Your World First

C/M/S/
Law.Tax

Cybercrime and ransom demands: is it a crime to pay?

2017

Cybercrime and ransom demands: is it a crime to pay?

In 2015, the Office of National Statistics (**ONS**) for the first time included cybercrime in the annual Crime Survey for England and Wales. It estimated that there were 2.46 million cyber incidents and 2.11 million victims of cybercrime in the UK in 2015.

In July 2016, the National Crime Agency (**NCA**) published its Cyber Crime Assessment, which called for stronger law enforcement and business partnership to fight cybercrime. It estimated that the cost of cybercrime to the UK economy is billions of pounds per annum.

Current trends

There has been an increased trend for cyber criminals to focus their efforts on corporate entities because the potential rewards are far greater. Threats such as Distribution Denial of Service (DDoS) and ransomware attacks have amplified in frequency in recent years as criminals gain a better understanding of the potential for profit. Cyber criminals have become the pirates of the modern age, holding businesses to ransom to release their data and systems from the attack and to recover their all-important customer data.

From Banks to telecommunication providers to media businesses and online retailers, all have been targeted as cyber criminals look to increase their revenue streams. In response, corporate entities have sought to improve their cyber controls to protect themselves from attacks. Perhaps the greatest vulnerability for a business lies in targeted malware sent to staff. Staff are reminded of the need to keep a vigilant watch on anything that may appear suspicious when accessing emails and to report any unusual messages to compliance and their IT teams.

When a ransomware or DDoS attack takes place, corporates will be immediately fearful of losing confidential business information, and client details. Coupled with the EU's new General Data Protection Regulation, which is due to come into force in 2018, corporate concern has been magnified as the EU looks to fine companies up to €20m or 4% of their annual turnover, whichever is greater, for allowing any security breaches to compromise customer data. Companies may not only be a victim of an attack, with all the business disruption, reputational harm and financial loss that may cause, but may then also be fined for failing to prevent the attack on their business.

With the above in mind, when a corporate is the subject of cyber-attack, what offences, if any, are committed by cyber criminals, and even by victims when ransom demands are made?

Cyber criminals

Blackmail

The process of demanding money following a cyber-attack is likely to be done through threats; if a payment demand is not met by a set time, files could be erased, details of accounts released or third parties' financial information disclosed online. Such a demand will be caught by the blackmail provisions under section 21 of the Theft Act 1968.

Money laundering

On the receipt of a ransom, the Proceeds of Crime Act 2002 (**POCA**) will apply to the sums held, which will be deemed criminal property; that is, property which is secured through criminal conduct. Cyber criminals, if their identity can be established, could be caught by one or more of the primary money laundering offences under sections 327 – 329 of POCA, i.e. concealing, acquiring, arranging, transferring, using or holding criminal property.

Victims

Prior to the 19th Century, The Ransom Act of 1782, which outlawed the payment of a ransom in respect of British ships taken by the King's enemies or persons committing hostilities against the King's subjects, was the only guiding piece of legislation on the legality of ransom payments. Since its repeal by section 1 of the Naval Prize Acts Repeal Act 1864, legislators in the UK and further afield ventured no further into this territory. Indeed *The Benga Melati Dua* case in 2011 *(Masefield A.G. v. Amlin Corporate Member Limited* [2011] EWCA Civ 24), highlighted the issue. In his judgment, Lord Justice Rix commented, *'there is no evidence of [ransom] payments being illegal anywhere in the world. This is despite the realisation that the payment of ransom, whatever it might achieve … itself encourages … the purposes of exacting more ransoms'.*

Counter terrorism

The Terrorism Act 2000 (**TA**), and to some extent the Counter-Terrorism and Security Act 2015 (**CTSA**), could put a ransom payer at risk of committing a criminal offence in certain circumstances, but they still fall short of placing any blanket rule on ransom payments, in the context of cyber-attacks.

