NORDIC NEWSLETTER

TOPICS COVERED

Welcome to Jenner & Block's Nordic Newsletter

Dear friends and colleagues,

We are delighted to share with you the Fall 2017 edition of the **Jenner & Block Nordic Newsletter**. We hope you enjoyed the summer, even if the weather didn't always cooperate with your vacation plans. The only safe thing to say is that it probably won't get any better in the next few months… Now that everybody is back, it appears that the US-Nordics cross-border deal activity is continuing to be robust and is keeping many of us, in house and external service providers, busy. Hand in hand with the continued deal activity, we continue to see a rise in focus on compliance and regulatory matters that impact Nordic-based multinationals that have operations in the United States and the United Kingdom. We expect that focus to continue and increase over time. To that end, we have included in this issue the following articles:

- An article that focuses on the increased use of Cyber and Kidnap/Ransom Insurance in light of the increased threat of cyber-attacks and ransomware;
- A link to our most recent "Business Guide to Anti-Corruption Laws," which includes updates and analyses regarding significant FCPA and anticorruption developments that will shape enforcement and compliance efforts in 2017 and 2018;
- An article focusing on recent trends in the US Department of Justice's approach to multinational investigations; and
- An article describing the growing danger to attorney-client privilege in investigations.

We hope you find the newsletter informative. We welcome any comments you may have and are open to suggestions regarding future content that is of interest to you. And if you no longer wish to receive this newsletter, feel free to unsubscribe.

Sincerely,

Uri Doron
Head of the Nordic Practice, Jenner & Block LLP
udoron@jenner.com +1 (212) 891-1677 Download V-Card

Cyber and Kidnap/Ransom Insurance Should Respond to Massive "WannaCry" and Similar Global Ransomware Attacks in More than 100 Countries

As companies become more and more prone to the threat of cyber-attacks and ransomware, they are more frequently turning to the protection afforded by some traditional insurance policies such as general liability and kidnap/ransom insurance, as well as specific cyber insurance coverage. Ransomware has been identified as the number one cyber-security risk facing computer and data storage systems by numerous international agencies, insurers and law enforcement groups. Ransomware locks down a user's access to computer systems, data and other information, and threatens to continue this lock down, until it is removed or neutralized through the use of a decryption key. The hacker then demands the payment of a ransom, in bitcoin – which is typically untraceable – in exchange for the decryption key or other means of removing the malware.

In June 2017, Maersk was the victim of a "NotPetya" ransomware attack that encrypted its computer systems around the world, affecting its container shipping, port, tug boat, oil and gas production, drilling services and oil tanker operations. The attack also debilitated the systems at no less than 17 of Maersk's shipping container terminals. The hackers behind the attack demanded a payment of $300 in bitcoin per user. The attack significantly impacted Maersk's operations and the company estimates that the attack will cost the company up to $300 million in lost revenue.

Similarly, a highly sophisticated type of ransomware, or malware, infected thousands of systems in more than 100 countries in May 2017. This attack was caused by something known as "WannaCry" or "WanaCyrpt0r 2.0" and is reported to exploit a security flaw in Microsoft software found by the National Security Agency for its surveillance toolkit. Although Microsoft, once warned by the NSA of the flaw, took steps to warn users of the problem, many systems remained open to attack, either because system administrators failed to apply the recommended patch or because they used outdated software. Here, the initial ransom demanded was only $300 or slightly more.

Ransomware remains the top cyber-security threat to education, transportation, financial and healthcare companies. For example, in October 2016, Beazley, a large cyber insurance underwriter, reported that there had been 1437 data breaches suffered by Beazley policyholders during the first nine months of 2016 whereas there had been only 931 such data breaches for the same time period in 2015. Also, according to Beazley, during the first nine months of 2016, a hack or malware accounted for the highest percentage of cyber incidents in the higher education (46%), financial services (39%) and healthcare (19%) industry sectors. The FBI estimated that ransomware payments in 2016 totaled more than $1 billion (compared with only $24 million in 2015). More than 72% of Australian businesses were hit by ransomware attacks in 2015.

