Cyberinsurance Coverage for Ransomware Payments vs US Sanctions Regulations

JACQUES DE WERRA, CÉLIAN HIRSCH

THOMAS HUA (as Guest contributor)

An insurance company did not have the right to refuse to pay its insured client, a victim of a cyberattack who had made a ransomware payment, even if it claimed that its obligation to reimburse the ransomware payment would expose it to US sanctions.

Judgment of the Federal Supreme Court of 17 August 2023

Case reference: 4A_206/2023

Facts

In July 2020, the IT systems of a group with its holding company in Switzerland ("the Company") were partially paralyzed by a ransomware attack which froze operations in call centres, websites and other online services for five days ("The Ransomware Attack"). It was publicly disclosed that the victim of the Ransomware Attack was the company Garmin.[1] The Company paid a ransom of 1,500 bitcoins (valued at approximately USD 13.5 million at the time) through an independent third-party company. Its files were consequently decrypted by the author of the Ransomware Attack. The Company reported damages of approximately USD 15 million as a result of the Ransomware Attack.

The Company had an insurance policy that had been entered into with a group of insurance companies under a syndicated insurance policy which covered cyber-risks ("the Insurance Policy").

Turning to its cyber-risk insurers, the Company sought to obtain the reimbursement of the damages that it had suffered as a result of the Ransomware Attack including the ransom payment under the Insurance Policy which provided for standard joint but not several liability of the insurance companies that were bound by the Insurance Policy (Swiss law was applicable to the Insurance Policy).

All the insurance companies bound by the Insurance Policy paid a fraction of the amounts of damages claimed by the Company under the Insurance Policy except for one ("the Insurance"). The Insurance, a UK-based entity indirectly controlled by a US company, refused to pay the Company by invoking a clause contained in the Insurance Policy that excluded insurance coverage in cases where the payment by the Insurance would expose it to "any sanction, prohibition or restriction" under "the trade or economic sanctions, laws or regulations" of the US (and other countries). The clause of the Insurance Policy had the following wording ("the Sanctions Clause"):

"SANCTION LIMITATION AND EXCLUSION CLAUSE

No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would *expose that (re)insurer to any sanction, prohibition or restriction* under United Nations resolutions or the *trade or economic sanctions, laws or regulations* of the European Union, United Kingdom or *United States of America*" (italics added).

In this respect, the Insurance claimed that the payment to the Company would expose it to US sanctions regulations because the Ransomware Attack was allegedly associated with a cybercrime organization ("Evil Corp") that was under US sanctions given that it was on the "*Specially Designated Nationals and Blocked Persons" (SDN)* list since 2019. A payment by the Insurance to the Company under the Insurance Policy would consequently expose the Insurance to US sanctions which would consequently trigger the application of the Sanctions Clause of the Insurance Policy so the Insurance had the right to refuse to pay the Company the ransomware payment.

The Insurance claimed more specifically that the Ransomware Attack was carried out by a group called Evil Corp, a Russia-based organization that was placed under US Sanctions in 2019 by the United States Office of Foreign Assets Control (OFAC) for their large-scale cybercrime activities.[2] The Insurance claimed that the Ransomware Attack was executed using Wasted-Locker, a malware similar to Dridex, which is associated to Evil Corp, therefore creating a sufficient link between Evil Corp and the Ransomware Attack.

The Company claimed the payment of USD 987,098 plus interests (which corresponded to approximately 10% of the damages suffered by the Company as a result of the Ransomware Attack) from the Insurance before the Commercial Court of the Canton of Zurich.[3] The Insurance filed an appeal against this judgment before the Federal Supreme Court.

Issue

The issue was whether the Insurance was contractually entitled to refuse to pay the Company the claimed amount of USD 987,098 plus interest by relying on the Sanctions Clause. This required interpreting the Sanctions Clause to determine whether or not the Insurance would be exposed to US sanctions if it paid the amount due to the Company.

