Fédération Bancaire Française

18, rue La Fayette - 75440 Paris cedex 09
Tél : 01 48 00 52 52 - Fax : 01 42 46 76 40

E-mail : extranet@fbf.fr

Communication Adhérents

Information

Numéro : 2018006

Date : 19/01/2018

Rédacteur : de Montbron Aude

Contact : cfonb@cfonb.fr

Class.FBF 5

mots clés : CFONB, FRAUDE, GUIDE, MOYEN DE PAIEMENT, **PERSONNEL, PREVENTION**

Communication CFONB n° 2018-0002 - Guide de sensibilisation à la prévention de la fraude (nouvelle version - janvier 2018)

Annule et remplace la Communication adhérents n° 2017/114 du 19/12/2017

Chers Adhérents,

Veuillez trouver ci-jointe la Communication CFONB n° 2018-0002 concernant le Guide de sensibilisation à la prévention de la fraude.

COMMUNICATION CFONB

Numéro : 20180002	**Contact** : cfonb@cfonb.fr	CFONB Comité Français d'Organisation et de Normalisation Bancaires
Date : 19/01/2018		
Mots clés : FRAUDE, GUIDE, MOYEN DE PAIEMENT, PERSONNEL, **PREVENTION**		
Guide de sensibilisation à la prévention de la fraude ***Référence(s) :*** ***Annule et remplace la communication n° 20170058 du 19/12/2017***		

Le Président

Paris, le 19 janvier 2018

Madame, Monsieur,

La présente communication annule et remplace la communication publiée le 19 décembre 2017[1] suite à une correction apportée à la partie « virement » du guide de sensibilisation à la prévention de la fraude.

Pour rappel, ce document expose les règles essentielles de prévention et de vigilance destinées à contrer les tentatives d'escroqueries dont pourraient être victimes les établissements ou leurs clients.

Ce guide traite d'une part des fraudes aux moyens de paiement suivants : chèque, virement, prélèvement et, d'autre part, des fraudes dites transversales (l'utilisation de la banque en ligne, l'ingénierie sociale, la « cavalerie » et les autres escroqueries diverses).

Nous vous remercions de bien vouloir vous référer à la version qui vient d'être publiée sur le site Extranet du CFONB (www.cfonb.org) à la rubrique Espace documentaire > Divers.

Pour mémoire :

- L'usage de ce guide est strictement réservé à la Profession.
- D'un point de vue pédagogique, une meilleure appropriation par les collaborateurs concernés a été constatée dès lors que le document faisait l'objet d'ajouts et/ou de commentaires, tels par exemple la présentation de cas concrets de fraude auxquels l'établissement a été confronté.

Veuillez agréer, Madame, Monsieur, mes salutations distinguées.

Yannick CHAGNON

[1] Communication n° 20170058 du 19/12/2017 - Guide de sensibilisation à la prévention de la fraude

CFONB

Comité Français d'Organisation et de Normalisation Bancaires

GUIDE DE SENSIBILISATION A LA PREVENTION DE LA FRAUDE

SUR MOYENS DE PAIEMENT SCRIPTURAUX AVEC UNE APPROCHE CONCERNANT LES FRAUDES TRANSVERSALES

A L'ATTENTION DES AGENTS D'ACCUEIL, DES COMMERCIAUX ET DES PERSONNELS DE BACK OFFICES

Usage strictement réservé à la Profession

Version décembre 2017

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

SOMMAIRE

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

GENERALITES

Ce guide a pour objet de rappeler aux collaborateurs des banques[1] les divers moyens mis à leur disposition pour lutter efficacement contre la fraude et les tentatives d'escroqueries dont pourraient être victimes les établissements ou leurs clients. Il expose les règles essentielles de prévention et de vigilance destinées à contrer les démarches frauduleuses réalisées notamment au moyen de documents faux, falsifiés ou volés.

Ce guide contient des règles fondamentales permettant de limiter le nombre d'escroqueries et leurs effets, voire de détecter de nouvelles fraudes. Son contenu concerne plus spécifiquement :

- la description des divers modes opératoires de la fraude,
- les mesures préventives et les règles de vigilance à observer pour déjouer les tentatives.

A l'origine, ce document présentait exclusivement des cas de fraude sur les moyens de paiement. En raison du constat situant « l'attaque » très souvent plus en aval de l'ordre que sur le moyen de paiement lui-même, le contenu du guide a été élargi.

Aussi, cette nouvelle version « revisitée » consacre une large partie spécifique aux fraudes transversales avec la fraude en ligne, l'ingénierie sociale, la « cavalerie » et autres escroqueries diverses. Dans ces derniers cas, il s'agit souvent de « bonnes vieilles escroqueries » avec un ordinateur comme vecteur de communication permettant une multiplication du nombre d'escroqués, basées essentiellement sur l'usage de la crédulité, voire l'appât du gain des victimes… Les autres chapitres concernant le chèque et le virement ont été actualisés. Une nouvelle partie concernant le prélèvement présente différents scénarios détaillés en raison des spécificités liées à cet instrument de paiement.

Ces informations :

- méritent d'être commentées aux collaborateurs concernés de la Profession ;
- sont à conserver dans des conditions permettant leur confidentialité. Leur contenu ne doit pas être divulgué à l'extérieur de l'établissement bancaire.

A L'ATTENTION DU LECTEUR

Pour des raisons de confidentialité et pour éviter tout détournement subversif, l'ensemble des mesures sécuritaires prises sur les différents moyens de paiements n'est pas exposé.
Ce guide sera complété au fil de l'eau par les travaux du CFONB.

Dans cette version de décembre 2017, seuls les modules le prélèvement et le virement SEPA ont fait l'objet d'une actualisation

[1] Par commodité et simplification de langage, le terme de « banque » est couramment employé. Au regard de la réglementation en vigueur, le vocable de « banque » est utilisé ici pour représenter l'ensemble des « Prestataires de Services de Paiements » [PSP], c'est-à-dire les personnes morales établissements de crédit et les personnes morales « qui fournissent à titre de profession habituelle les services de paiement mentionnés à l'article L.314-1 » du code monétaire et financier [CMF]. De même, l'expression « comptes bancaires » est utilisée pour désigner les « comptes de paiement » des clients tenus par les PSP.
La Banque de France, l'IEDOM, le Trésor Public ainsi que la Caisse des dépôts et consignations (Art. L.521.1 CMF), lorsqu'ils fournissent des services de paiements sont également des prestataires de services de paiement.

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LES FRAUDES AUX MOYENS DE PAIEMENT TRADITIONNELS

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LE VIREMENT

1. PRESENTATION DU MOYEN DE PAIEMENT

De façon générale, il existe deux types de virements/transferts :

- SEPA : virement en euros à l'intérieur et entre pays de l'espace SEPA[2].

Dans le cadre de l'harmonisation des paiements en euros au sein de la communauté européenne, un service de virement domestique européen en euros (€), le virement SEPA (en anglais SEPA Credit Transfer), dit « SCT » a été créé. Ce virement permet à la communauté bancaire européenne d'offrir à sa clientèle un virement ordinaire en euros, utilisable pour tout paiement entre deux comptes de clients ouverts sur les livres des banques de cet espace.

- Transfert International (non SEPA) en devises ou en euros.