In addition to the Maersk and WannaCry malware incidents, there have been numerous high-profile ransomware attacks in the United States recently, including the Los Angeles Valley College District ($28,000 in bitcoin demanded) and the Hollywood Presbyterian Medical Center ($17,000 in bitcoin demanded). In each case, the ransom demanded (which has been, on average, less than $1,000) was well below the applicable self-insured retentions (SIR), or deductibles, in the relevant cyber policies.

Most current versions of cyber insurance policies provide some form of "extortion" coverage, which is what a ransomware attack initially generates: an extortionate request for the payment of money. A typical cyber insurance policy might include the following coverage provision and definitions:

Cyber-Extortion

The Insurer will reimburse the Insured Company for cyber-extortion expenses that the Insured Company incurs resulting from a cyber-extortion threat.

Cyber-Extortion Threat

A threat or connected series of threats to commit an intentional attack against a network first made during the policy period to:

1. Disrupt the Insured's business operations;
2. Alter, damage or destroy data stored on the network;
3. Use the network to generate and transmit malware to third parties;
4. Deface the Insured's website; or
5. Access, distribute, remove, alter, damage or otherwise misuse personally identifiable information, protected health information or confidential business information stored on the network,

made by a person or group, whether acting alone or in collusion with others, demanding payment or a series of payments in consideration for the elimination, mitigation or removal of the threat.

Cyber-Security Breach

Any unauthorized access to, use or misuse of, modification to the network and/or denial of network resources by attacks perpetuated through malware, viruses, worms and Trojan horses, spyware and adware, zero-day attacks, hacker attacks and denial of service attacks.

The above-listed provisions, definitions and conditions raise numerous considerations for a policyholder. Initially, before a ransom payment can even qualify for coverage under the above definition, the policyholder must inform the insurer of the ransom demand and must obtain the insurer's consent (which cannot be "unreasonably withheld") before paying the ransom. What if the insured does not want to pay the ransom, and is, in fact, being encouraged by local law enforcement authorities not to pay the ransom? If further damage results from not paying the ransom, will a cyber insurer refuse to pay for that damage and business interruption? Do insurers want to encourage policyholders to ignore the direction of law enforcement authorities? After some initial ransomware attacks, law enforcement authorities recommended against the payment of ransom, as such payments might only encourage more attacks and might not stop the hackers from launching new attacks. More recently, however, some law enforcement agencies have taken a neutral position and have informed victims that they should, or should not, pay the ransom based on their own analysis and how their business operations would be impacted by either scenario.

Finally, when does a "cyber-extortion threat" become a "cyber-security breach"? A cyber-security breach in most cyber policies triggers both Business Interruption and Extra Expense, and Data Recovery, first party coverage parts. This question raises a separate host of considerations.

Policyholders will carefully want to consider whether or not to report such attacks, even if the ransom paid (or demanded) is far less than the applicable self-insured retention or deductible, as the failure to do so could result in adverse consequences in the future. One should note that because the self-insured retention or deductible in most kidnap and ransom policies is often much lower than that in a cyber policy, the notice analysis could be far simpler and coverage might be available much sooner.

Notice to the current insurer could be critical, and disclosure of a ransomware attack is also an important consideration, when applying for a new cyber insurance policy or renewing an existing policy. Policyholders, therefore, need to be vigilant and well-informed when addressing issues of notice of a current attack or disclosure in the context of a cyber insurance (or other) application. Moreover, the legal standards governing the scope of a policyholder's notice and disclosure obligations at the time of a cyber-attack or cyber insurance policy application can vary widely depending upon applicable law.

All of these issues demonstrate that a policyholder must carefully consider all the complex issues surrounding post-cyber-attack actions and that the guidance of experienced insurance counsel, as well as insurance brokers, may be necessary to preserve insurance coverage in the face of such events.

