Les Arnaques aux faux ordres de virement (FOVI) : quels recours en indemnisation pour les victimes ? Par Charlyves Salagnon, Avocat.

Parution : vendredi 10 juin 2022

Adresse de l'article original :
https://www.village-justice.com/articles/les-arnaques-aux-faux-ordres-virement-fovi-quels-recours-indemnisation-pour-les,42895.html

Récente, mais désormais courante, l'arnaque aux faux ordres de virement (ou FOVI) est en pleine recrudescence.

Dirigeant de société, locataire, employeur, il leur est arrivé d'effectuer un virement à un fournisseur, à un bailleur ou à un employé sans que ceux-ci ne le reçoivent.

Ce virement a été détourné par des escrocs organisés profitant d'un contexte de dématérialisation progressif, qui est par ailleurs accélérée par la crise sanitaire.

Pour prendre un cas d'espèce, un couple de normands avait dernièrement fait appel à un artisan pour la construction d'une piscine.

Réceptionnant la facture et le RIB de celui-ci sur leur boîte mail, ils procèdent légitimement au paiement par ordre de virement bancaire.

Quelques jours plus tard, en l'absence de paiement de son côté, l'artisan les contacte, et l'arnaque se révèle.

Leur boîte mail a en réalité été piratée, puisque des escrocs ont détourné les échanges de mails entre le couple et l'artisan et ont frauduleusement remplacé le RIB de ce dernier par celui d'un compte bancaire leur appartenant.

I - Quelle est la typologie de ces arnaques ?

L'arnaque au faux ordre de virement (ou FOVI) désigne un type d'escroquerie qui, par usurpation d'identité, vise à amener la victime à réaliser, à son insu, un virement de fonds sur un compte bancaire frauduleux.

L'usurpateur peut se faire passer pour tiers connu de la victime (c'est l'exemple d'un dirigeant, d'un fournisseur ou bien d'un salarié).

Cette escroquerie peut être réalisée par voie téléphonique. Néanmoins ce sont les boîtes mails qui sont, et de manière exponentielle, les plus touchées par la pratique.

Il s'agit donc de cybercriminels qui profitent du piratage des systèmes de messagerie numérique pour usurper l'identité de personnes telles qu'un salarié, qu'un fournisseur, ou qu'un dirigeant de société, dans le but de faire verser de l'argent sur un de leurs comptes bancaires.

II - Quels sont les recours juridiques ?

Il convient de préciser le comportement à adopter à la suite d'une arnaque identifiée (A), avant de déterminer quels sont les outils juridiques accordés aux victimes afin d'obtenir l'indemnisation de leur préjudice (B).

A - Les étapes préalables à tout recours en indemnisation.

Avant d'envisager les recours juridiques à disposition des victimes, certaines étapes doivent être effectuées afin de permettre aux victimes de mettre toutes les chances de leur côté et de limiter le préjudice résultant d'une telle arnaque.

Identifier les opérations frauduleuses : Il est préférable, dans un premier temps, d'identifier précisément les virements frauduleux exécutés ainsi que tous ceux qui serons susceptibles de l'être.

Bloquer les coordonnées du compte destinataire : Puis, les coordonnées bancaires du compte destinataire doivent être bloquées.

Information de la hiérarchie et des autorités : enfin, il convient, lorsque l'attaque vise une société, d'informer immédiatement la hiérarchie, le service comptable ainsi que toute personne responsable ou chargée d'effectuer ces virements pour renforcer leur niveau de vigilance.

Si le virement est en cours, il est impératif d'alerter, selon la situation, l'établissement bancaire concerné, le cabinet comptable ou le service comptabilité afin d'en obtenir la suspension. S'il est exécuté, avertir son établissement bancaire du caractère frauduleux de l'ordre de virement est impératif à toute demande de restitution des fonds. Dans l'hypothèse d'un piratage de boite mail, un changement immédiat du mot de passe est capital.

Enfin et surtout, il est fondamental de conserver toutes les preuves relatives au virement frauduleux. Il peut s'agir des mails, des messages, d'un RIB, de numéros de téléphone, de noms, de factures, ou de tout élément qui faciliterait l'identification de la fraude. Ces éléments seront mobilisés à l'appui de la demande ultérieure en indemnisation.

B - Les outils juridiques.

Avant d'engager toute procédure à l'encontre de l'établissement bancaire (2) il convient, pour toute victime d'une telle arnaque, d'immédiatement déposer plainte (1).

1 - Le dépôt de plainte.

Il existe des infractions autonomes, sanctionnées par le droit pénal, qui correspondent aux cas d'arnaques aux faux ordres de virement. Il est important de systématiquement déposer plainte en parallèle des démarches à effectuer auprès de l'établissement bancaires (voir infra). Il faudra, en ce sens, déposer plainte au commissariat de police ou à la brigade de gendarmerie de dépendance en fournissant l'ensemble des preuves à disposition, rapidement à la suite de l'identification de l'arnaque.