DEFINITION

Un ordre de virement (également appelé ordre de transfert dans certains établissements) est un ordre écrit et signé par lequel un client demande à sa banque de transférer une somme déterminée de son compte vers un autre compte :

- détenu par un tiers bénéficiaire ou par le donneur d'ordre lui-même,
- géré soit par la même banque, soit par un autre établissement.[3]

Son exécution peut être immédiate (1 jour ouvrable) ou différée. Dans tous les cas, la fourniture des coordonnées bancaires du bénéficiaire est nécessaire.
Cette opération est réalisée en euros ou en devises à destination de la France ou d'un autre pays.
Cette opération implique pour le donneur d'ordre un dessaisissement définitif et irrévocable[4] des fonds en faveur du bénéficiaire.

➲ Il est donc impératif de s'assurer, avant exécution de l'ordre de virement, quelle que soit la destination des fonds (zone SEPA ou internationale), de sa régularité et de son authenticité.

De façon générale, l'ordre de virement doit obligatoirement être signé, de façon électronique ou manuscrite, par le titulaire du compte ou un de ses mandataires dûment habilité.

NOUVEAUTE

Au sein de l'espace SEPA, un nouveau service de Virement SEPA Instantané[5] sera proposé. Il s'agit d'un service de paiement en temps réel avec mise à disposition immédiate des fonds, qui sera proposé en euros à tous les acteurs dont le traitement sera automatisé de bout en bout ; les normes et les pratiques étant harmonisées, ce service sera offert 24 heures sur 24 et tous les jours du calendrier de l'année. Un délai cible d'exécution et un délai maximum d'exécution de la transaction sont prévus.

---

[2] Liste à jour des pays et des territoires de l'espace SEPA disponible sur le site de l'EPC (http://www.europeanpaymentscouncil.eu/).

[3] Français ou étranger

[4] Selon l'article L. 133-8 du code monétaire et financier, l'ordre de virement est irrévocable dès lors qu'il a été reçu par le prestataire des services de paiement du donneur d'ordre sauf à ce que ces derniers ne soient convenu que l'exécution de l'ordre de virement commencera soit à une date précise soit à l'issue d'une période déterminée. Dans ce cas, l'ordre de virement est révocable par le donneur d'ordre jusqu'à la fin du jour ouvrable précédant le jour convenu.

[5] « Le virement SEPA Instantané »

Pour toute précision complémentaire, n'hésitez pas à vous référer à la documentation CFONB[6] disponible sur les sites Internet et Extranet (www.cfonb.org) du CFONB.

MODALITES D'ECHANGES

- L'ordre de virement sous forme électronique doit être privilégié.
- Les échanges avec les banques doivent être sécurisés via des canaux sécurisés (EBICS, SWIFTnet…) ou à partir de l'outil banque en ligne de l'établissement, ou à l'agence en fonction des services offerts par l'établissement.
- La forme papier doit désormais rester exceptionnelle ; les pratiques consistant en une utilisation du papier, du fax… étant plus faciles à contrefaire.

[6] Le virement SEPA – SEPA Credit Transfert

2. TYPES D'ATTAQUES

Souvent l'ordre frauduleux est destiné à transférer des fonds vers un compte préalablement ouvert en France ou à l'étranger sous une fausse identité ou non, identité réelle ou usurpée. Le compte bénéficiaire des fonds est fréquemment destiné à être vidé dans les 24 heures qui suivent la réception de ceux-ci.

Des comptes de tiers, complices ou non (comptes de mules), peuvent également être utilisés.

- **Les attaques de type Ingénierie sociale utilisent fréquemment le moyen de paiement virement.** Voir module spécifique (fraude au Président, technicien/faux tests).

Avec la Compromission d'IBAN
Les coordonnées bancaires et la signature d'un donneur d'ordre peuvent être obtenues par le vol ou la ruse sous des prétextes divers en récupérant tout document ou tout support contenant ces informations

Un fraudeur vole (ou achète) **une liste d'IBAN**. Une autre méthode non exclusive, utilisée pour obtenir **frauduleusement les coordonnées bancaires et la signature d'un client** donneur d'ordre est le vol de chèques et des courriers d'accompagnement. Cette « subtilisation » peut être effectuée lors de l'acheminement du courrier, lors des différents tris ou bien après la distribution dans les boîtes à lettres des destinataires des plis.

- **Les attaques peuvent être liées à du phishing, du rançongiciel avec ou non l'utilisation détournée de la Banque En Ligne (BEL)** Voir module Utilisation de la banque en ligne.

Boîte e-mail piratée
Le piratage de la boîte mail du client peut générer des attaques particulières. La demande de changement des coordonnées bancaires de la contrepartie est suivie de l'envoi d'un faux ordre de virement. Celui-ci est transmis selon les canaux habituels, voire établi sur le modèle des précédents ordres de virement déjà transmis par le client.

- **D'autres attaques plus anciennes restent encore d'actualité.**

- Munis d'informations concernant les coordonnées bancaires et la signature d'un client, les fraudeurs confectionnent des ordres de virement :
  - en utilisant les imprimés propres aux établissements ou en imitant ces documents
  - Sur du papier libre
  - Sur papier à en-tête de la société, papier volé et aménagé pour l'occasion.

- Les ordres de virements quelle que soit leur destination (France ou étranger) ainsi créés sont transmis à une agence, parfois directement à l'attention du collaborateur en charge de la relation commerciale avec le client ou directement vers le service de traitement spécialisé.

- La signature du client est reportée sur l'ordre selon divers procédés et souvent bien imitée ou reproduite à partir de l'original.

3. MESURES PREVENTIVES

Les mesures préventives concernent essentiellement **la CONNAISSANCE DU CLIENT** donneur d'ordre au travers de ses habitudes.

De façon générale, il est indispensable de vérifier la signature et les pouvoirs[7], en fonction des seuils déterminés par l'établissement, *et de s'interroger sur le bien-fondé de l'opération.*

Quel que soit le canal utilisé, il est souvent nécessaire à l'établissement bancaire de contacter le donneur d'ordre pour obtenir un complément d'informations ou lever certaines interrogations par rapport à l'ordre reçu.

Ainsi, **de simples questions peuvent permettre de détecter un ordre frauduleux**

- Les modalités correspondent-elles aux habitudes du client ?
  - L'opération est-elle en lien avec son activité ?
  - Est-elle conforme aux procédures habituellement utilisées par le client et portées à votre connaissance ? Par exemples : le type d'ordre (document papier ou non…), son mode de transmission (électronique, courrier…)

Dès lors que le client procède habituellement par virements électroniques, la réception d'ordre(s) papier nécessite une attention particulière

  - l'objet du règlement :
    - le libellé indiqué sur l'ordre correspond-il aux affaires traitées par le client ?
    - lorsqu'il s'agit d'un virement SEPA, l'ordre comporte-t-il les références reprises habituellement dans ce type d'ordre présenté par le client (pour rappel, le client a la possibilité de remplir son libellé avec 140 caractères) ?
  - bénéficiaire : il est rare que des entreprises émettent des virements pour un montant important en faveur de particuliers
  - pays de destination : le client est-il en relation d'affaires avec l'étranger ? Avec ce pays plus spécifiquement ?
  - montant de l'opération : est-il plus important que les virements habituellement réalisés par ce client ?

- L'ordre est-il cohérent ?
  - Certains ordres portent en référence « règlement facture », ce qui peut être surprenant lorsqu'il s'agit d'un paiement émanant d'une entreprise en faveur d'un particulier.

- Les coordonnées téléphoniques du donneur d'ordre n'ont-elles pas été changées récemment ?