Under section 17 TA, becoming concerned in an arrangement as a result of which money or other property is or is to be made available to another for the purposes of terrorism, is an offence. However, it must be established that a person knew or had reasonable cause to suspect that the funds would or may be used

for the purposes of terrorism. So in the case of a DDoS or ransomware attack, unless the ransom-payer is aware or has reasonable cause to suspect that the ransom is to be paid to a designated terrorist organisation or to a group concerned with terrorism, it is highly unlikely that an offence will have been committed. Cyber-attacks tend to be perpetrated by faceless individuals and entities, without affiliation to a cause, political or otherwise. Therefore, it will be difficult, if not impossible, to identify those behind the attack.

Separately, under section 42 of the CTSA it is an offence for insurance companies to make a payment pursuant to an insurance contract in respect of any money or other property that has been, or is to be, handed over in response to a demand made wholly or partly for the purposes of terrorism. For the reasons set out above, unless the insurer (or a person authorising the payment on the insurer's behalf) knows or suspects that the money or other property has been, or is to be, handed over in response to a terrorist demand, the offence will not be made out.

Sanctions

Similarly to terrorist organisations, making payments, whether directly or indirectly, to 'designated' individuals or entities listed in the consolidated list of financial sanctions targets prepared by the Office of Financial Sanctions Implementation (**OFSI**), is a criminal offence. If a ransom is paid following a cyber-attack, sanctions will only ever be breached if the identity of the cybercriminal can be established, and then only if that individual or group is on the OFSI's list.

As noted above, it will be rare for those involved in making cyber ransom demands to make themselves known to the victim. Anonymity is crucial if the perpetrator is to evade justice.

Money laundering

While ransoms received by cyber criminals may constitute the proceeds of crime under POCA, they only become criminal proceeds once they have been received as a ransom by the criminal. Assuming there was nothing about the funds used to pay the ransom that tainted them as criminal proceeds prior to the ransom payment, the payment itself would not be a money laundering offence. There had been some uncertainty on this point until *R. v. GH* [2015] UKSC 24, which clarified that where otherwise clean money was paid to someone pursuant to a criminal offence, such that it became criminal proceeds in the hands of the receiver, the payment did not make the payer liable under section 328 of POCA for entering into, becoming concerned in, an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. The rationale of the court was that the funds had to be criminal proceeds before the payment was made for the offence to be triggered.

Conspiracy

Another potential question is whether a payer can be held to have entered into a conspiracy with the person(s) making the demand when ransom monies are transferred. This argument is unlikely to succeed and, even if it could, it is unlikely to be in the public interest (a key consideration to be satisfied before any prosecution can be brought) to prosecute.

This is because a conspiracy is an *agreement* with another that a course of conduct is to be pursued with a view to committing an offence. Payments of ransoms are not *agreements*, but instead are forced arrangements made following the unwarranted approach by the ransom demander.

Conclusion

Whilst there is legislation that can be used to tackle instances where demands are made by cyber criminals, there are limited circumstances when a victim could be held criminally liable for complying with the ransom demand.

Legislation may be breached on the making of a ransom payment, however, much will depend not only on establishing the identity of those making or benefiting from the demand but also, in the case of terrorism issues for example, whether that person's beliefs/ideals were known to, or suspected by, the victim when the ransom was paid. Victims are rarely, if ever, held accountable for the actions of criminals, unless connivance can be established. Backed into a corner where their livelihoods or everything that has been tirelessly worked for could disappear in an instant, public policy will seldom pursue those that have been wronged.

For further information, please contact the below authors or your usual CMS contacts.

Omar Qureshi
Partner, Financial Crime
T +44 20 7367 2573
E omar.qureshi@cms-cmck.com

Tom Scourfield
Partner, Cybersecurity
T +44 20 7367 2707
E tom.scourfield@cms-cmck.com

Stephen Tester
Partner, Insurance
T +44 20 7367 2894
E stephen.tester@cms-cmck.com

Iskander Fernandez
Associate, Financial Crime
T +44 20 7367 3960
E iskander.fernandez@cms-cmck.com

CMS Cameron McKenna LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1612-0131-2