Il est possible de se faire assister d'un avocat dans ces démarches. Celui-ci entamera les procédures nécessaires à la récupération des fonds frauduleusement versés. D'autant plus que ceux-ci auront très souvent été versés à l'étranger, ceci complexifiant ledit processus.

Son expertise permettra d'identifier le titulaire du compte localisé à l'étranger en se mettant en relation avec l'établissement bancaire au sein duquel figure ledit compte.

Trois infractions correspondent à la situation d'arnaque au faux ordre de virement : l'escroquerie, l'usurpation d'identité et l'accès frauduleux à un système de traitement automatisé de données.

- L'**escroquerie** est définie à l'article 313-1 du Code pénal : Il s'agit du fait

> « *soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende* ».

Les arnaques aux faux ordres de virement correspondent à la lettre de l'article sus-retranscrit dès lors qu'il s'agit bien de personnes usant d'un faux nom ou d'une fausse qualité (celle de fournisseur, de salarié ou de bailleur par exemple) (1), trompant une personne physique ou morale (la société ou le locataire ou l'employeur trompés par exemple) (2) à remettre des fonds (3).

La Cour de cassation précise que l'infraction d'escroquerie est caractérisée lorsque celui qui, par l'usurpation des identités de trois clients, donne des ordres de virements par internet et télécopie à une banque afin de faire transférer de leur compte réel ouvert auprès d'une banque néerlandaise, aux moyens de comptes ouverts en France, des sommes approchant un à deux millions d'euros [1].

Il faut ici noter que la tentative d'escroquerie est réprimée à l'article 313-3 du Code pénal, leurs auteurs encourant les mêmes peines que l'infraction effectivement réalisée. Il ne faut donc pas hésiter à déposer plainte dès lors qu'une telle tentative est identifiée. Cette vigilance permettra de lutter plus globalement contre ces pratiques frauduleuses.

- **L'usurpation d'identité** est visée à l'article 226-4-1 Code pénal. Il s'agit ici du fait

> « *d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 euros d'amende* ».

Les auteurs des arnaques aux faux ordres de virement se faisant régulièrement passer pour un fournisseur, pour un salarié ou pour un locataire, l'infraction d'usurpation d'identité sera aisément caractérisée. L'on pense par exemple à l'escroc qui, ayant infiltré la boite mail d'un employé d'une société, observe la réception d'une facture d'un fournisseur. Il se fera passer pour lui en modifiant le RIB figurant en pièce jointe, afin d'y insérer le sien.

Ici encore la tentative d'usurpation d'identité est également réprimée [2] les peines encourues étant, à nouveau, identiques à celle de l'infraction effectivement réalisée.

- **L'accès frauduleux à un système de traitement automatisé de données** est proscrit à l'article 323-1 du Code pénal. Il s'agit là du

> « *fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende* ».

Cette infraction pourra être caractérisée dans l'hypothèse où l'escroc à l'origine de l'arnaque infiltre un service de messagerie numérique. En réalité, cette infraction sanctionne plus largement la pratique dite du phishing à l'origine dudit piratage. Le phishing est une cyber-attaque utilisée par des cybercriminels pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Ils envoient généralement des courriels ou des sms comportant de faux messages de type « *vous avez gagné un cadeau, veuillez cliquer sur le lien ci-dessous pour en savoir plus* ». Le fait de cliquer sur cet hyperlien permettra le piratage. Il faut donc faire preuve de prudence lors de la consultation de courriels suspects.

A l'instar des infractions sus-évoquées, nous invitons les victimes à déposer plainte en cas de tentative d'accès frauduleux à leur boîte mail conformément aux articles 323-1 à 323-3-1 du Code pénal.

L'action peut toutefois sembler limitée dans ses effets.

Elle ne peut suffire, dès lors qu'il est rare que les enquêtes permettent de parvenir à identifier, dans des délais raisonnables, les auteurs de ces arnaques.

Il est donc recommandé, pour la victime, de tenter d'actionner la responsabilité des différents intervenants, pour tenter d'obtenir le remboursement des sommes versées en engageant la responsabilité de cette dernière.

2 - Engager la responsabilité civile des banques.

L'article L133-24 du Code monétaire et financier dispose que : « *l'utilisateur de services de paiement signale, sans tarder, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et au plus tard dans les treize mois suivant la date de débit* ».

Il est, dès lors, impératif de signaler à sa banque le virement frauduleux, et ceci dès son identification. La banque devra immédiatement rembourser à son client le montant du virement, sauf pour elle à démontrer que « *l'opération était en réalité dûment autorisée* » ou que son client n'a « *pas satisfait intentionnellement ou par négligence grave, aux obligations* » qui lui incombent. Il est néanmoins possible, pour la victime, dans ce dernier cas, de prouver le manquement de la banque à ses obligations à son égard [3].