[7] L'approche pratique est fonction du canal utilisé.

En cas de doute
- ✓ Prendre contact avec le client donneur d'ordre à partir des coordonnées figurant au fichier de la banque.

Par sécurité, ne **JAMAIS** utiliser le numéro de téléphone figurant sur l'ordre de virement.

LES DEMANDES DE RECALL

Définition[8] et causes de rappel

- Le Recall de virement SEPA est une opération par laquelle une banque demande à une autre de lui restituer des fonds correspondant à un virement SEPA émis par erreur.

- Un recall pour motif « FRAD » (identification AT-48) peut être initié dans le cadre d'un virement frauduleux. Cela étant, une fraude sur virement peut recouvrir différents périmètres.

① Opération non autorisée :

L'opération a été ordonnée par une personne ne disposant pas des habilitations (salarié indélicat, suite à l'introduction d'un malfaisant dans les systèmes informatiques du client…). Il peut s'agir d'un virement faux ou falsifié ou détourné par un malfaisant. Le titulaire du compte doit être remboursé immédiatement par son prestataire de service de paiement[9].

② Opération autorisée par le client mais

- Les fonds au crédit du compte ne sont plus disponibles (exemple : le virement faisait suite à une remise de chèque revenue impayée pour fraude)
- Le Client a été trompé (exemple : fraude au Président).

Quelle que soit la situation, une intervention rapide est essentielle en cas de fraude.

AU PERSONNEL DES ETABLISSEMENTS

- Respectez les règles de confidentialité. Ne communiquez pas d'informations concernant votre établissement, même si celles-ci vous apparaissent anodines (par exemple, renseignements relatifs à l'organisation, aux procédures, aux outils, ou aux membres du personnel….)
- Soyez prudent dès lors que votre interlocuteur (donneur d'ordre) se montre très « pressant » pour faire exécuter une opération (appel – rappels…). N'hésitez pas à analyser l'opération avec votre hiérarchie, notamment lorsque l'opération ne correspond pas aux habitudes du client.
- La période de congés ou celle des week-ends prolongés sont souvent un « moment privilégié » pour les tentatives de fraude ; une plus grande attention peut être nécessaire.
- Redoublez de vigilance pour des ordres émanant de clients ayant signalé un incident (ex. vol de documents, de valeurs …).

[8] « Le recall de virement SEPA»
[9] Directive Services de paiement

Points d'attention particuliers

Les ordres de virements frauduleux sont parfois précédés et/ou suivis d'un appel téléphonique. Cela ne doit pas limiter la vigilance quant à l'ordre lui-même. En effet, l'escroc peut téléphoner en se faisant passer pour un employé de l'entreprise cliente pour se faire confirmer l'exécution de l'ordre. Dans ce cas, un contre-appel[10] est encore plus opportun.

Le cas où le nom du titulaire de compte bénéficiaire est identique à celui du donneur d'ordre (notamment si le compte est ouvert à l'étranger) mérite également une certaine vigilance.

- Tout changement de coordonnées téléphoniques ou géographiques est une opération méritant une attention spécifique. Une entreprise change très rarement ses coordonnées en la matière, sauf délocalisation ou autre raison spécifique.

Une demande de changement de coordonnées peut être réalisée préalablement à la tentative de virement frauduleux. Dans cette situation, le contre-appel vers un autre numéro de téléphone (présent dans le dossier client) ou à partir des pages jaunes (annuaire) peut se révéler nécessaire.

- Les numéros de téléphone affichés ne garantissent pas l'origine de l'appel. Soyez attentifs si un client passe à titre exceptionnel un ordre par téléphone.
- Concernant les quelques cas de virement papier encore existants, le fait de recevoir un ordre de virement avec un relevé d'identité bancaire agrafé à celui-ci n'est pas une garantie.
- Renforcer la vigilance lorsque l'opération présente un caractère inhabituel (remise au guichet exceptionnelle, par une personne inconnue, réception d'un ordre via un télécopieur, dans la boîte à lettres du point de vente…)

Encouragez vos clients à

- Privilégier les émissions de virements automatisés/électroniques (ex : virements permanents, virements transmis par le biais d'outils de banque à distance, etc.) ; s'orienter vers un système de contrôle des ordres proposé par la banque, basé sur des mécanismes d'authentification du donneur d'ordre…

Se reporter à la plaquette « Identifiants bancaires Être vigilant, c'est important »[11] Extraits concernant le virement : « Ne confiez vos coordonnées bancaires à personne, sauf à un créancier devant effectuer un prélèvement sur votre compte….. » « …une personne devant vous régler par virement. Assurez-vous que cette personne est légitime et de bonne foi.»

- Faire part au plus tôt à leur(s) interlocuteur(s) habituel(s) au sein de la banque de tout changement d'habilitations sur leurs comptes.
- Sensibiliser leurs équipes en charge des paiements et désigner l'interlocuteur interne habilité à répondre aux interrogations en cas de doute.

Conseiller la mise en place d'une procédure au sein de l'Entreprise concernant le changement de coordonnées bancaire.

---

[10] Un contre-appel téléphonique est un échange **à l'initiative exclusive de l'établissement** (et non du client) ; (utiliser les coordonnées téléphoniques présentes au dossier client).

[11] https://www.banque-france.fr/fileadmin/user_upload/banque_de_france/Stabilite_financiere/Identifiants-bancaires-depliant.pdf

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LE CHEQUE

1. PRESENTATION DU MOYEN DE PAIEMENT

DEFINITIONS

Le chèque est un Moyen de paiement, présenté sous forme de carnet de chèques, avec lequel le titulaire (tireur) d'un compte donne l'ordre à son banquier (tiré) de payer à vue au bénéficiaire du chèque une certaine somme inscrite sur celui-ci. La provision doit toujours être disponible lors de l'émission du chèque et maintenue jusqu'à sa présentation (par la banque du bénéficiaire à la banque du tireur).

