

## Legal Alert: Law establishing the limitation of liability for loss, theft or fraud



June 1, 2020 / By [Paulo Larrain](#), [Ricardo López](#) y [Felipe Riedel](#)

On May 29, 2020, Law No. 21,234 (hereinafter the "Law") was published in the Official Gazette, which amended Law No. 20,009, changing the name of the latter to "Establishment of a regime of limitation of liability for holders or users of payment cards and electronic transactions in case of loss, theft, robbery or fraud" and replacing articles 1 to 5 of the Law.

Modifications introduced by the Law are the following:

### 1. **Title I:** scope and general rules:

This Law regulates the liability regime applicable in cases of loss, theft, robbery or fraud of credit cards, debit cards, payment cards with provision of funds, or any other similar system, hereinafter jointly referred to as "payment cards", issued and operated by entities subject to the supervision of the Financial Market Commission and the regulation of the Central Bank of Chile. It also regulates the liability regime in cases of loss, theft, robbery or fraud of payment cards issued and operated by entities not subject to the supervision and regulation of the aforementioned entities, unless expressly provided otherwise. It will also apply to fraud in electronic transactions. For the purposes of this Act, payment cards and electronic transaction systems may be designated jointly as "means of payment".

- Holders or users of means of payment, as well as holders of other accounts or similar systems enabling electronic

transactions (referred to as "users") may limit their liability in the event of theft, robbery, loss or fraud, to the extent that timely notice is given to the issuer.

- The issuer or provider of the financial service (referred to jointly as "issuers") must provide qualified and free channels, available 24 hours a day and permanently, that allows the making and recording of notices to users, providing a reception and identification code. Once the notice has been received, the issuer must immediately block the means of payment to carry out transactions. In addition, the user must be sent a communication that includes the number, reception code or tracking identifier, and the date and time of the notice.
- For **operations carried out after the notice**: The issuer will be responsible.
- With respect to **operations carried out prior to the notice**: Users can claim from the issuer, within a period of 30 days, those operations with respect to which users do not know they had granted his authorization or consent. The claim may include operations carried out in the 120 calendar days prior to the date of the notice given by the user.
- In relation to **unauthorised operations**, special consideration will be given to the fact that the issuer has sent a fraud alert to the user, identifying suspicious operations, and that there is proof of receipt by the user, in accordance with the service provision contract.
- In cases **were users do not know that they had authorised an operation**, it will be up to the issuer to prove that the operation was authorised by the user and that it is registered under his name. The registration of transactions alone will not necessarily suffice to prove that the transaction was authorized by the user.

## **2. Title II: Cancellation of charges or restitution of funds:**

- The issuer must proceed to the cancellation of charges or the restitution of funds corresponding to the operations claimed:

**a) If the amount is equal or less than 35 UF<sup>[1]</sup>**: The issuer must proceed to the cancellation of the charges or the restitution of the funds within 5 working days from the date of the claim.

**b) If the amount is higher than 35 UF**: Within 5 working days from the claim, the issuer must cancel the charges or restate 35 UF. For the amount higher than that figure, the issuer will have 7 additional days to cancel them, refund them to the user or exercise the following actions, notifying the user of the decision taken.

- **Actions**: If within the previous term, the issuer compiles background information that accredits fraud or serious fault on the part of the user, the issuer may exercise the actions provided by the Law before the respective Local Police Court. The procedure for exercising this action is established in Paragraph 1 of Title IV of Law No. 19,496 on consumer protection rights.

**a) If the Court declares that there is no sufficient background to prove the existence of fraud or serious fault on the part of the user**: the issuer is obliged to return the claim funds, duly adjusted, applying for this purpose the maximum conventional rate from the date of the notice, and to pay the judicial costs.

**b) If the Court declares there is fraud or serious fault on the part of the user**: the cancellation of the charges or restitution of funds will be left without effect, without prejudice to the compensation for damages.

- **The issuer is prevented from offering users the contracting of insurance whose coverage corresponds to risks or losses that the issuer must assume in accordance with this Law.**
- **The issuers must block all those means of payment that are inactive for more than 12 consecutive months**, notifying the user, and must publish every six months on their electronic sites the number of users affected, indicating the amounts involved and deadlines for response or compliance with their obligations. In addition, they must send the information to the Financial Market Commission.
- **Issuers must have the following security measures:**

**a) Monitoring systems to detect operations that do not correspond to the user's usual behaviour**

**b) Implement internal procedures to manage the alerts generated by such monitoring systems.**

**c) Identify patterns of potential fraud, in accordance with industry practices and recommendations, which must be incorporated into the operations monitoring system. The issuer is prevented from offering users the contracting of insurance whose coverage corresponds to risks or losses that the issuer must assume in accordance with this Law.**

- Issuers must block all those means of payment that are inactive for more than 12 consecutive months, notifying the user, and must publish every six months on their electronic sites the number of users affected, indicating the amounts involved and deadlines for response or compliance with their obligations. In addition, they must send the information to the Financial Market Commission.

## **3. Title III: Liability for fraud in payment cards and electronic transactions**

- Although the new Article 7 of Law No. 20.009 maintains a similar structure to the previous Article 5, it should be noted that the change in its name constitutes an **extension of criminal protection** to other means of payment, other than

credit and debit cards, such as payment cards with provision of funds and electronic transactions. In this sense, letters a) to f) of Article 7 of Law No. 20,009 maintain their governing verbs, but the denomination of the object of protection is modified to extend it to the passwords or other security measures of authentication to make payments or electronic transactions.

- In addition, the new article 7 of Law 20.009 **incorporates two new conducts as letters g) and h)**, which are related to the sanction of the impersonation of the holder or user to obtain the authorization required to carry out transactions; and the malicious obtaining, for oneself or a third party, of an undue payment, either by simulating the existence of unauthorized operations, intentionally provoking it, or presenting it before the issuer as having occurred for causes or in circumstances different from the true ones.
- **Article 7 adds a new criminal type in its final paragraph which sanctions**, in general terms, anyone who by means of any deception or simulation obtains or violates the information and security measures of a current bank account, deposit account, a funds provision account, a payment card or any other similar system, for the purpose of impersonating the holder or user and making payments or electronic transactions.

These offences are now punishable with imprisonment and a fine corresponding to three times the amount defrauded.

- But **Law No. 21,234 not only made the abovementioned modifications. It also incorporated two additional innovations to Law 20.009.** First, it **authorized the use of special investigation techniques in cases where the crimes sanctioned in Article 7 are committed by an illicit association or by an organization or association composed of two or more people**, such as telephone interceptions, the use of undercover agents and informants, among others. Secondly, it provides that the **penalties set out in Article 7 shall be applied without prejudice to any penalties that may also apply to the offences established in Law 19,233 on cyber crime**, being these new conducts considered separate crimes.

[\[1\]](#) 35 UF “unidades de fomento” is equivalent to USD \$1,300. - approx.

## Contacts

For more information, please contact: