



NEWSFLASH

Important Supreme Court decision on wire transfers


#159 July - September 2022 | August 24, 2022

In May 2021, the First Chamber of the Mexican Supreme Court of Justice (the "SCJN" for its initials in Spanish), in decision 206/2020 resolving prior contradictory rulings, held that electronic transfers carried out through systems provided by banking institutions should not be considered infallible; therefore, there is no absolute legal presumption as to their proper functioning or reliability. This implies that the SCJN has considered that the electronic transfer systems generated by banks have a certain degree of risk, which must be evaluated in accordance with the specific case, and any alleged security breach.

In its decision, the SCJN referred to an example that, in 2018, the Bank of Mexico reported that hackers stole around \$300 million pesos by creating ghost orders to transfer funds to fake accounts and then withdraw such funds. The foregoing occurred through a cyber-attack on the application software used by some banks to connect to SPEI, which affected wire transfers, and confirmed the performance of unauthorized operations. Considering this, the Bank of Mexico itself has admitted the violation of its own security systems, which highlights the risks to the security of bank services users.

In the same way, the SCJN resolved that it is not enough to prove that the user identified himself through the mechanisms used by the bank, such as keys or passwords, but also that the bank must prove that it is in compliance with the General Provisions applicable to Financial Institutions issued by the National Banking and Securities Commission (the "General Provisions"). A contrary interpretation would mean a disproportionate burden on the procedural process for the banking user, as it would be necessary to prove the non-compliance of the financial institution with respect to said provisions.

On August 5, 2022, a judicial precedent was published by the Second Collegiate Court in Civil Matters in the State of Jalisco, through which it held the nullity of a bank transfer that was not recognized by the user. Said nullity was based on the bank's breach of the General Provisions, since the electronic operation was performed using an IP address from Israel, without the bank's security systems detecting said operation as unusual.



The Collegiate Court pointed out that the bank's failure to identify and classify the operation as unusual based on the place where it was carried out is relevant to conclude the lack of reliability of the electronic banking system since it is an unusual operation in the eyes of any rational observer, which casts doubt on whether it was actually the account holder who carried out or authorized the operation. The Second Collegiate Court of Circuit in Civil Matters in the State of Jalisco held that the IP address of Israel proves the deficiency of the security mechanisms of the electronic banking system, due to non-compliance with article 312 Bis 2 of the General Provisions, which establishes certain obligations for financial institutions, such as identification of the accessing device, "address range of communication protocols, geographical location, among others", including the detection of the parameters of "regular use" by users.

Therefore, in the opinion of the aforementioned Collegiate Court, having carried out an operation with an IP address from Israel constitutes an unusual activity that warranted, as a basic precaution, automatically terminating the session and suspending the use of the electronic banking service or rejecting the operation.

From what was held, this created a judicial precedent under the heading "ELECTRONIC BANK TRANSFERS. When the internet protocol (IP) address has an unusual place of origin and despite it the bank authorizes the operation without first suspending the electronic banking service or cautionary rejecting the transaction, it should be considered that the customer has not granted its consent, even when all the necessary authentication factors have been used to approve it", which can be consulted in Spanish by [clicking here](#).

Based on the foregoing, although the purpose is to protect the user, this may cause that banks, in order to comply with the General Provisions, require travel notices, either within the country or abroad, as was the case a few years ago with debit and credit cards, or some other requirement such as authorizing the geolocation of the mobile device used to access, which can cause inconvenience for users and the violation of certain fundamental rights.

It should be noted that the judicial holding described above does not authorize users to claim the nullity of any banking transaction, but that the specific case will have to be assessed to identify the breach in security or a lack of reliability of the electronic system and the General Provisions in order to be able to legally claim the payment of the amount that was lost through the unrecognized transaction.

Contact:

Eduardo Parroquín

Associate

eparroquin@ccn-law.com.mx