Matthew L. Jacobs, Partner • mjacobs@jenner.com

BACK TO TOP

Foreign Corrupt Practices Act (FCPA)

We are pleased to present the 2017 Mid-Year edition of Jenner & Block's Foreign Corrupt Practices Act (FCPA) Business Guide. This Guide – published in January and mid-year – provides the most current practical guidance on how best to confront the reality of corruption in the world's marketplaces, both before and after the government is involved.

Click here for an electronic version of the 2017 Mid-Year Foreign Corrupt Practices Act (FCPA) Business Guide.

Click here to order your complimentary copy of the publication.

BACK TO TOP

DOJ Signals More Fairness in Multinational Investigations

Recognizing the increasing number of multinational criminal and regulatory investigations, the United States Department of Justice (DOJ) has recently and repeatedly indicated a desire to resolve cases in ways that will prevent companies from being unfairly penalized by multiple countries. This is an encouraging development that companies will welcome as signaling greater fairness and transparency.

In a May 24, 2017 speech delivered at an anti-corruption conference in Brazil, a high-ranking DOJ official discussed increasing US cooperation with foreign governments on two initiatives: (1) the acquisition of evidence and (2) the global resolution of criminal cases. During the speech, DOJ Acting Principal Deputy Assistant Attorney General Trevor McFadden called both initiatives part of "developing" and "emerging" trends in white collar crime prosecutions.

On the first point, McFadden said that the DOJ's investigations "almost always have an international nexus, often involving several different countries." As a result, McFadden stated, the DOJ has an "ever- increasing utilization" of evidence exchange with other countries. Over the last five years, according to McFadden, the number of requests for assistance in evidence gathering by foreign governments has increased by nearly 150%, while the DOJ's requests to foreign governments for assistance has increased by 75%.

Notably, McFadden indicated that the requests for assistance themselves sometimes cause multiple countries to be interested in investigating the same conduct. McFadden said there "has been an increase in multi-jurisdictional prosecutions of criminal conduct," which he said was "due in part to the significant assistance" the DOJ provides to other countries.

This is at least the second time in recent months that the DOJ has publicly linked the increase in international cooperation in the gathering of evidence to the opening of multi-jurisdictional investigations. In a March 2017 speech at the American Bar Association National Institute on White Collar Crime in Miami, Acting Assistant Attorney General Kenneth Blanco stated that these evidence-gathering efforts have caused "an increase in multi-jurisdictional prosecutions of criminal conduct." Using the same language as McFadden, Blanco called the increase in multinational investigations and prosecutions "an emerging trend." Because foreign requests for assistance can trigger additional scrutiny by other countries, companies and their attorneys should consider whether any strategy in the early stages of an investigation would make it less likely for authorities to seek assistance from foreign authorities in gathering evidence. If such a strategy is successful, it could significantly limit companies' exposure and costs.

Other recent news may cause further increases in the number of multi-jurisdictional investigations. Specifically, in his May speech, McFadden announced that in the coming months the DOJ will detail a white collar prosecutor to work in the United Kingdom for the Financial Conduct Authority, which is a financial regulatory body that is somewhat similar to the US Securities and Exchange Commission. This will be the first time that the DOJ will

send one of its prosecutors to work for another county's foreign regulatory agency on white collar issues. McFadden called this decision "part of our ongoing efforts to collaborate with our international partners in the fight against corruption and financial fraud." Indeed, if embedding a prosecutor in the UK's Financial Conduct Authority is successful, a logical next step will be for the DOJ to look to do so elsewhere as well.

Additionally, in June 2017, 20 European Union member states agreed to form the European Public Prosecutor's Office. The entity will begin to investigate crimes allegedly occurring across those member states in October 2017. Once established, there will certainly be multi-jurisdictional investigations and prosecutions that overlap between the European Public Prosecutor's Office and the DOJ.

