the Murgio and Vinnik defendants and co-conspirators, and are merely providing critical technical advice. However, these otherwise innocent consultants may nonetheless find themselves ensnared in a FinCEN AML investigation of the scheme.

RANSOMWARE: TO PAY OR NOT TO PAY

For now, it seems that paying ransomware, while obviously risky and empowering/encouraging ransomware attackers, does not appear to break any laws – and even if payment is arguably unlawful, seems unlikely to be prosecuted. Thus, the decision whether to pay or ignore a ransomware demand seems less of a legal, and more of a practical, determination; almost like a cost-benefit analysis.

The arguments for rendering payment include:

- Payment is the least costly option;
- Payment is in the best interest of stakeholders (e.g. a hospital patient in desperate need of an immediate operation whose records are locked up);
- Payment can avoid being fined for losing important data;
- Payment means not losing highly confidential information; and
- Payment may mean not going public with the data breach.

The arguments against payment include:

- Payment does not guarantee that the right encryption keys with the proper decryption algorithms will be provided;
- Payment further funds additional criminal pursuits of the attacker, enabling a cycle of ransomware crime;
- Payment can do damage to a corporate brand;
- Payment may not stop the ransomware attacker from returning;
- If victims stopped making ransomware payments, the ransomware revenue stream would stop and ransomware attackers would have to move on to perpetrating another scheme; and
- Using Bitcoin to pay a ransomware attacker can put organizations at risk. Most victims must buy Bitcoin on entirely unregulated and free-wheeling exchanges that can also be hacked, leaving buyers' bank account information stored on these exchanges vulnerable.

*John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He also worked for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime, and for five years as managing director of a global data breach response firm, including three years heading its Washington, D.C. office. Mr. Stark is the author of, "The Cybersecurity Due Diligence Handbook," available as an eBook on Amazon, iBooks and other booksellers.