News – December 03, 2021

HACKING AND DIVERSION OF INTERNATIONAL PAYMENTS

We are increasingly requested to assist our corporate clients in cases of computer fraud perpetrated by hackers who first divert and then steal international payments.
The most commonly used techniques to divert payments from the buyer to the seller are phishing, the installation of viruses (e.g. Trojans) and the so-called man in the middle technique.
More frequently, the hacker (man in the middle) enters the relationship between seller and buyer:

- enters the system of the seller who must receive a payment from the buyer;
- acquires or counterfeits the seller's e-mail account;
- writes an email to the buyer, apparently coming from the seller, informing him that the seller has modified and/or substituted his bank account, and provides a new IBAN, asking him to make the payment to the new bank details;
- in communicating the modification of the bank account the hacker usually adduces reasons of apparent credibility.

Consequently, the buyer follows the new payment instructions, but once the transfer is made to the new "replacing" IBAN, the seller is not credited.

The reason for the missing of the credit is that the email containing the payment instructions was not sent from the seller's e-mail account, but from a fictitious e-mail account created by the hacker to disguise that of the seller.
The payment is sent to a new account of the hacker, and the unsuspecting buyer will find it very difficult to recover the amount transferred to the fake seller's account, as the hacker usually withdraws the money immediately or transfers it to a foreign account.

From a legal point of view - without going into complex analysis on the law applicable to the case - the failure to credit the seller's bank account almost always integrates a breach of contract attributable to the cheated buyer, who is not discharged from the payment obligation by virtue of the payment made to the hacker; so he will be required to make a new payment to extinguish his obligation to the seller.

And what measures should be taken to eliminate or reduce the risk of intrusion by hackers and, consequently, the risk of payment diversion?

The most immediate precaution, simple but effective, in case one receives from his/her own contractual counterpart an email containing a communication of variation of the payment details or a request for payment to a different bank account from the usual one, is that of ascertaining by telephone the genuineness of the email received and of the modification of the payment provisions.

In any case, it must be kept in mind that the seller is not always and completely exempted from responsibility towards the cheated buyer.
In fact, in case the hacker has intruded in the system of the vendor and taken data to perpetrate the fraud towards the purchaser, the same purchaser could invoke the responsibility of the vendor (joint or exclusive)

HACKING AND DIVERSION OF INTERNATIONAL PAYMENTS

for not having sufficiently protected the data of the purchaser and to have rendered possible the intrusion of the hacker and the perpetration of the fraud.
If that is the case, the buyer may refuse to repeat the payment diverted by the hacker.

The aforesaid possible responsibility of the seller is supported by article 1189 of the Italian Civil Code, according to which "The debtor who makes payment to those who appear legitimated to receive it on the basis of unequivocal circumstances, is freed if he proves to have been in good faith"; and all the more the debtor is to be relieved if the error in identifying the apparent creditor was caused by a fact and/or culpable behavior attributed to the actual creditor, such as that of not having sufficiently protected the data of his own computer system.
In fact, article 82 of the General Data Protection Regulation (GDPR) provides that anyone who suffers damage caused by a breach of the Regulation is entitled to compensation.

For this reason, it is absolutely necessary for companies to equip themselves with effective cybersecurity tools as well as particularly stringent operating procedures, also to avoid incurring in serious violations of the personal data protection legislation (GDPR) and to suffer, in addition to the damage of fraud, also the infliction of a possible penalty for personal data breach.

Other lines of protection could be sought by the defrauded buyer towards the bank where the hacker has opened the new bank account on which he has made the payment.

According to banking regulations, the bank is not liable for non-execution or incorrect execution of the payment if the buyer, who orders the transfer, provides an inaccurate IBAN or other inaccurate information.
But the purchaser could ask the bank where the hacker has opened the new account to account for its level of diligence in carrying out all the checks and investigations that the bank is required to carry out when opening a bank account.
In this regard, it is important to check the following steps in sequence:

- the hacker requests the opening of a bank account on behalf of a different party - the seller - qualifying as such;
- the bank must verify the correspondence and truthfulness of the identity declared by the hacker;
- the bank must request a series of documents, in particular in accordance with anti-money laundering legislation;
- the bank must request and ascertain the powers of legal representation of the hacker requesting the opening of a bank account.

Given the above sequence, it would even seem impossible for a hacker to falsify all the elements listed above and, more importantly, for a bank to be fooled on all the elements listed above.

As a Firm, we are increasingly shifting and intensifying the search for liability on the part of the bank that, with careless behavior, opens the account to the hacker, in order to pursue the recovery of the stolen sums, also invoking copious case law that imposes on the bank "the diligence of the shrewd banker" (Italian Court of Cassation judgment no. 13777/2007; Italian Court of Cassation judgment no. 806/2016).