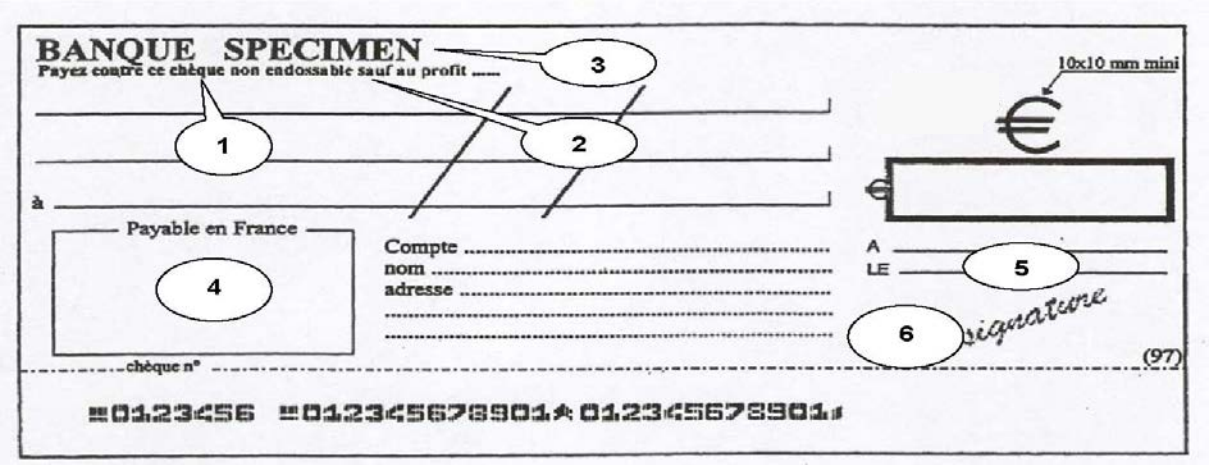
LA NORME

La norme NF K11-111 – Formules de chèques payables en France a été établie pour rationaliser les traitements du chèque en France. L'arrêté du 5 novembre 1998, du Ministère de l'Economie, des Finances et de l'Industrie, portant homologation et mise en application obligatoire de normes françaises a rendu obligatoire l'application de cette norme, Ainsi, en établissant un standard d'usage aujourd'hui généralisé en France et reconnu par l'ensemble du public, cette norme est devenue un élément de base de la sécurité du chèque. La lutte contre la fraude sur le chèque s'appuie sur cet usage généralisé de la norme NF K11-111 de la formule de chèque.
Une autre norme, la NF K11 112 concernant « la production de formules de chèques normalisées selon la norme NF K 11-111 », définit les règles de fabrication des formules de chèques normalisées et personnalisées, depuis la prise de la commande jusqu'à la livraison au destinataire final.

LES MENTIONS OBLIGATOIRES DU CHEQUE (art.L131-2 du Code Monétaire et Financier)

1 La dénomination de chèque, insérée dans le texte même du titre et exprimée dans la langue employée pour la rédaction de ce titre ;
2 le mandat pur et simple de payer une somme déterminée ;
3 le nom de celui qui doit payer, nommé le tiré ;
4 l'indication du lieu où le paiement doit s'effectuer ;
5 l'indication de la date et du lieu où le chèque est créé ;
6 la signature de celui qui émet le chèque, nommé le tireur.

Exemple indicatif de formule de chèque non endossable et prébarrée.



N.B. : le symbole € situé au-dessus du cadre montant en chiffres n'est pas apposé systématiquement du fait qu'il est devenu facultatif avec la fin légale du franc français.

LA LIGNE MAGNETIQUE DU CHÈQUE

Toute formule de chèque normalisée comporte une partie magnétique dite ligne "CMC7" (ensemble de caractères magnétiques servant à son traitement).

LA VALIDITÉ DU CHÈQUE

Les chèques bancaires émis et payables en France métropolitaine ont une validité de UN AN et HUIT JOURS à compter de leur date d'émission[1].
Un chèque non daté ne vaut pas comme chèque.

UN CHÈQUE SPECIFIQUE : LE CHÈQUE DE BANQUE

Rappel de définition extraite de la communication CFONB n° 2008 233 du 28 juillet 2008.

" Le chèque de Banque est un chèque délivré par un banquier, à la demande d'un client, contre paiement immédiat par débit en compte, ou versement d'espèces. Cette délivrance doit être réalisée dans les conditions de vigilance et de précaution renforcées portant notamment sur la connaissance du client dans le cadre de la lutte contre le blanchiment de l'argent.

Ce chèque a pour effet de garantir au bénéficiaire l'existence de la provision pendant le délai légal de prescription du chèque qui est de 1 an et 8 jours après sa date d'émission [1][2] .Le chèque de banque peut être barré non endossable ou non barré endossable (soumis au droit de timbre).

En juillet 2009, un renforcement de la sécurité sur la formule du chèque de banque a été décidé en France. Ainsi, tous les chèques de banque fournis à la clientèle sont désormais dotés d'un filigrane normalisé, identique en motif et en taille pour l'ensemble des banques opérant en France.

Le filigrane choisi présente un haut niveau de protection : le motif est intégré au papier, et non pas imprimé sur celui-ci, afin d'éviter les contrefaçons. Le filigrane est facile à reconnaître à l'œil nu par transparence. Il couvre une partie importante de la surface du chèque. Il comporte la mention « CHEQUE de BANQUE », lisible au dos du chèque. Cette mention est bordée en haut et en bas par deux flammes rayées et, de part et d'autre, par deux semeuses dont les parties claires et sombres du dessin de l'une sont inversées par rapport à celles de l'autre (voir plaquette de communication établie par la Banque de France page ci-après).

---

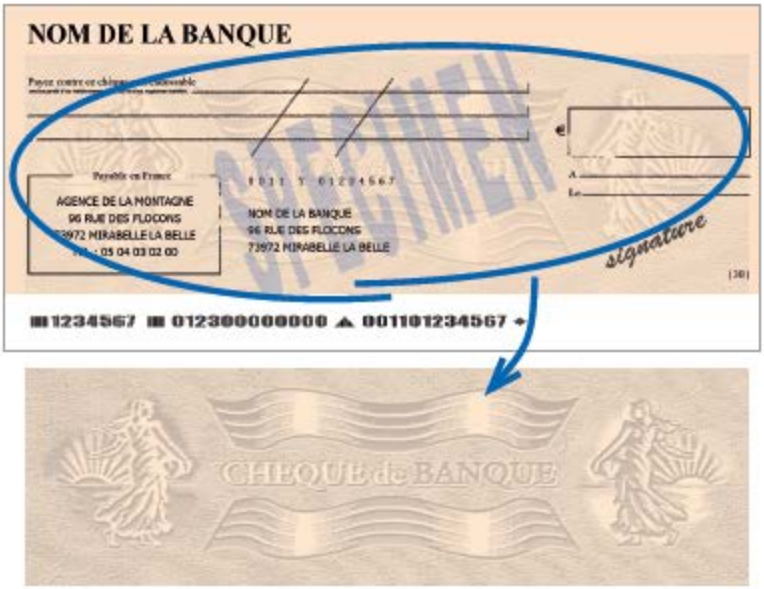
[1] Article L 131.32 du Code Monétaire et Financier

« Le chèque émis et payable dans la France métropolitaine doit être présenté au paiement dans le délai de huit jours.
Le chèque émis hors de la France métropolitaine et payable dans la France métropolitaine doit être présenté dans un délai, soit de 20 jours, soit de 70 jours, selon que le lieu de l'émission se trouve situé en Europe ou hors d'Europe. Pour l'application de l'alinéa précédent, les chèques émis dans un pays riverain de la Méditerranée sont considérés comme émis en Europe.
Le point de départ des délais indiqués au deuxième alinéa est le jour porté sur le chèque comme date d'émission.»

PLAQUETTE DE COMMUNICATION

CHÈQUE DE BANQUE
AYEZ LE BON RÉFLEXE !

Vérifiez le filigrane
visible par transparence et lisible au verso



Le filigrane est identique pour toutes les banques. Il comporte la mention CHEQUE de BANQUE lisible sur le verso du chèque. Le texte est encadré de deux semeuses dont les parties claires et sombres de l'une sont inversées par rapport à celles de l'autre.

Le paiement par chèque de banque est parfois exigé par le vendeur lors d'une transaction de montant élevé (ex : véhicule, bien immobilier, œuvre d'art), pour se prémunir contre le risque d'absence de provision. Le chèque de banque obtenu par l'acheteur auprès de sa banque a la particularité d'être débité sur le compte de la banque et non sur celui de l'acheteur, la banque ayant préalablement retiré la provision nécessaire du compte de celui-ci.

