CENTRE DE DROIT
BANCAIRE ET FINANCIER

Cyber attack

# The insurer must pay

Par Célian Hirsch le 23 October 2023

How can an insurer object to having to compensate a listed company for damage estimated at nearly a million following a successful cyber attack ? On the grounds that the payment would contravene US sanctions, since the cyberattack was allegedly the work of Russian hackers under sanctions. However, the Zurich Handelsgericht and then the Swiss Federal Supreme Court were not convinced by this argument (4A_206/2023).

In July 2020, a company listed on the NYSE fell victim to an attack by the Wasted-Locker ransomware, which encrypted its customer data among other things. The attackers demanded a ransom of 1,500 bitcoins (around CHF 13.5 million at the time) in exchange for the decryption key. The company eventually pays the cyber attackers a sum of probably 10 million to obtain the key.

The company takes legal action against one of its UK insurers, which refuses to pay. The insurer claims that the attack originated from Evil Corp, Russian hackers on the Specially Designated Nationals and Blocked Persons-List (SDN list) of the U.S. Treasury Department's Office of Foreign Assets Controls (OFAC). Payment of the insurance benefit would therefore contravene US sanctions. In particular, the insurer relies on the following contractual 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.

The Zurich Handelsgericht accepted the company's claim for payment of almost one million dollars. The court considered that the insurer had failed to prove that the attack originated from Evil Corp, or that Evil Corp benefited financially from the attack. It would therefore be highly unlikely that the insurer would be sanctioned by the FOCA in the event of payment of the insured sum.

The insurer referred the matter to the Swiss Federal Supreme Court, which examined the clause invoked by the insurer.

Firstly, the mere fact that the software used came from Evil Corp, i.e. an entity on the SDN list, is not sufficient to refuse payment of the indemnity. Indeed, as the contractual clause indicates, it is necessary for the insurer to establish a risk of being reprimanded for violating US sanctions.

Secondly, the Federal Court is reviewing whether, as held by the Handelsgericht, it was highly unlikely that the insurer would be sanctioned by the FOCA in the event of payment of the insured sum. The Federal Supreme Court is only examining this question from the angle of arbitrariness, since it concerns the application of foreign law in a pecuniary case.

In the cantonal judgment, the Handelsgericht held firstly that it had not been proven that the attack originated from Evil Corp. Secondly, it held that not every deployment of the Wasted-Locker software constitutes an “interest” of Evil Corp within the meaning of US sanctions law (property or interests in property). Indeed, even if Evil Corp were to be the author of this software, it cannot be ruled out that it could be used by other cyber-attackers, without Evil Corp deriving any financial interest from it. Finally, the FOCA has not yet opened any proceedings against the listed company, nor against the American company that negotiated and paid the ransom, nor against the other insurers who paid their benefits in connection with this cyberattack.

The Federal Court considers that this reasoning is arbitrary. In particular, it rejects the insurer’s argument that any use of Wasted-Locker (even by third parties) leads to a prohibited transaction, since Evil Corp would participate in this transaction either directly or indirectly via Wasted-Locker. The Federal Court therefore dismissed the insurer’s appeal.

This ruling is interesting for several reasons, and calls for a few brief comments.

Firstly, it is the first ruling by the Swiss Federal Supreme Court on the payment of ransom following a cyber-attack. This issue has been the subject of recent doctrinal publications, which examine in particular whether the payment of ransom, by the victim or by the insurer, constitutes a criminally reprehensible act (cf. Benhamou Yaniv/Wang Louise, Cyberattack and ransomware : legal risks to be paid and insurability of ransoms, RSDA 2023 p. 80 ff ; Sarrasin Delphine/Pangrazzi Sara/Meyer Pauline, The Legal Risks of Ransomware Payments, PJA 2023 pp. 1077 ff).

Secondly, this ruling is a reminder of the very broad scope of U.S. sanctions (see also Emmenegger Susan/Zuber Florence, To Infinity and Beyond : U.S. Dollar-Based Juristiction in the U.S. Sanctions Context, RSDA 2022 pp. 114 ff). However, in its ruling, the Handelsgericht points out that the FOCA has not yet published any decisions on cyber sanctions, which makes it difficult to understand its practice in this area.

Finally, the insurer failed in casu to prove that the attack was attributable to Evil Corp. However, the standard of proof was lower than in Swiss law, since US law applied as the lex causae. The latter provides for a “more likely than not” criterion (degree of proof of preponderance). Unfortunately for the insurer, the Handelsgericht ruled that several of the cyberexpertises it had produced were filed late and therefore inadmissible (cf. art. 229 al. 1 let. b CPC).