The good news for companies that find themselves to be subjects of these increasing multinational investigations is that the DOJ now recognizes a need for global resolutions. Not only can global resolutions help avoid penalties that amount to double-counting of fines, but they also may provide needed closure as a whole for companies that are the subjects of the investigation. In their speeches, McFadden and Blanco, using the exact same words, stated that the goal of these global resolutions is to ensure that companies "are not unfairly penalized for the same conduct by multiple" countries and agencies. The fact that the two DOJ officials used the same language indicates that the DOJ is motivated to find ways of globally resolving multi-jurisdictional investigations and is attempting to persuade other nations to enter into these resolutions as well.

The DOJ's statements about global resolutions are encouraging. In the past, the DOJ has been receptive to these arguments, but results have been mixed and the calculations are not always transparent. The comments by DOJ leadership at least reflect a sensitivity to the issue of unfair penalties at the highest levels, and can now be used in negotiations. Indeed, a recent global resolution is consistent with the DOJ's comments. In a Foreign Corrupt Practices Act investigation that was resolved in January 2017, Rolls-Royce plc agreed to be fined $195 million in the United States as part of an $800 million global settlement that included the United Kingdom and Brazil. In the press release announcing news of the resolution, the DOJ explained that Rolls-Royce would not be obligated to pay all $195 million, but instead would credit the company with $25 million that Rolls-Royce had agreed to pay Brazil in an overlapping facet of the investigations. This resolution provides a road map for how to negotiate global settlements so companies do not pay twice for the same conduct. It appears the DOJ will be satisfied if it can include all of the fines to be paid for overlapping conduct in its global resolutions, yet credit companies with the amounts they have paid or will pay to foreign governments for that conduct.

This article was also published in *Law360*.

Brandon D. Fox, Partner • bfox@jenner.com

BACK TO TOP

The Growing Danger to Privilege in Investigations

More than three decades ago in *Upjohn Co. v. United States*, the US Supreme Court held that memoranda and notes of interviews that lawyers conduct of a corporate client's employees are generally protected from disclosure by both the attorney-client privilege and the attorney work-product doctrine.

In two recent cases, the English High Court of Justice ruled the opposite way under English law, holding that notes and Interview memoranda created in internal investigations enjoyed no privilege protection at all. Instead, both English judgments ordered the lawyers' notes and interview memoranda to be turned over – in one instance to prosecutors and in another to private litigants. See *Serious Fraud Office v Eurasian Natural Resources Corporation Ltd* ("ENRC")*; The RBS Rights Issue litigation* ("RBS").

The facts of one of the cases show just how far English courts might take the doctrine. The RBS case was civil litigation stemming from the financial crisis of 2008. In 2017, nearly a decade later, the English court ordered the disclosure of lawyers' notes and memoranda that had been created during an internal investigation years earlier. These materials included memoranda written by US lawyers summarizing interviews conducted by US lawyers that took place within the United States to counsel the client how best to defend an investigation by the US Securities and Exchange Commission.

In light of these two decisions, UK prosecutors and private plaintiffs alike may now see it as open season on documents long viewed as protected by US privilege law – at least pending review by the UK Supreme Court. In the meantime, ENRC has sought leave to appeal from the lower court's decision, potentially affording the UK Supreme Court a chance to blaze a different trail than the one the President of the Law Society of England and Wales has called "deeply alarming."

The US position

US lawyers conducting internal investigations have known since *Upjohn* that their notes and memoranda of interviews of employees of corporate clients are typically privileged under US federal law. The Supreme Court held that the attorney-client privilege protects not only the giving of advice, but also the "giving of information to the lawyer to enable [the lawyer] to give sound and informed advice." The Court further held that frequently "[mid]-level – and indeed lower-level – employees can...have the relevant information needed by corporate counsel ...to advise the client," and therefore communications with those employees should also be protected by the corporation's attorney-client privilege.

