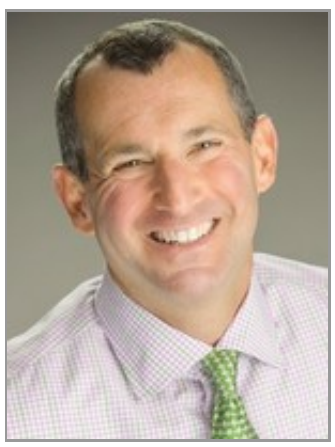
Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Risks In Making A Ransomware Payment

By **John Reed Stark**

Law360, New York (July 10, 2017, 1:05 PM EDT) -- In the 2000 American thriller film "Proof of Life," the title refers to a phrase commonly used to indicate proof that a kidnap victim is still alive. As an expert negotiator in kidnapping cases, Terry Thorne, played by Russell Crowe, is engaged to bargain for a corporate kidnap victim's safe return.



John Reed Stark

The film "Proof of Life" is not just a compelling narrative — its premise and main character also provide some useful insights into managing the emerging threat of ransomware. Ransomware, a special and more nascent type of malware, prevents or limits users from accessing their data, by locking system screens or user files, unless and until a ransom is paid.

The "Proof of Life" screenplay was partly inspired by Thomas Hargrove's book "The Long March to Freedom,' which recounts how the release of the once-kidnapped Hargrove was negotiated by Thomas Clayton, the founder of his eponymous kidnap-for-ransom consultancy Clayton Consultants (now part of risk management firm Triple Canopy Inc.).

Just like Clayton Consultants, the team advising a ransomware victim company, whether a hospital or global corporate conglomerate, must employ a thoughtful, careful and methodical protocol to survive the ransomware crisis. Like any hostage situation, when a cyberattacker locks up critical data files, the logistics and legalities of ransomware refusal, acquiescence or capitulation can be both elaborate and complicated.

To make matters worse, seeking law enforcement help for a ransomware attack unfortunately remains a very limited option. First, law enforcement has become inundated with ransomware reports and lacks the resources and wherewithal to assist victims. Second, most of the ransomware attackers are overseas, where merely obtaining an electronic evidence or interviewing a witness, let alone successful extradition and prosecution, are rarely possible. Finally, ransomware demands are often at monetary levels in the hundreds or thousands of dollars — too small to warrant federal law enforcement consideration while clearly outside of the jurisdiction of local law enforcement.

Thus, it should come as no surprise that a significant number of ransomware victims opt to pay the ransom. When padlocked files are business-critical (e.g., an important intellectual property formula); when encryption cannot be defeated (no matter how good the code-breaker) or when time is of the essence (e.g., when patient data is needed for life-saving surgery), paying the ransom can become the proverbial best worst option. Moreover, the typically de minimus ransomware payment demands (on average, about $679) are more akin to a financial nuisance than a material fiscal line item, so from a cost-benefit perspective, payment can make the most sense.

Under any circumstance, ransomware has quickly become a novel, multifaceted and emerging risk to all corporate enterprises, and like any other material risk, should be addressed and mitigated in

a reasonable, lawful, robust and effective manner.

This article provides guidance on the unique legal issues that can arise when seeking proof of life and opting to meet the monetary demands of ransomware attacker.

What Is Ransomware?

Ransomware is a type of malicious software that infects a computer and restricts users' access to certain data, systems and/or files until a ransom is paid. Ransomware can come in many forms and iterations and like any other virus or infection, ransomware can evolve and transmogrify to counter cyber defenses and remediation. Although only a fraction of ransomware attacks are actually reported to federal authorities, the U.S. Department of Justice reports over 4,000 ransomware attacks occur daily.

A ransomware victim company's files are rarely exfiltrated by a ransomware attacker, rather the attacker encrypts the files so a victim company cannot access them. Then the hacker offers to sell the encryption key to the victim, typically payable in an anonymizing online cryptocurrency such as Bitcoin. The usual ransomware demand comes with a deadline — after which time, the ransomware attacker threatens that the key will be destroyed or will expire, rendering the kidnapped files forever inaccessible. In many cases the ransom note that hijacks the victim's screen is accompanied by a digital clock ominously ticking down the minutes and seconds from 72 hours. When the timer expires, the ransom demand usually goes up or even doubles — or the data is permanently locked and henceforth unrecoverable.

Bitcoin and other convertible cryptocurrencies have become the keystone to current ransomware schemes, rendering the transactions practically untraceable and well suited for criminal transactions. Unlike the sequence of events during to a common kidnapping scenario, where the exchange of money arguably places criminals in their most vulnerable position, virtual kidnapping of ransomware actually facilitates anonymity throughout the Bitcoin transaction process.

Ransomware Payment

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. Cryptographer and ransomware expert (and Johns Hopkins professor) Matthew Green 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 portray 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 complicated and rife with challenges. First off, while a digital forensics firm can

validate a solution that minimizes the cost of recovery and prevents further extortion from the attacker, 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, with reports that as many as 70 percent of ransomware victims paid the ransom.

