LA BNP CONDAMNÉE À REMBOURSER 54.000 EUROS

mardi 18 avril 2023

La cour d'appel de Versailles a considéré que la "négligence" du client n'était pas avérée. Ce dernier avait été piégé par des escrocs se faisant passer pour sa conseillère bancaire.

Le non-remboursement des clients en cas de fraude bancaire est devenu quasi-systématique depuis la généralisation des systèmes d'authentification de paiement. Mais les choses pourraient changer.

La cour d'appel de Versailles a condamné le 28 mars la BNP Paribas à verser 54.000 euros à un client victime d'une arnaque. Une somme prélevée frauduleusement sur son compte par des escrocs se faisant passer pour sa conseillère bancaire, relate l'association de consommateurs UFC-Que Choisir.

Une arnaque bien ficelée puisque la victime a été contactée via un numéro d'appel identique à celui de sa vraie conseillère bancaire, enregistré dans son téléphone. De plus, les SMS d'authentification des virements bancaires s'affichaient à la suite des précédents messages envoyés par la banque.

Le client s'est rendu compte trop tard de la supercherie. Il a alors prévenu sa banquière et demandé un remboursement des sommes prélevées frauduleusement. Mais la BNP

Paribas a refusé, l'accusant de "négligence grave".

Des systèmes d'authentification loin d'être infaillibles

Un argument de plus en plus souvent avancé par les banques pour échapper à leur obligation légale de remboursement en cas d'opération frauduleuse. Selon elles, si un paiement ou virement a été validé par un SMS ou via l'application dans le cadre de l'authentification à double facteur, le client a commis une "négligence" et ne peut donc pas être remboursé.

Comme le note l'UFC-Que Choisir, cet argument laisse entendre que les dispositifs d'authentification renforcée des banques sont infaillibles. Or, plusieurs failles de sécurité ont été rapportées ces dernières années.

Cette décision de justice fera jurisprudence. Pour obtenir gain de cause, la victime avait conservé et fourni plusieurs éléments de preuves comme des captures d'écran des SMS et appels reçus de la part des escrocs. Il est donc conseillé d'en faire de même en cas de suspicion d'arnaque. De manière générale, il est judicieux de contacter soi-même son conseiller en cas de doute sur l'identité de son interlocuteur et d'inspecter régulièrement ses relevés de compte pour repérer tout mouvement suspect. En cas d'arnaque, contactez immédiatement votre conseiller.

Source: Pauline Dumonteil Journaliste BFM Tech