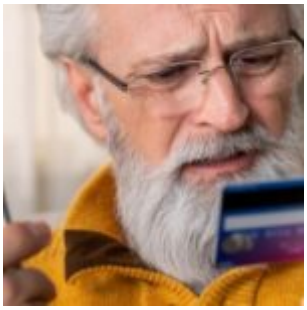
Escroquerie bancaire par téléphone : la banque doit-elle rembourser ?



De plus en plus pratiqué, le « spoofing » téléphonique consiste pour un escroc à se faire passer pour un employé d'une banque, souvent un conseiller bancaire, dans le but de soutirer de l'argent du compte d'un client. La pratique est d'autant plus habile que, très souvent, le numéro de téléphone qui apparaît sur l'écran du téléphone de la victime est celui du conseiller bancaire en question. Mieux, la voix de l'escroc peut même être transformée pour ressembler à celle du conseiller ! Du coup, la victime est en confiance et procède, sans se méfier, aux opérations de paiement que lui demande d'effectuer son interlocuteur.

En principe, la banque est tenue de rembourser le client victime de l'escroquerie sauf si celui-ci a fait preuve d'une négligence grave. La preuve de la négligence grave devant être apportée par la banque. Une preuve qui, selon les circonstances, peut être difficile à établir, ce qui profite alors à la victime.

À ce titre, dans une affaire récente, une employée d'une société de transport avait été contactée par téléphone par une personne qui s'était présentée comme étant un technicien de la banque et qui, prétextant un incident informatique, lui avait demandé d'effectuer différentes manipulations via le système

de paiement à distance afin de permettre la réinscription d'opérations sur le compte de la société. Deux virements avaient alors été exécutés vers des comptes domiciliés en Allemagne pour une somme totale de 98 000 €.

Après avoir déposé plainte pour escroquerie, la société de transport avait demandé à la banque de la rembourser, faisant valoir qu'elle n'avait pas autorisé ces virements. Mais la banque avait refusé, invoquant la négligence grave de la société dans la conservation et l'utilisation de ses données personnelles de sécurité.

Pas de négligence grave

Saisis du litige, les juges ont estimé, au contraire, que la société n'avait pas commis de négligence grave compte tenu des éléments suivants :

– à la demande de l'escroc, l'employée de la société s'était connectée au service de paiement en ligne à l'aide du dispositif de sécurité personnalisé et avait effectué diverses manipulations afin de reconstituer les écritures sans se méfier de son interlocuteur qui ne lui avait pas demandé de mot de passe ;

– la circonstance que l'escroc ait pu usurper le numéro de téléphone de la banque et annoncer le code qui s'affichait sur l'écran de l'utilisatrice était de nature à persuader celle-ci qu'elle était en relation avec un technicien ;

– la connaissance par son interlocuteur des opérations réalisées avant l'appel et de leur disparition avait pu conforter l'employée de la société dans la croyance qu'un incident informatique était survenu.

Cassation commerciale, 12 juin 2025, n° 24-13777