Legal reasoning

As part of the general terms and conditions of insurance resulting from the Insurance Policy, the Sanctions Clause had to be interpreted like any other contractual provision (142 III 671). Based on the general rules of contractual interpretation under Swiss contract law, (subjective interpretation) and, only in the absence of such intent, can it interpret the contract as it could be understood by a third party in the same context (objective interpretation) (art. 18 para. 1 SCO)[4].

The specificity in this case was the contractual reference made in the Sanction Clause to penalties under foreign laws, namely sanctions regulations of the United States of America. From a procedural standpoint, foreign law is considered a legal matter: Swiss courts must establish the contents of foreign laws with the assistance of the parties if necessary (art. 16 para. 1 PILA). The Company and the Insurance (together "the Parties") contributed significantly to establish the content of foreign law (in this case US law) by submitting a total of seven legal opinions on US sanctions regulations.

The Sanctions Clause provided that the Insurance could refuse to pay the Company if a payment "would expose" the Insurance "to any sanction, prohibition or restriction" under US law.

The Parties agreed that the Sanctions Clause would apply if the Insurance faced a "significant risk" of being sanctioned under US law, no concurring intent (subjective interpretation) of the Parties could be established as to what constituted a significant risk, thereby calling for an interpretation under the principle of trust (objective interpretation).

Based on a literal interpretation of the Sanctions Clause, the cantonal court ruled, on the one hand, that the mere risk of enforcement proceedings against the Insurance was insufficient and, on the other hand, that the sanction to which the Insurance would be exposed must not be final nor confirmed by US courts. Hence, in the cantonal court's view, the meaning of the expression "expose to sanctions" in the Sanctions Clause meant that there had to be a significant risk that OFAC would not only initiate enforcement proceedings, but also inflict a sanction on the Insurance (judgment of the cantonal court *Handelsgericht des Kantons Zürich*, HG 210017 of March 9, 2023, paras. 6.3.1-6.3.4).

In order to estimate how exposed the insurer was to a penalty from OFAC, the cantonal court had to first establish the contents of US sanctions regulations before applying them. Regarding the contents of US sanctions regulations, the cantonal court held as follows (HG 210017, paras. 6.3.11-6.3.15):

- Though the insurer is a non-US person, the insured's USD claim against the Insurance (i.e. USD 987,098 plus interest) would cause it to process a payment in USD through the USD clearing and settlement system, both of which exposed the Insurance to penalty under US sanctions regulations (OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments dated 21 September 2021).
- The cantonal court held that OFAC does not, as a general practice, penalize victims of cyber extortion who pay a ransom to a sanctioned party, nor has any penalty ever been imposed on a victim's auxiliary (such as a cyber insurer). The cantonal court presumed that OFAC would exercise the greatest restraint in such matters as inflicting penalties on extorted companies would be tantamount to punishing the victim twice and this would be contrary to US economic interests.
- On the other hand, OFAC's policy states that "[f]acilitating ransomware payments on behalf of a victim may violate OFAC regulations" and that the self-reporting of a ransomware attack to OFAC is a "mitigating factor" (OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments dated 21 September 2021), both of which clearly indicate that a ransom payment can lead to penalty under US sanctions regulations.
- From OFAC's point of view, as long as the interests (as broadly defined by US sanctions regulations) of a sanctioned party are affected, then there is a connecting factor under US sanctions regulations. Insurance payments to policy holders indirectly affect the interests of the sanctioned party, irrespective of whether it is made before or after the ransom payment.

Thus, the cantonal court considered that the Insurance would violate US sanctions regulations if the interests of a sanctioned party were affected by the payment of the claim by the Insurance to the Company (HG 210017, para. 6.4). To establish this, the insurer essentially sought to demonstrate similarities between the ransomware program associated to Evil Corp and the one used in the Ransomware Attack on the Company. The cantonal court found that this was not sufficient to trigger the application of the Sanctions Clause for the following reasons:

- The *lex causae* (i.e. Swiss law as chosen by the Parties) defines the burden of proof ("*Beweislast*") as well as the standard of proof ("*Beweismass*"). According to this, the burden of proof that Evil Corp's interests would be affected by the payment was to be borne by the Insurance. Even though Swiss law defines the standard of proof, the Sanctions Clause referred to US laws so that the standard of proof was to be established under US sanctions regulations. The violation of US sanctions must be established with a "preponderance of reliable, probative and substantial evidence" (preponderance of the evidence) for OFAC to act. It means that a fact must be "more likely than not" true to be considered established (HG 210017, para. 7.2.2).
- Though its forensic method and evidence are not published, OFAC announced sanctions on Evil Corp by mentioning extorted payments above USD 100 million. This suggested that Evil Corp had been identified and sanctioned based on payment flows. In this case, the evidence provided by the Insurance only showed that the ransom payment made for the Ransomware Attack had been transferred to a crypto wallet that was not associated to any entity sanctioned by OFAC at the time of the cantonal judgment.
- Although the authorship of the software that was used for the Ransomware Attack may be relevant for tracking the authors of such attacks, this does not demonstrate, on its own, that Evil Corp benefitted from the Ransomware Attack and constituted an interest for the organization within the meaning of US sanctions regulations. Consequently, this cannot establish a link that the author of the software had an interest in the Ransomware Attack given the widespread use of such software and botnets amongst cybercrime groups (HG 210017, para. 7.3.3).
- Lastly, OFAC had been informed of the Ransomware Attack and had not initiated any enforcement proceedings neither against the insured nor against the intermediary tasked with making the ransomware payment (HG 210017, para. 7.3.4).

The cantonal court thus ruled that it was highly unlikely that the Insurance would be subject to penalties under US sanctions regulations for the ransomware payment. It consequently admitted the Company's claim against the Insurance for the full amount (HG 210017, para. 7.3.5).

In its appeal before the Federal Supreme Court, the Insurance mainly challenged the finding made by the cantonal court that it had not established that Evil Corp, a SDN within the meaning of US sanctions regulations, was involved in the Ransomware Attack. Without delving into detailed considerations, the Federal Supreme Court rejected the appeal for the following reasons:

- Since the matter ultimately revolved around the application of foreign laws concerning a monetary claim, the cantonal court judgment could only be reversed if the appellant had shown an arbitrary application of such rules (96 para. b Federal Supreme Court Act). Arbitrary application implies both that the application of the law is obviously undefendable or contrary to facts, and that the result is untenable (ATF 144 I 113 para. 7.1).
- It was not arbitrary to hold that the mere proof that Evil Corp was at the source of ransomware was not sufficient to mean in and of itself Evil Corp benefitted from the Ransomware Attack within the meaning of US sanctions regulations. It was not arbitrary either to hold that each use of such ransomware by third parties would not necessarily benefit Evil Corp. This was also highlighted in the Insurance's cyber expert report, that pointed out that commodity malware is frequently sold to interested parties for mass distribution. Even assuming that Evil Corp would have profit from each use of its ransomware in the form of license fees (it being noted that the Federal Supreme Court imprecisely referred to the "lease" of the software/"Honorar aus der Vermietung von D.", 7.2.3), it would still not be arbitrary to consider that such fee does not correspond to the level of "interest" within the meaning of US sanctions regulations. In any case, the Insurance's argument is overly broad when it argues that any use of the ransomware (even by third parties) would lead to a prohibited transaction because Evil Corp's interests would always be affected.
- Lastly, the fact that the cantonal court took into account the actual conduct of OFAC as an additional factor when assessing the risk of penalty is not objectionable.

Since the Insurance had failed to demonstrate an arbitrary application of US sanctions regulations, the Federal Supreme Court rejected the appeal of the Insurance and upheld the Company's claim.

Key takeaway

Insurance companies offering cyber-risk/ransomware coverage cannot easily avoid paying their clients (victims of cyberattacks who have paid the ransom) merely by claiming that the cyberattack was carried out by or benefitted a sanctioned entity (under sanctions regulations) unless they can establish and prove that the sanctioned entity was truly behind the cyberattack. In this case, the Insurance failed to establish that an entity sanctioned under US sanctions regulations (Evil Corp) was involved in the Ransomware Attack and was the beneficiary of the ransom payment that was made by the Company. The Insurance consequently failed to demonstrate that it was exposed to the risk of being sanctioned under US sanctions regulations. As a result, the Insurance could not rely on the Sanctions Clause in order to escape from its contractual obligation to pay the Company under the Insurance Policy.

Comments

This case prompts the following comments:

First, it serves as an interesting illustration of the cases (that go beyond cyber-insurances and ransomware) in which a contracting party claims that the performance of its contractual obligation can trigger sanctions under foreign sanctions regulations (in particular US sanctions regulations[5]) to avoid the performance of its obligations.[6] This is, unfortunately, a very frequent issue given the current geopolitical situation in which sanctions can be imposed on companies in many jurisdictions.

Secondly, this case is relevant because it shows the factual challenge that the Insurance had to face to establish the origin of the Ransomware Attack and to try to show a link between the sanctioned entity (under US sanctions regulations) and the Ransomware Attack. In this respect, this case demonstrates the difficulties of attribution of cyberattacks which is a major policy challenge that goes way beyond contractual disputes[7] (concerning contract law, the attribution of cyberattacks can lead to various contractual issues, particularly related to the scope of coverage of cyber-insurance policies beyond the specific issue at hand, in this case about the interpretation of the Sanctions Clause). This can particularly arise in the case of Act of War clauses – excluding insurance coverage – that may apply provided that it can be established that governmental entities were at the source of the cyberattack for which insurance coverage is claimed.[8]

In this respect, this case is interesting in terms of the conditions to establish the attribution of a cyberattack because it discusses whether the use of a given ransomware in a cyberattack means that the author of such ransomware has taken part in the attack. The issue is whether it can consider that any cyberattack that would have been committed using said ransomware could solely be attributable to the author of the ransomware.

Thirdly, this case is interesting from a contractual perspective in defining how a contractual clause such as the Sanctions Clause should be drafted to make it possible for a contracting party to refuse the performance of its contractual obligation if that would expose said party to sanctions under foreign law and what evidence shall be brought forward for this purpose.

In this case, the Sanctions Clause provided that the Insurance shall not "be liable to pay any claim or provide any benefit hereunder" to the extent that this "would *expose that (re)insurer to any sanction, prohibition or restriction* under United Nations resolutions or the *trade or economic sanctions, laws or regulations* of the European Union, United Kingdom or *United States of America*" – italics added.

The crux of the dispute was consequently about the contractual meaning of what the terms "would expose" to "any sanction, prohibition or restriction" under US sanctions regulations would mean.

Hinging on the definition of "exposure" to a decision to be made by a foreign authority (in this instance, the OFAC), this issue of substantive law may also touch upon other aspects, i.e. the burden of proof and the standard of proof that shall apply to establish the exposure to foreign sanctions.

Being exposed to sanctions must be understood to mean that the relevant entity *risks* facing sanctions. It does not mean that the relevant entity must have been sanctioned or that it will be sanctioned with certainty. A reasonable interpretation of this concept of exposure to a risk implies that the risk must not be purely theoretical but must rather have a certain degree of probability. Otherwise, the debtor could too easily avoid the performance of its contractual obligation by invoking a remote risk of being sanctioned in a foreign country.

This interpretation of the Insurance Policy and thus of the Sanctions Clause was governed by Swiss law. One may wonder why the cantonal court still applied US law by claiming that the Insurance Policy (i.e. the Sanctions Clause) referred to US

law (para. 7.2.2. "*Insofern ergibt sich letztlich aus dem vertraglichen Verweis auf das U.S.-amerikanische Recht das anzuwendende Beweismass*"). Two legal issues should be distinguished here: the first one is about the meaning of being exposed to a risk and the level of likelihood of this risk exposure which is something that must be defined by application of Swiss contract law (it being noted that it is necessary to have one standard also because the Sanctions Clause refers to various international and foreign regulations, i.e. UN, EU, UK and US). The second issue is about the risk of sanctions under US sanctions regulations for which US law logically applies.

This case offers an opportunity to think about how the Sanctions Clause could have been drafted differently. One could particularly consider that it would make sense to add a qualifier that would specify the degree of exposure to foreign sanctions, e.g. "would *concretely* expose" to "any sanction, prohibition or restriction".