BANQUE DE FRANCE
EUROSYSTÈME

2. TYPES D'ATTAQUES

DÉFINITION LA CONTREFAÇON DU CHÈQUE (OU FAUX CHÈQUE[13])

Toute formule non mise en circulation par un établissement habilité à être tiré de chèque et dont les caractéristiques interdisent en tout état de cause la bonne fin de l'opération clientèle.

Sans préjuger des nombreux cas de figure possibles, ni des multiples procédés de contrefaçon liés à l'évolution des technologies, deux types de contrefaçons sont observés :

- Création d'un faux de toutes pièces : formule tirée sur un établissement existant, imaginaire ou ayant cessé son activité ;
- Reproduction à partir d'un modèle existant : par photocopie couleur ou numérisation d'un vrai chèque, notamment reproduction de la signature, formule issue d'un procédé informatique (montage à partir d'éléments issus de plusieurs formules).

La ligne magnétique CMC7 du chèque contrefait peut indifféremment être non cohérente, partiellement cohérente et magnétique, totalement cohérente et magnétique, absente, non magnétique, … .

Observation : Le Fichier National des Chèques Irréguliers (FNCI)[14] recense les éléments d'identification des faux chèques. Les modalités de déclaration ont été rappelées dans la communication CFONB 2014 0015 du 3 avril 2014.

DEFINITION CHÈQUE FAUX (OU CHÈQUE APOCRYPHE[8])

Chèque perdu ou volé (formule en blanc), revêtu d'une fausse signature n'émanant ni du titulaire du compte, ni de son mandataire.

DEFINITION CHÈQUE FALSIFIÉ

Altération volontaire d'un chèque régulièrement émis destinée à tromper (atteinte au libellé initial).

La falsification peut porter sur :

- le nom du bénéficiaire, et/ou
- le montant, et/ou
- la ligne magnétique, notamment la zone correspondant au numéro de chèque.

Elle est apparente (rature, surcharge, gommage, grattage, lavage, …) ou non.

La formule du chèque est correcte, tout comme la signature du client.

Des falsifications en matière de lettres-chèques sont observées en particulier lorsque les recommandations relatives à la rédaction de la partie formule de chèque ne sont pas appliquées : montant non repris en toutes lettres, absence d'astérisques pour borner les zones "montant en chiffres", "montant en lettres", "bénéficiaire", impression des éléments concernant les montants et le nom du bénéficiaire en écriture blanche sur fond noir,….

[13] Terminologie utilisée dans certains établissements
[14] En application des articles 1 et 2 de l'arrêté du 4 juillet 1992

DEFINITION CHÈQUE DÉTOURNÉ

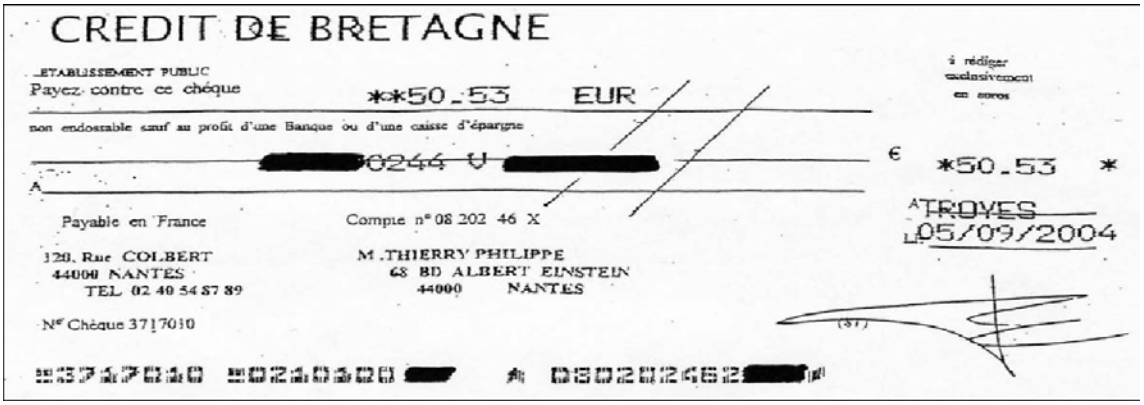
Il s'agit d'un chèque régulièrement émis par le tiré, perdu ou volé lors de son acheminement vers le bénéficiaire par exemple. La formule du chèque est correcte, la ligne CMC7 est valide tout comme la signature du client. Le chèque ne porte aucune altération et, la fraude est, de ce fait, impossible à déceler.

Les détournements (dénommés également sous le terme de « rejeu ») sont le fait de tiers, parfois même il s'agit d'un employé d'une société cliente.

Exemples concrets

LA CONTREFAÇON DU CHEQUE (OU FAUX CHEQUE)

Exemple Chèque émis sur une banque imaginaire


CREDIT DE BRETAGNE

ETABLISSEMENT PUBLIC

Payez contre ce chèque **50.53 EUR

non endossable sauf au profit d'une Banque ou d'une caisse d'épargne

0244 U

€ *50.53 *

TROYES le 05/09/2004

Payable en France

Compte n° 08 202 46 X

120, Rue COLBERT
44000 NANTES
TEL 02 40 54 87 89

M. THIERRY PHILIPPE
68 BD ALBERT EINSTEIN
44000 NANTES

N° Chèque 3717010

QUELQUES ZOOMS SUR DES CAS DE CONTREFACON (OU FAUX CHEQUE)

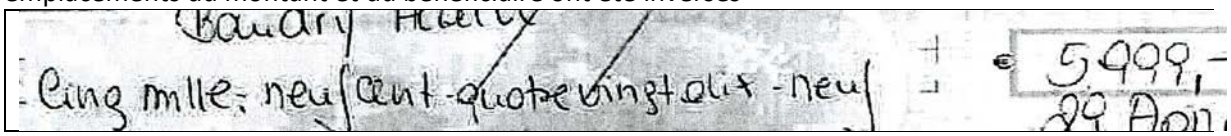
Une contrefaçon particulière a été observée :

- la ligne CMC7 était valide, tout comme la clé RLMC.
- Le numéro de compte inscrit dans la zone « paiement » du chèque (qui comporte également les noms-adresse du titulaire du compte) pouvait être sans rapport avec le contenu de la ligne CMC7.
- Très souvent, les adresses figurant sur la formule (titulaire du compte – agence) et le lieu de l'achat étaient localisés dans le même secteur géographique
- Les pièces d'identité présentées lors de la remise du faux chèque étaient véritables et valides.

Ce type d'escroqueries s'appuie en principe sur un réseau pyramidal, avec par exemple, un faussaire, des « rabatteurs », des « acheteurs » (des mules) ayant déclaré au préalable auprès des Autorités la perte ou le vol de leur pièce d'identité...

Exemple 2 :

La formule a été imaginée en utilisant le logo et le fond de chèque réel de la banque, à noter que les emplacements du montant et du bénéficiaire ont été inversés


Cinq mille neuf cent quatre vingt dix neuf

€ 5999,-

EXEMPLES D'UTILISATION

- dans les commerces de proximité non équipés de matériel d'interrogation au fichier VERIFIANCE notamment ;
- dans les transactions entre particuliers.

Utilisation de faux chèques de banque

Ce moyen de paiement est particulièrement prisé par les escrocs puisqu'il permet de réaliser des opérations sur des montants élevés tout en inspirant une certaine confiance chez la victime à qui l'on propose un paiement présumé garanti. Il peut être utilisé dans les transactions entre particuliers (achat de véhicule notamment).

