24 Fraudes aux services de paiement en ligne : le devoir de vigilance de l'utilisateur

Face à l'augmentation du nombre de fraudes aux services de paiement dématérialisé (fraude au président et hameçonnage), les tribunaux attendent de plus en plus de vigilance de la part des utilisateurs de ces services. Le point sur la question avec Me Mongin-Archambeaud, avocat Counsel au cabinet Osborne Clarke.

1 Ces dernières années, les **services de paiement en ligne** ont pris une place prépondérante dans les modes de consommation, ce qui a engendré, pour les utilisateurs de ces services, de **nouveaux risques** tels que la « fraude au président » ou encore l'hameçonnage (« phishing »).
En trois ans, selon l'Office central pour la répression de la grande délinquance financière (OGRGDF), la fraude au président a entraîné un **préjudice** évalué à 430 millions d'euros pour les entreprises françaises.

I. Obligations respectives de la banque et de l'utilisateur

Jusque récemment, une forme d'indulgence pour la personne physique victime de « phishing »

2 Les juridictions avaient habituellement une forme d'indulgence pour ces utilisateurs, qu'elles considéraient avant tout comme les victimes de **fraudes** dont les **procédés** paraissaient **complexes** et étaient méconnus.
La communication à des tiers de coordonnées bancaires comme la transmission à l'établissement bancaire de « faux virements » paraissait « excusable » puisqu'elle était commise à l'insu des victimes.

3 En matière d'**hameçonnage**, les juridictions avaient tendance à appliquer largement les dispositions du Code monétaire et financier relatives au **remboursement** d'**opérations** de paiement **contestées**, figurant actuellement à l'article L 133-18 qui prévoit qu'« en cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu », sans rechercher la faute de l'utilisateur.

4 Elles s'attachaient également à rappeler aux établissements bancaires leur **obligation de restitution des fonds au titulaire du compte** au titre des dispositions de l'article 1937 du Code civil, sauf à démontrer que l'utilisateur avait divulgué « à un tiers, de manière intentionnelle, par imprudence ou par négligence grave, des éléments d'identification strictement confidentiels ayant permis les paiements contestés » (Cass. com. 18-1-2017 n° 15-18.102 F-PBI : BRDA 3/17 inf. 15).
Or, la charge d'une telle **preuve** est extrêmement difficile à rapporter et ce, d'autant plus que dans plusieurs arrêts du 18 janvier 2017 concernant des pratiques de « phishing », la chambre commerciale de la Cour de cassation rappelait que celle-ci ne peut « se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés » (Cass. com. 18-1-2017 n° 15-18.102, précité).

« FRAUDE AU PRESIDENT », « HAMEÇONNAGE » : EN QUOI CONSISTENT CES FRAUDES ?

La fraude au président consiste à s'adresser au service comptable d'une société en se faisant passer pour le dirigeant et à demander le virement de sommes vers des comptes bancaires à l'étranger sous un prétexte trompeur plus ou moins habile, par exemple pour réaliser une opération particulièrement confidentielle.
L'hameçonnage (« phishing ») vise, quant à lui, des personnes physiques et non des sociétés. La victime reçoit un e-mail semblant provenir d'une entreprise de confiance (site de e-commerce, banque, réseau social...) l'invitant, par le biais d'un lien hypertexte, à transmettre des données de paiement (numéro de carte bancaire, nom d'utilisateur, cryptogramme...).

LUCIE MONGIN-ARCHAMBEAUD
Avocat Counsel
Osborne Clarke

Diplômée de l'ESSEC et du CAPA, Lucie Mongin-Archambeaud intervient dans tous les types de contentieux susceptibles de survenir dans le cadre de la vie de l'entreprise. Elle accompagne les dirigeants et entreprises dans la mise en place de programmes de compliance anticorruption, et plus généralement dans la gestion des risques.

5 La **doctrine** a largement critiqué cette position jurisprudentielle en y voyant une « déresponsabilisation » de l'utilisateur de carte bancaire (T. Samin et S. Torck : RD bancaire et fin. 2017 comm. n° 44) et une sorte de responsabilité automatique de l'établissement bancaire.
Cette jurisprudence a donc évolué pour se rapprocher des solutions retenues en matière de fraude au président, plus exigeantes à l'égard de l'utilisateur.

La naissance et l'affirmation du devoir de vigilance de l'utilisateur

6 C'est dans ce contexte que les juridictions ont rétabli un **équilibre dans les obligations respectives** de l'établissement bancaire et de l'utilisateur.
Dans deux décisions récentes en matière de « phishing », la chambre commerciale de la Cour de cassation s'est fondée sur les dispositions de l'article L 133-6 du Code monétaire et financier - qui im-

pose à l'utilisateur du service de paiement de prendre toute mesure raisonnable pour préserver la **sécurité de ses dispositifs de sécurité personnalisés** – pour lui rappeler son devoir de vigilance (Cass. com. 25-10-2017 n° 16-11.644 FS-PBI : BRDA 23/17 inf. 12 ; Cass. com. 28-3-2018 n° 16-20.018 FS-PB : BRDA 9/18 inf. 16).