Moreover, even to the extent that the lawyers' memoranda and notes do not reveal attorney-client communications, they are nonetheless protected by the federal work-product doctrine. The US Supreme Court deemed them "work product based on oral statements," noting that they "reveal the attorneys' mental processes in evaluating the communications" even when they do not reveal actual communications. The Court found that "forcing an attorney to disclose notes and memoranda of witnesses' oral statements is particularly disfavored because it tends to reveal the attorney's mental processes."

The English position

In RBS and ENRC, the English High Court found no protection for lawyers' interview notes or memoranda under any of the (1) legal advice privilege, (2) lawyers' working papers privilege and (3) litigation privilege.

Nor, in the end, did it deter the High Court in the RBS case that it was compelling disclosure of communications created in the United States by US lawyers and that are privileged under US law. England has carefully struck the privilege balance in its courts as a matter of public policy, said the Court, and that overrides even legitimate expectations under US law.

Legal advice privilege

In English law, the nearest equivalent to the attorney-client privilege is "legal advice privilege," which protects confidential communications passing between a client and its lawyers, acting in their professional capacity in connection with the provision of legal advice. Legal advice privilege, though, does not apply to information provided by a client's employees to the client's lawyers, said the High Court. Communications with mere employees are "not privileged communications," and instead legal advice privilege protects communications only with the small group of employees "authorised to seek and receive legal advice from the lawyer."

As a practical matter, internal investigations involve interviewing corporate employees. Indeed, typically the very problem is that management does not know the facts, and consequently the lawyer is instructed to unearth the facts as an essential part of rendering legal advice. It is difficult, indeed, to do that without interviewing employees. Currently (and if the High Court's rulings stand upon any appeal to the UK Supreme Court) these interviews will be unprotected by English legal advice privilege. And as the RBS case shows, this doctrine can uncloak interviews by US lawyers, even if the interviews took place outside England.

Lawyers' working papers privilege

In RBS and ENRC, the High Court also examined – and rejected – the applicability of the lawyers' working papers privilege, a subset of the legal advice privilege doctrine. Lawyers' working papers privilege protects certain papers created during the course of the provision of legal advice to the client. In those cases, the High Court wrote that lawyers' internal memoranda are privileged only when they give a "clue" as to the "trend" of legal "advice" (*RBS*) and "[t]he protection afforded to lawyers' working papers is justified if, and only if, they would betray the tenor of the legal advice." (*ENRC*) The High Court described a lawyer's decisions about what facts to try to uncover and what facts to memorialize as being "not sufficient...to substantiate the claim to privilege" because as a matter of English law "there is a real difference between reflecting a 'train of inquiry' – which is what the selection of material would divulge – "and reflecting or giving a clue to the trend of legal advice."

This, too, contrasts sharply with *Upjohn*, and shows a vastly different approach between the US and UK systems about the centrality of facts in providing legal advice. To the US Supreme Court, "the first step in the resolution of any legal problem is ascertaining the factual background and sifting through the facts with an eye to the legally relevant."

Litigation privilege

The final potentially relevant English doctrine that the High Court examined was Litigation Privilege, akin to the US attorney work-product doctrine. In *ENRC*, the Court wrote that "the purpose of the [Litigation Privilege] doctrine is to enable someone to prepare for the conduct of reasonably anticipated litigation," but it held that lawyers' interview notes and memoranda were not protected under this doctrine either.

In ENRC the Court focused on three aspects of Litigation Privilege: (1) That "adversarial litigation" must be (2) "reasonably in contemplation," and that the documents at issue (3) must be made with the "dominant purpose" of conducting that litigation.