L'attention des clients est à attirer sur les risques encourus en acceptant un règlement par chèque de banque sans consulter préalablement la banque émettrice. Plus particulièrement, en cas d'achat d'un véhicule par chèque de banque, qui est l'escroquerie la plus courante, il est conseillé aux clients d'appeler l'établissement bancaire tiré (rechercher le n° dans l'annuaire, ne pas se fier à celui inscrit sur le chèque) et, si c'est un week-end, d'attendre l'ouverture de l'établissement pour concrétiser la transaction.

CHEQUE FAUX (ou CHEQUE APOCRYPHE)[15]

EXEMPLES D'UTILISATION

- auprès des commerçants,
- auprès des banques. Citons par exemple :
  - les retraits déplacés ;
  - l'ouverture de compte avec remise de chèque faux et retrait des fonds dans un délai très court ;
  - l'utilisation du chéquier de son entreprise par un employé indélicat : soit par retrait d'espèces, soit par remise de chèques sur son compte.

ZONES DE RISQUES DE VOL DU CHEQUIER, VOIRE DE QUELQUES FORMULES DE CHÈQUES EN BLANC

- En amont de la délivrance au client :
  - dans les circuits d'acheminement,
  - lors des transports des chéquiers du façonnier vers les agences bancaires,
  - dans les boîtes à lettres des clients.

- Lors de la remise au guichet sur présentation de pièces d'identité volées ou falsifiées.

- Après remise du chéquier au client.

CHEQUE FALSIFIE

EXEMPLES D'UTILISATION

Cette façon de procéder est fréquemment associée à une ouverture de compte frauduleuse. L'utilisation de compte de tiers, complices ou non, pour l'encaissement des chèques falsifiés se développe. Les fraudeurs « jouent » sur les délais d'encaissement et réalisent des retraits avant le retour impayé des chèques.

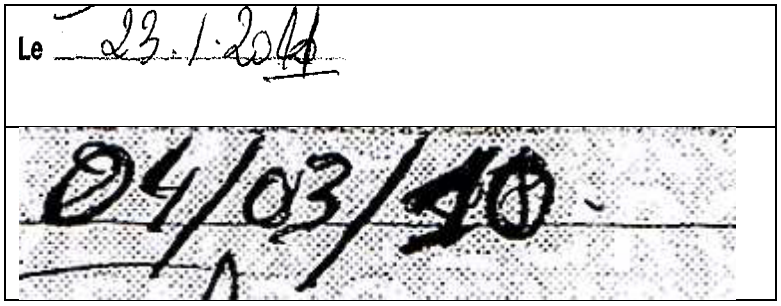
[15] Terminologie utilisée dans certains établissements

ZONES DE RISQUES DE VOLS

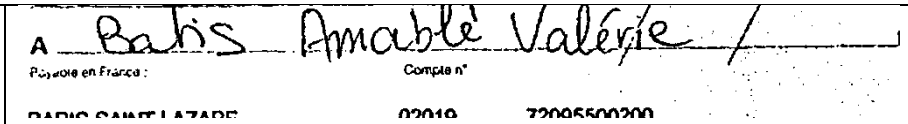
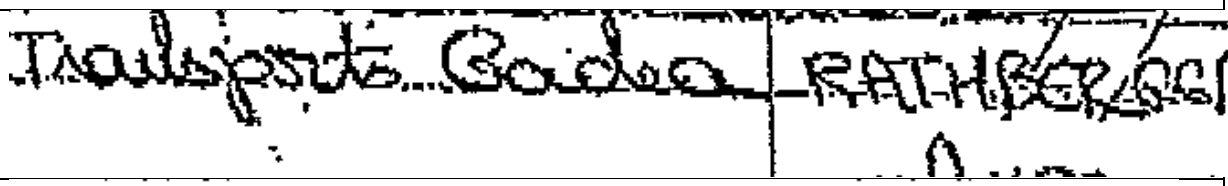
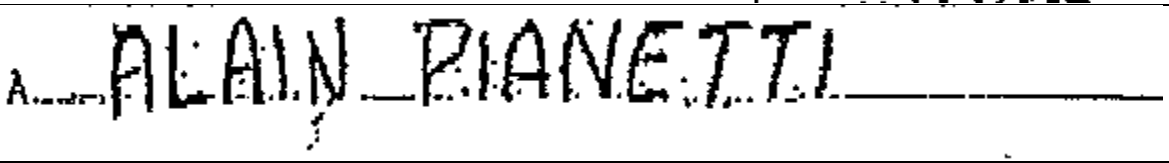
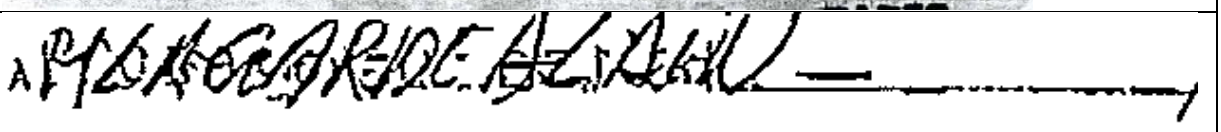
Les fraudeurs collectent les chèques émis dans les circuits d'acheminement (circuits du courrier, …), jusque dans les boîtes à lettres.

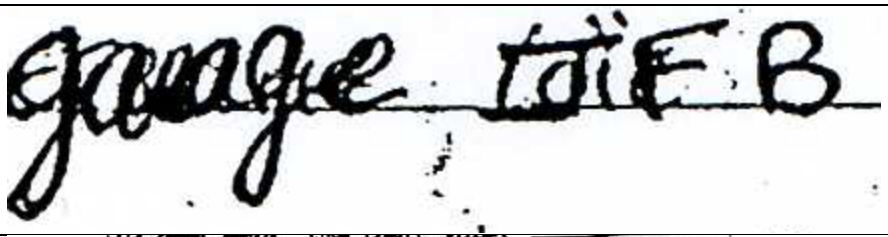
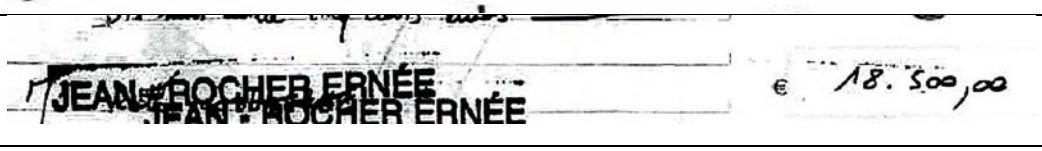
QUELQUES ZOOMS SUR DES FALSIFICATIONS

Modification de date :