One could also consider adopting sanctions clauses that would expressly provide that the debtor who claims to have the right to avoid the performance of its contractual obligation bear the burden of proof of establishing that it runs the concrete and actual risk of being exposed to foreign sanctions and that would define how the debtor should prove this. One could also think to include in the clause a time period after which the parties would agree that the debtor shall no longer have the right to avoid the performance of its contractual obligation. This period of time could be defined by referencing the statute of limitations that may apply under the relevant laws relating to the sanctions that could be imposed on the debtor.

Furthermore, one could wonder about the impact the burden of proof has on the outcome of the case. As the party raising an exception, the Insurance had the burden of proving the risk of US sanctions under general legal principles (art. 8 SCC), which it sought to do by showing similarities between the ransomware used by the hackers and the ransomware associated to Evil Corp. It is, however, somewhat surprising that the cantonal court cited the Insurance for failing to comment on the ransom payment, which seems to have been settled and decided by the Company alone. Given that the Company's duty to disclose and report was not challenged here, little is known about these circumstances. However, one must note that Swiss law defines the burden of proof as a matter of substantive law (rather than procedural law). The Swiss legal literature, which to the authors' knowledge has not been confirmed yet by the Federal Supreme Court, considers that clauses modifying or qualifying evidentiary standards are enforceable, subject to excessive restrictions of the other party's defence rights (art. 27 SCC)[9].

The clause of the Insurance Policy that was disputed in this case is a type of Lloyd's Market Association (LMA) sanctions clause, specifically LMA3100, which was first issued in 2010.[10] It was amended in October 2023 to adapt to a judgment handed down by a French Court of Appeal. The French court interpreted the clause as an exclusion clause and ruled that it did not comply with the necessary criteria for such a clause to be valid under French law,[11] which prompted LMA to revise it. These modifications resulted in LMA3100A[12] and LMA3200[13] which aim to enhance clarity, especially concerning the suspension of coverage rather than its outright exclusion. Given the Federal Supreme Court's restrictive interpretation in this case, it seems advisable to have the clause reviewed again following this judgment. Such a review could help clarify the conditions under which sanctions clauses are triggered, ensuring that they are applied consistently and in a predictable manner across different jurisdictions.

The UK case of Mamancochet[14] further provides a compelling comparative perspective on the interpretation of a sanctions clause that was similar to the one discussed in this Swiss Federal Supreme Court judgment. In the Mamancochet case, the English High Court dealt with a sanctions clause under circumstances involving U.S. re-imposed sanctions on Iran. The court interpreted the use of the term "exposure" in the sanctions clause not to mean a mere risk of sanctions but rather that any payment made under the claim shall be explicitly prohibited by law.

On a final note, due to the current geopolitical situation, it is likely that the potential application of foreign sanctions regulations will continue to be litigated in contractual disputes in the future, and this not only in the context of cybersecurity/ransomware disputes but in many other commercial disputes.

Other comments on this judgment

Célian Hirsch, L'assureur doit payer, published on 23 October 2023 (https://cdbf.ch/1303/)

Célian Hirsch, Les sanctions américaines et l'assurance cyberattaque, published on 25 October 2023, (www.swissprivacy.law/260)

[1] See https://www.garmin.com/en-US/newsroom/press-release/uncategorized/2020-garmin-issues-statement-on-recent-outage/; see also https://jusletter.weblaw.ch/fr/juslissues/2023/1170/garmin-versicherer-m_0df39bd8a2.html__ONCE&login=false.

[2] See US Department of the Treasury, Press Release "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware", dated December 5, 2019, available at: https://home.treasury.gov/news/press-releases/sm845.

[3] The cantonal court granted the claim of the Company and consequently ordered the Insurance to pay USD 987,098 plus interests to the Company.

[4]For other judgments on the interpretation of contracts, see: https://new.swisscontract.law/2/; https://new.swisscontract.law/3/; https://new.swisscontract.law/10/; https://new.swisscontract.law/16/; https://new.swisscontract.law/21/; https://new.swisscontract.law/25/; https://new.swisscontract.law/28/; https://new.swisscontract.law/29/.