Il est en effet possible de se prévaloir du manquement d'un établissement bancaire à ses obligations afin d'obtenir la réparation de son préjudice résultant de l'opération frauduleuse.

Les établissements bancaires sont, conformément à l'article 1937 du Code civil, et à leur qualité de dépositaires des fonds de leurs clients, tenus de « *restituer la chose déposée qu'à celui qui la lui a confiée, ou à celui au nom duquel le dépôt a été fait, ou à celui qui a été indiqué pour le recevoir* ». Le principe de non-ingérence dans les affaires de leur client leur interdit, *a priori*, d'interférer dans la gestion des affaires de ceux-ci, notamment en appréciant le bien-fondé ou l'opportunité des opérations réalisées [4].

Ce principe doit être tempéré en ce sens qu'il est limité par une obligation de vigilance de la part des établissements bancaires. Il est ainsi possible de reprocher à une banque de ne pas avoir procéder aux diligences et aux vérifications nécessaires qui leur incombent.

L'article L561-6 du Code monétaire et financier met à la charge de la banque, pendant toute la durée de la relation d'affaires et ce, dans la limite de ses droits et obligations, un devoir de vigilance constante et d'examen attentif des opérations effectuées. Il doit identifier les irrégularités formelles ou matérielles qu'il peut constater [5]. Le changement soudain des coordonnées bancaires d'un fournisseur de la société, dans le cas d'une arnaque au faux ordre de virement, peut constituer une telle irrégularité.

Ce qui pourrait dans cette situation engager la responsabilité de la banque est précisément le caractère inhabituel que peut revêtir ce type d'opération. L'on pourrait reprocher à une banque de ne pas avoir effectué d'acte de vérification ou de mise en garde vis à vis d'un ordre de virement.

La situation pourrait être inhabituelle en raison du montant du virement mais également en raison de la localisation compte bancaire du destinataire [6]. En ce sens, si la victime n'a jamais adressé de virement aux Pays-Bas, par exemple, une banque devrait s'interroger quant à la normalité de cette opération [7].

A défaut, et si elle n'attire pas l'attention de son client quant au transfert, ni ne sollicite de confirmation de sa part, elle pourrait voir sa responsabilité engagée.

La victime pourra dès lors prétendre à des dommages et intérêts sur fondés sur la responsabilité contractuelle du banquier manquant à ses obligations de mandataire en raison du contrat auquel l'exécution du virement se rattache.

Elle est tenue d'effectuer ces vérifications sans qu'il ne s'agisse d'un acte d'ingérence dans les affaires de son client. Il lui est impossible de s'exonérer en invoquant ce motif [8].

On ne peut davantage reprocher à la victime de ne pas s'être informée des risques relatifs à ce virement. En effet, les escrocs se faisant passer pour des tiers connus de la victime, usent de techniques permettant de rendre plus vraisemblables encore les demandes de virement [9].

L'on pense ici au cas du fournisseur habituel d'une société adressant une facture et un RIB sur lequel doit être effectué le paiement. La société cliente croît légitimement verser l'argent à son cocontractant alors même que des escrocs se sont introduits dans sa messagerie pour modifier les coordonnées bancaires indiquées.

Les établissements bancaires sont de surcroît régulièrement confrontés à ce type d'arnaques. Ils connaissent les méthodes mais surtout les États en direction desquels les virements frauduleux sont communément adressés.

Certaines banques ont décidé d'alerter leur client par mail ou par sms en mettant en place des procédures permettant de sécuriser les virements de sommes importantes.

En tout état de cause, l'accompagnement d'un professionnel du droit nous paraît devoir être envisagée par les victimes de telles arnaques.

Charlyves Salagnon, Avocat Associé (Cabinet BRG Nantes-Paris) Avocat au Barreau de Nantes [->salagnon chez brg-avocats.fr]

[1] Crim. 12 janvier 2011, n° 10-83.180.

[2] Article 225-2 Code pénal.

[3] CA, Paris, 29 juin 2018, n° 16/19003.

[4] Chambre commerciale, 11 mai 1999, n°96-16.088.

[5] Chambre commerciale, 9 juillet 1996, n° 94-17.119.

[6] Paris, 12 janv. 1996, le client n'avait ici aucune activité à l'étranger.

[7] CA, Versailles, 2 février 2021, n° 19/08729.

[8] CA Paris, 14 avril 2016, n° 14/23355 ; CA Caen, 4 novembre 2021 / n° 18/03523 ; CA Versailles, 10 septembre 2019 / n° 18/02972.

[9] Com. 22 janvier 2002, n° 99-16.571.