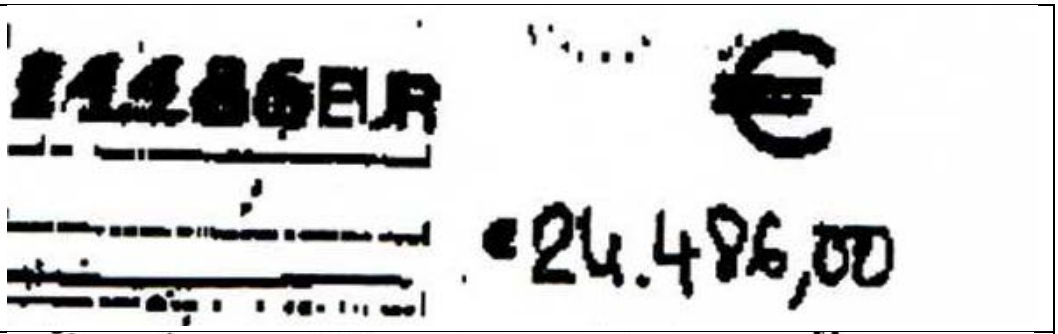
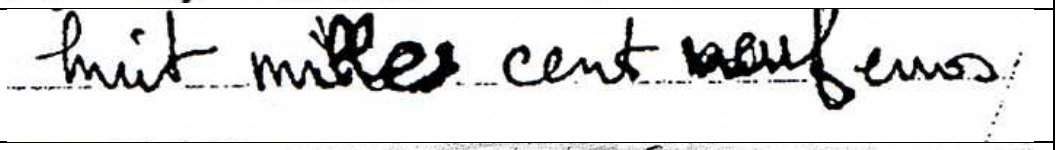
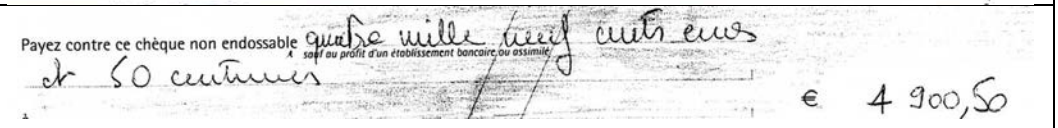


Modification du nom du bénéficiaire :

Ajout du nom (AMABLE Valérie)	
Ajout du nom (RATHBERG ….)	
Après grattage	
Après grattage	
Réécriture d'un nom de bénéficiaire sur le premier nom	

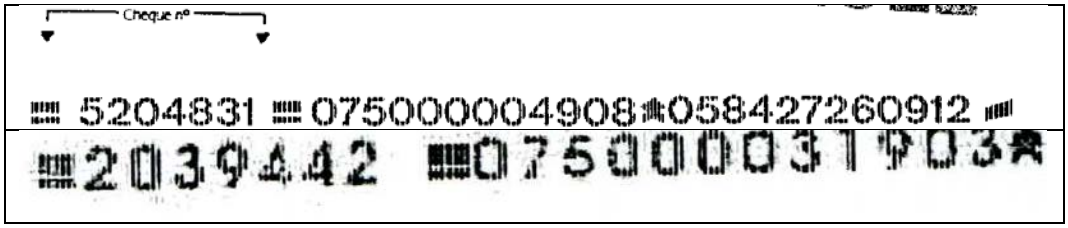
Réécriture d'un nom de bénéficiaire sur le premier nom	
Tampons insérés sur le nom du bénéficiaire	

Modification des montants :

Les deux montants ont été changés, y compris celui indiqué à l'origine à la machine Todd	
Deux cent deux euros à l'origine	
Mille neuf cent euros et 50 centimes à l'origine	

Ligne magnétique :

Les caractères magnétiques peuvent ne pas correspondre aux caractères magnétiques normalisés repris sur les chèques tirés sur la France



CHEQUE DETOURNE

Lors de l'encaissement, le paiement du chèque n'est pas effectué au porteur légitime. Cette pratique est également souvent associée à une ouverture de compte frauduleuse (souvent associée à des pièces d'identité contrefaites ou falsifiées) ou par utilisation d'un compte existant sans mouvement (dénommé également "dormant") ou très peu connu du conseiller de clientèle.

3. MESURES PREVENTIVES

La première des mesures préventives concerne la connaissance du client : il faut tenir compte de ses habitudes. Son activité mène à une récurrence des opérations (bénéficiaires, montants, ….). Un changement brusque doit éveiller l'attention du teneur de compte.

AVANT DE DELIVRER UN CHEQUIER

Les conditions de délivrance des chéquiers peuvent mettre en jeu la responsabilité du banquier, aussi un contrôle très strict est-il nécessaire, notamment lors de la remise de chéquier à de nouveaux clients (interrogation du Fichier Central des Chèques de la Banque de France, vérifications liées à l'ouverture du compte).

De même, toutes les demandes de renouvellement de chéquiers formulées par la clientèle doivent faire l'objet d'un contrôle préalable (vérification signature, absence d'une surveillance du compte – INJ, INB[16] ou surveillance interne-).

Enfin, la banque a la faculté de réclamer à tout moment la restitution des formules antérieurement délivrées. Elle est, en outre, tenue de le faire lorsqu'elle constate un incident de paiement ou en cas de clôture de compte.

Lorsque les carnets sont mis à disposition des clients, des précautions particulières sont nécessaires, notamment en ce qui concerne les modalités selon lesquelles ces carnets sont retirés :

- la délivrance au guichet contre reçu signé par un titulaire ou par un mandataire habilité (vérification de l'identité, de la signature et des pouvoirs le cas échéant) ;
- ou l'expédition par pli de type recommandé (ou tout autre mode d'envoi dans lequel la délivrance du chéquier se fait contre signature du client) sauf décision expresse du titulaire du compte qui, dans ce cas, serait sensibilisé à la responsabilité qu'il encourt avec un envoi par courrier simple. Ne pas hésiter à se reporter aux règles internes en la matière !

LES VERIFICATIONS LORS DE LA REMISE A L'ENCAISSEMENT DES CHEQUES

Ces vérifications concernent la présence effective des mentions obligatoires (cf. partie Définitions), notamment, la signature du tireur au recto et celle de l'endos (signature du bénéficiaire ou de son mandataire) au verso.

Reportez-vous aux instructions de votre Etablissement en la matière.

LES RECOMMANDATIONS AUX EMETTEURS ET AUX BENEFICIAIRES DE CHÈQUES

Dans le cadre de la relation commerciale, un certain nombre de conseils peuvent aider le client à se protéger contre les risques de fraude sur les chèques détenus ou émis.

La communication adhérents CFONB n° 2012 070 du 02 avril 2012[17] est un outil à disposition des établissements pour leurs besoins de communication à destination de leur clientèle de particuliers et

[16] Interdit Judiciaire – Interdit Bancaire
[17] Recommandations sur l'utilisation et la rédaction de chèques

de professionnels, qu'ils soient émetteurs ou bénéficiaires de chèques.
De même, un mini-guide LES CLES DE LA BANQUE spécifique au chèque a été édité.[18]

EN CAS DE PERTE OU DE VOL DE FORMULES SIGNALE PAR UN CLIENT, EN CAS D'UTILISATION FRAUDULEUSE, DE DECISION DE JUSTICE AU TITRE D'UNE PROCEDURE COLLECTIVE DU PORTEUR.

Enregistrement immédiat des demandes d'opposition formulées par les clients.

En cas d'impossibilité pour joindre la banque, les clients peuvent également déclarer la perte ou le vol de chèques auprès du Centre National d'Appels Chèques Perdus ou Volés, service de la Banque de France ouvert 7j/7 et 24h/24 au 08.92.68.32.08. Cette déclaration doit impérativement être confirmée au plus tôt par une opposition auprès de l'agence.

EN CAS DE CLOTURE DE COMPTE

Enregistrement dans les meilleurs délais dans le système d'information de l'établissement.

Les coordonnées bancaires des comptes clôturés tirés de chèques et des comptes pour lesquels une déclaration pour perte ou vol a été enregistrée notamment, alimentent de façon permanente le Fichier National des Chèques Irréguliers (FNCI) de la Banque de France que les commerçants ont la possibilité de consulter sous certaines conditions.