The Legalities of Ransomware Payment

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 possesses the requisite level of criminal intent, not the victim who agrees to pay. However, there is little 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:

> [T]here 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 Barack 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 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, the 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 U.S. Department of Justice-U.S. Securities and Exchange Commission guidance on the 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 the 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 U.S. District Court for the Southern District of New York ruled that extortion or duress under the threat of imminent physical harm would excuses the conduct (essentially negating a corrupt intent), stating:

> [W]hile 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 cybercriminal has a known connection to a foreign government. While the concealed identity of cybercriminals 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 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 cyberattack against the British National Health System, the attackers appeared to be ISIS and in particular, the Tunisian Falange Team, which posted graphics and pictures decrying 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 OFAC is unclear and untested. However, any digital forensic findings of a ransomware attack indicating terrorist attribution or involvement, is certainly worthy of consideration when contemplating a ransomware payment.

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, other profiting and culpable participants in the Bitcoin payment scheme to pay a ransomware attacker might find themselves facing criminal penalties. Anthony Murgio, who recently 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 five and a half years in prison. Federal prosecutors alleged that Murgio and his co-conspirators benefited from transactions providing victims with Bitcoin to pay off ransomware demands. The Murgio 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 a part of the payment process and clearly facilitated the ransomware transactions with unclean hands — possessing the kind of felonious intent required for money laundering criminal liability. Cryptocurrency 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 criminally 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," criminal liability seems wholly inappropriate.

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 ransomware attacker will ultimately provide the right encryption keys with the proper decryption algorithms;
- 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 crypto-exchanges vulnerable.

Final Thoughts

When confronted with a ransomware attack, the options all seem bleak. Pay the hackers — and the victim may not only prompt future attacks, but there is also no guarantee that the hackers will restore a victim's dataset. Ignore the hackers — and the victim may incur significant financial damage or even find themselves out of business. The only guarantees during a ransomware attack are the fear, uncertainty and dread inevitably experienced by the victim.

Even under the best-case scenario, where a victim has maintained archives and can keep their business alive, the victim companies will incur significant remedial costs, business disruptions and exhaustive management drag. Moreover, having a backup storage solution in place is not always ideal; not only can outside storage of data create additional cybersecurity risks, but sometimes data archives are more like the proverbial roach motels, where data checks in but it can't check out.

No doubt that the ease, anonymity and speed of cryptocurrency payments such as Bitcoin, has revolutionized the ransomware industry, prompting its extraordinary growth. Bitcoin not only makes it simpler to remain anonymous, but also enables a nameless payment mechanism where the extorted funds can be immediately transferred into criminal hands.

Transactions in cryptocurrencies like Bitcoin lack a discernable audit trail and operate outside of regulated financial networks and are alarmingly unregulated. There is no central issuer of Bitcoins, nor a Federal Reserve of Bitcoins monitoring and tracking transactions or controlling their value. In short, government surveillance and regulation of cryptocurrency is virtually nonexistent (no pun intended) and so long as cryptocurrency payment schemes exist, ransomware attacks and iterations will likely continue to thrive.

Though too early to tell, there may emerge some form of Bitcoin regulation via Executive Order No. 13,694 (April 2015), which expands sanctions to include "blocking" the property of persons

engaging in "Significant Malicious Cyber-Enabled Activities." The order declares a "national emergency" to deal with cyber-enabled threats and extends to the assets of those who "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any [malicious cyber-enabled activities]."

Given that ransomware Bitcoin payments are made to cybercriminals, per Executive Order 13,694, the U.S. Secretary of the Treasury, the U.S. attorney general and/or the U.S. secretary of state could freeze or "block" assets of any participant in the Bitcoin financial chain. Such dramatic government intervention could discourage the purveyors of ransomware attacks, who depend on Bitcoin for receiving payments.

The government could also take additional steps to combat ransomware such as:

- Providing financial incentives for private investment in ransomware prevention and remediation technologies;
- Speaking more boldly discouraging ransomware payments that monetize crime, perhaps via the Financial Crimes Enforcement Network or via a task force of state and federal law enforcement agencies; or
- Creating new legal penalties for ransomware payments in a manner similar to the FCPA, punishing the payer (rather than the perpetrator), imparting additional risk to ransomware payers, and increasing the cost of engaging in the payment transaction.

But these government measures are theoretical and even if implemented, might still not sojourn the dramatic growth of ransomware. The reality is that when it comes to ransomware attacks, the government seems idle and relatively powerless, which means ransomware victims are unfortunately on their own. So what should companies do to manage the increasing risk of the current ransomware crime wave?

As would probably be preached by Thomas Clayton (and perhaps also Russell Crowe), companies struggling with ransomware threats should apply the same lessons to ransomware protection that Clayton uses for employee protection:

- Be prepared (e.g., deploy backups, consistent software patching, firewalls, intrusion detection monitoring, password changing protocols, employee education and the like);
- Be thoughtful (e.g., use professionals to implement preemptive measures and help handle the response); and
- Be vigilant (e.g., never underestimate the impact of ransomware and never take the threat lightly).

John Reed Stark is president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. He previously 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, and for five years as managing director of a global data breach response firm. He is the author of "The Cybersecurity Due Diligence Handbook."