The overriding reality for ENRC was that much of its internal investigation was conducted under a well founded fear of imminent criminal investigation. As ENRC's Head of Compliance wrote in a graphic email: "I predict a sh!tstorm and a SFO [Serious Fraud Office] dawn raid in London before summer's over." Indeed, ENRC received a letter from the SFO which the Court said left "no doubt" that the prospect of a criminal investigation was "tacitly being used as a strong incentive" to persuade ENRC to cooperate. Throughout, there were newspaper articles, apparent attempts at cooperation, and then, finally, a breakdown between the ENRC and the SFO that led to the SFO opening its own criminal investigation and compelling the production of the interview memoranda. But, the High Court held that this concrete fear of investigation – or even of a government raid – does not count as fear of "adversarial litigation" on the simple ground that "an investigation is not adversarial litigation." Thus the Court held that ENRCs claim to litigation privilege failed on the first ground.

It also failed on the second ground – the "reasonable contemplation" requirement. Indeed, here the Court created a doctrinal Catch-22. The Court held that a company is unlikely to be in "reasonable contemplation" of litigation at the outset of most internal investigations because it will not yet know the very facts that the investigation is designed to uncover. That is, if you are at a stage where you need to investigate, then you cannot yet "reasonably" anticipate litigation because you are still ignorant of unpleasant truths. Instead, "prosecution only becomes a real prospect once it is discovered that there is some truth in the accusations." The High Court enunciated the rule, as follows:

> Criminal proceedings cannot be reasonably contemplated unless the prospective defendant knows enough about what the investigation is likely to unearth, or has unearthed, to appreciate that it is realistic to expect a prosecutor to be satisfied that it has enough material to stand a good chance of securing a conviction.

Finally, the Court also ruled against ENRC on the third ground – the so-called "dominant purpose" test. Specifically, the High Court held that a "purpose" of developing facts to avoid prosecution differs from developing facts for use in defending oneself during a prosecution, and that a purpose of avoiding prosecution is insufficient to warrant privilege protection. Indeed, it is apparently even the Court's view that one might also fail the "dominant purpose" test if the client contemplates sharing facts from the internal investigation to make a presentation to the prosecutor designed to stave off charges; the Court deemed that flavor of advocacy "collaborative rather than adversarial." Nor, apparently, does one meet the Court's test if the purpose of the investigation is merely "to meet compliance requirements," – notwithstanding that having an effective compliance program is a ground in the United States to persuade prosecutors to forgo charges under the US Department of Justice's Attorneys' Manual.

Evidential bases

One aspect of the ENRC and RBS cases that is being debated in the London defense community is the extent to which the decisions are fact bound. Both cases discuss at some length various failures of the party seeking privilege in coming forward with evidence that demonstrated the privileged nature of the documents.

Consequently, even under the doctrines as the High Court has enunciated them, there is at least some possibility

of a different result if: (a) fuller or different evidence is adduced when resisting disclosure of lawyers' notes, (b) a full contemporaneous record about the purpose of the interviews is made, or (c) lawyers adopt practices in taking notes and writing memoranda that place them within the privilege protections as described by the Court, such as, for example, writing them so they more clearly reflect the trend of legal advice given to the client. This is unlikely to be a cure all, however. Depending on the specific case, lawyers might find making that different kind of record impossible, impracticable, or imprudent.

Conclusion

The English High Court has twice ruled recently that a lawyer's notes of interviews of a client's employees have no privilege protection. It has ruled that, in English proceedings, the public policy underpinning English privilege law trumps US privilege law, and it has ordered that memoranda written by US lawyers of interviews in the US be produced in English courts and to English prosecutors.

We have not seen the final word. The High Court itself has recognized that the doctrine adopted by the English courts has been heavily criticized by academics and other jurisdictions. There will be more debate, and in the words of the High Court itself, "if there is to be any change of approach to bring the law in this jurisdiction into line with the more liberal approach adopted in other jurisdictions, it will have to be made by the Supreme Court or by Parliament."

This article was also published in New York University School of Law's *Compliance and Enforcement Blog*.

Peter B. Pope, Partner • ppope@jenner.com
Kelly Hagedorn, Partner • khagedorn@jenner.com
Kathleen W. Gibbons, Associate • kgibbons@jenner.com
Tracey Lattimer, Associate • tlattimer@jenner.com

BACK TO TOP