[5] For more information, see Emmenegger Susan/Zuber Florence, To Infinity and Beyond: U.S. Dollar-Based Jurisdiction in the U.S. Sanctions Context, RSDA 2022 p. 114 ss.

[6] See e.g. the UK cases: *Lamesa Investments Limited v Cynergy Bank Limited,* [2019] EWHC 1877 (Comm) *and* Mamancochet Mining Ltd -v- Aegis Managing Agency Ltd & Ors [2018] EWHC 2643 (Comm) (discussed at the end of this document) *and the comments about these cases at:* https://www.hfw.com/Managing-sanctions-risk-in-contracts-the-High-Court-provides-guidance.

[7] See e.g. Rachel Anne Carter and Julian Enoizi, Mapping a Path to Cyber Attribution Consensus, Geneva Association (March 29, 2021) ; Kristen E. Eichensehr, The Law & Politics of Cyberattack Attribution, 67 UCLA L. Rev., p. 520 ss (September 28, 2020) ; see also the important policy work of the CyberPeace Institute, The CyberPeace Institute calls the United Nations Security Council to enforce accountability in cyberspace (July 1, 2024), and Untangling Accountability in Cyberspace (July 21, 2022).

[8] See the recent judgment of Merck & Co. Inc. et al. v. Ace American Insurance Company Co. et al., No. UNN-L-002682-18, 1 (N.J. Super. Ct. Law Div. Jan. 13, 2022), aff'd, Nos. A-1879-21, A-1882-21 (N.J. App. Div. May 1, 2023) ; Nynke Brouwer, Reliance on war exclusion clause after cyberattack fails; insurers must pay out over a billion dollars in damages (May 26, 2023); see also Justine Ferland, Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case, Computer Law & Security Review, Volume 35, Issue 4, 2019, p. 369 ss.

[9] For a recent review of the current legal literature, see e.g. Arnaud Nussbaumer-Laghzaoui, L'interprète du contrat face aux clauses d'intégralité et de confidentialité, in RSJ 119/2023, p. 367, 374-375 with references.

[10] https://www.lmalloyds.com/LMA/News/Releases/lma_051023.aspx.

[11] Cour d'appel de Paris – Pôle 4 – Chambre 8, 21 juin 2022 / n°20/10832 ("faute d'être formelle et limitée, la clause « sanctions » ne peut être valablement opposée à la SA LAFARGE qui est incapable d'en mesurer la portée et l'étendue exactes."), unofficial translation: "Due to its lack of formality and limitations, the 'sanctions' clause cannot be validly enforced against SA LAFARGE, which is unable to ascertain its exact scope and extent".

[12] According to the guidance, only the word "exclusion" in the title was changed to "limitation" as it more accurately reflects the way in which the clause works:

"Sanctions Limitation Clause

No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction, prohibition or restriction under United Nations' resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America."

[13] According to the guidance, this clause is intended to have the same legal effect as LMA3100 and LMA 3100A, but it is described instead as a condition, typically for a court which is unfamiliar with an English insurance clause (specifically a non-common-law jurisdiction). The court can apply it without having to assess whether, for instance, it qualifies as an exclusion within that jurisdiction.

"Sanctions Suspension Clause

It is a condition of this (re)insurance, and the (re)insured agrees, that the provision of any cover, the payment of any claim and the provision of any

benefit hereunder shall be suspended, to the extent that the provision of such cover, payment of such claim or provision of such benefit by the (re)insurer would expose that (re)insurer to any sanction, prohibition or restriction under any:

1. United Nations' resolution(s); or

2. the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America.

Such suspension shall continue until such time as the (re)insurer would no longer be exposed to any such sanction, prohibition or restriction."

[14] Mamancochet Mining Ltd v Defendants Managing Agency Ltd [2018] EWHC 2643 (Comm).

Reproduction authorized with the following reference: Jacques de Werra, Célian Hirsch, Thomas Hua, "Cyberinsurance Coverage for Ransomware Payments vs US Sanctions Regulations", published on: Swiss Contract Law, September 17, 2024, https://swisscontract.law/50-2/