« L'utilisateur doit veiller à la sécurité de ses dispositifs de sécurité personnalisés »

Cette position se rapproche de celle retenue par la Cour de cassation en matière de fraude au président : elle avait clairement posé comme principe, depuis juin 2016, que l'obligation de remboursement de l'utilisateur des sommes « détournées » ne s'imposait qu'en cas d'« anomalie dans le fonctionnement du compte » pouvant être détectée par l'établissement bancaire (Cass. com. 28-6-2016 n° 14-21.256 F-D : BRDA 15-16/16 inf. 13) ou d' « irrégularité matérielle apparente des demandes ou d'opérations au caractère inhabituel ou anormal » (CA Paris 16-2-2018 n° 16/12192).

7 C'est en réalité toujours le principe de **limitation** de la **réparation** du préjudice en cas de **faute de la victime** qui s'applique en vertu des dispositions de l'article L 133-19 IV du Code monétaire et financier : « la victime ne peut prétendre au remboursement intégral des sommes indûment versées dès lors que la fraude a été favorisée par son comportement fautif » (CA Lyon 31-3-2016 n° 15/06043 ; Cass. com. 28-6-2016 n° 14-21.256 F-D : RJDA 11/16 n° 809).
Les établissements bancaires n'ayant pas à s'immiscer dans les affaires de leurs clients, leur devoir se limite à la « surveillance de la cohérence des opérations effectuées avec la connaissance actualisée de leurs clients » (Cass. com. 28-6-2016 n° 14-21.256 précité et CA Colmar 8-11-2017 n° 16/03529).

Dorénavant, les juridictions s'attacheront donc, en matière de fraude au président comme en matière d'hameçonnage, à examiner précisément si l'utilisateur a lui-même commis « une négligence grave » en transmettant un ordre de virement ou des données personnelles alors qu'il pouvait détecter la fraude.

II. Appréciation de la responsabilité de l'utilisateur

Eléments caractéristiques de la négligence grave

8 Il ressort de l'examen des différentes décisions rendues en matière de fraude au président ou de « phishing » que plusieurs **éléments factuels** seront **pris en considération** par la juridiction pour déterminer si l'utilisateur a commis une négligence grave (C. mon. fin. art. L 133-19, IV).
Depuis l'arrêt du 27 octobre 2017 en matière de « phishing », la juridiction recherche si l'utilisateur a pu avoir conscience que l'e-mail lui demandant des éléments d'identification confidentiels était frauduleux (Cass. com. 25-10-2017 précité).
Pour cela, elle examinera attentivement le **niveau de sophistication** de la fraude et les mêmes indices que ceux qui étaient analysés en matière de fraude au président.
La victime ne pourra pas prétendre au remboursement intégral des sommes indûment versées dès lors qu'elle aurait dû douter de la **provenance du message électronique** en raison notamment des fautes d'orthographe et de syntaxe, de l'adresse e-mail dont la structure est anormale, émanant d'un interlocuteur inhabituel, éventuellement accompagné d'une signature grossièrement imitée (CA Lyon 31-3-2016 n° 15/06043 et CA Paris 17-11-2017 n° 16/06685). Son manque de réactivité sera également un critère d'appréciation de sa négligence grave (CA Paris 16-2-2018 n° 16/12192).

« L'orthographe du mail, son auteur doivent attirer l'attention de l'utilisateur »

Recommandations en cas de « phishing » ou de fraude au président

9 L'utilisateur devra donc bien s'attacher à examiner la provenance des messages reçus. Sa **vigilance** lui permettra d'éviter la fraude ou, le cas échéant, de réclamer un remboursement intégral des sommes indûment versées auprès de l'établissement bancaire puisqu'il aura satisfait à ses propres obligations en prenant « toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées » (C. mon. fin. art. L 133-16) et en ayant informé « sans tarder, aux fins de blocage » l'établissement bancaire (art. L 133-17).

10 Parallèlement, un **dépôt de plainte pénale** contre les auteurs du « phishing » et de la fraude au président est recommandé. Même s'il est évident que l'identification des auteurs de telles infractions, agissant le plus souvent depuis des adresses IP à l'étranger, sera difficile, que la procédure pénale reste longue et que rien ne garantit la solvabilité des auteurs de l'infraction, le dépôt de plainte renforcera la qualité de victime de l'utilisateur dans le cadre de la demande en remboursement auprès de l'établissement bancaire.

11 Dans le cas de la fraude au président, la victime pourra déposer plainte des **chefs** d'escroquerie (C. pén. art. 313-1) ou d'usurpation d'identité (C. pén. art. 226-4-1, al. 2) lorsque l'auteur de l'infraction se sera fait passer pour le dirigeant, par exemple.
Dans le cas d'hameçonnage, c'est davantage l'infraction de collecte frauduleuse de données à caractère personnel (C. pén. art. 226-18) qui devra être privilégiée.

12 C'est donc sur l'utilisateur que repose dorénavant un devoir de vigilance accru qui s'explique par une meilleure maîtrise des technologies et une plus grande connaissance de ces fraudes.