ATTENTION *au risque de faux chèque*

Aspect du chèque

Si le chèque présente :

UNE APPARENCE INHABITUELLE :

- épaisseur du papier, papier parfois glacé,
- côtés du chèque lisses,
- fond de chèque différent de celui du banquier tiré,
- logo erroné, couleur du chèque inhabituelle.

DES MENTIONS INCOHERENTES :

- numéro de compte non indiqué au-dessus du nom du client, numéro de téléphone agence indiqué souvent erroné ; il correspond, par exemple, à un numéro de portable …

Il n'est pas évident pour une banque, quelle qu'elle soit, de connaître tous les modèles de chèques qui peuvent être tirés sur environ 600 organismes financiers existant en France.
En cas de doute, seul un contact avec le confrère émetteur permettra de se faire confirmer la validité du chèque.

ATTENTION AU RISQUE DE CHEQUE FALSIFIE

Si le chèque présente : DES RATURES, DES SURCHARGES, DES TRACES DE GOMMAGE OU DE GRATTAGE, DE DECOLORATION DE FOND DE CHEQUE, DES TACHES, DES TRACES DE LAVAGE, notamment sur les mentions sensibles telles que le BENEFICIAIRE, le MONTANT, la ZONE NUMERO DE CHEQUE DE LA LIGNE MAGNETIQUE.

[18] www.lesclesdelabanque.com

En cas de doute, ne pas hésiter à vérifier auprès de la banque tirée la régularité de la vignette en s'inquiétant plus particulièrement de l'exactitude du montant et du nom du bénéficiaire.

ATTENTION AU RISQUE DE CHEQUE DETOURNE

Il s'agit essentiellement d'appliquer les précautions habituelles.
Cohérence entre le nom du bénéficiaire du chèque et le nom du titulaire du compte sur lequel le chèque est déposé.

Signalons qu'il est rare que des entreprises émettent des chèques de plusieurs centaines de milliers d'euros en faveur de particuliers.
Il convient de prêter une attention particulière aux comptes de non-résidents, aux comptes récemment ouverts ainsi qu'aux comptes présentant peu de mouvements.

ATTENTION AU RISQUE D'OUVERTURE DE COMPTE FRAUDULEUSE

- Incohérence entre l'activité déclarée du titulaire du compte et le montant de la remise de chèque.
- S'agissant d'un mode opératoire très courant, toute demande de retrait de fonds correspondant à tout ou partie du montant d'une remise de chèque réalisée peu de temps auparavant sur un compte peu connu ou récemment ouvert, doit éveiller l'attention et pousser l'agence à vérifier auprès du banquier tiré le bien-fondé de l'opération.

Il convient, lorsqu'il y a présomption de faux, d'avertir sans délai sa hiérarchie et les services compétents (Contrôle Permanent, Audit, Services Fraude, etc…).

CAS PARTICULIER

LE CAS PARTICULIER DU RETRAIT DÉPLACÉ[19]

Certaines possibilités de retrait par chèque hors agence domiciliataire peuvent permettre dans certains cas aux fraudeurs de dépasser les plafonds hebdomadaires autorisés.
Exemple d'utilisation : le fraudeur dispose d'une fausse pièce d'identité ou de document falsifié. Il falsifie les grilles de retrait ou réalise une contrefaçon de la grille. A noter que rarement des fausses griffes à date sont apposées.

LES PRECAUTIONS

- porter une attention toute particulière à ces opérations, notamment celles de montant important ;
- vérifier les papiers d'identité de manière attentive ;
- examiner soigneusement l'aspect général du chéquier (souche – feuillet spécial) ;
- respecter les procédures internes spécifiques à ces opérations (ex : examen des grilles pour les établissements concernés, avec notamment le montant des opérations déjà réalisées …).

[19] Service existant dans certains établissements

CHEQUES ETRANGERS

DEFINITION

Sont visés dans ce guide les chèques étrangers « export », c'est à dire remis pour encaissement en France et payables à l'étranger en euros ou en devises. Contrairement aux chèques français, ils ne répondent pas nécessairement à la norme NF K11-111.

La fraude sur les chèques étrangers ne se différencie pas de celle sur les chèques en euros payables en France pour ce qui concerne les types d'escroqueries rencontrées. Ainsi, on observe des cas de chèques étrangers faux, falsifiés, contrefaits et détournés.

En revanche les spécificités du traitement de ces chèques, en particulier les circuits utilisés, nécessitent une très grande vigilance lors de l'acceptation de ces valeurs et lors de leur acheminement vers la banque tirée. A ce titre et de façon générale, deux modes de paiement peuvent être utilisés : le « sauf bonne fin » et le « crédit après encaissement » :

- **Sauf Bonne Fin** (SBF) : il s'agit d'un crédit client immédiat avec la possibilité pour la banque de revenir sur l'écriture en cas de rejet et ce quel que soit le motif et le solde du compte. En fonction des pratiques locales, les délais peuvent être très variables d'un pays à un autre, voire même parfois sans délai maximum d'impayé(s).
- **Crédit Après Encaissement** (CAE) : crédit client ferme, effectué après le débit du chèque chez le correspondant étranger. Le client bénéficiaire est crédité de façon irrévocable après réception des fonds du correspondant, sauf quelques cas exceptionnels de fraude.

MESURES PREVENTIVES

- **Connaître le client**
  - La connaissance du client au travers de ses habitudes reste fondamentale pour détecter des tentatives de fraude.
  - Vérifications lors de la remise à l'encaissement de ces chèques.
  - Les rejets peuvent intervenir dans des délais plus ou moins longs selon les pays. Relevons qu'il n'existe pas de délai maximum d'impayé(s) sur certains états (exemple, les USA)...

Ainsi en cas de fraude signalée très tardivement par la banque tirée à la banque remettante, celle-ci risque d'être dans une situation délicate vis-à-vis de son client bénéficiaire.

- **Appliquer les précautions habituelles (cf. partie « chèques ») avec la plus grande vigilance notamment en termes d'aspect du chèque.**
- **Porter une attention toute particulière à la sécurisation de l'envoi de ces chèques vers l'étranger**
  - Acheminement du chèque vers la banque tirée. Pour être encaissé, ce chèque doit être adressé physiquement à la banque tirée qui est à l'étranger. En fonction des cas, ce moyen de paiement sera amené à transiter par plusieurs banques intermédiaires avant d'atteindre la banque tirée. Ces multiples acheminements comportent donc un risque fort de perte ou de vol des chèques.
  - En cas de doute, ne pas hésiter à solliciter les cellules spécialisées de votre établissement.
  - Dans toute la mesure du possible, incitez vos clients à solliciter un moyen de substitution pour leurs règlements en provenance de l'étranger.

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LE PRELEVEMENT SEPA

1. PRESENTATION DU MOYEN DE PAIEMENT

GENERALITES

Dans le cadre de l'harmonisation des paiements en euros au sein de la communauté européenne, deux instruments de prélèvement européens sont définis[20] :

- **Le prélèvement SEPA**[21] (SEPA Core Direct Debit ou SDD) : Il permet d'offrir à la clientèle un prélèvement ordinaire en euros. Ce prélèvement SEPA peut être utilisé par tout type de clientèle.
- **Le prélèvement SEPA interentreprises**[22] (SEPA Business-To-Business Direct Debit ou B2B), destiné aux « non-consommateurs » souhaitant régler tout ou partie de leurs créances selon des conditions particulières.

DEFINITION

Un prélèvement SEPA est un moyen de paiement automatisé utilisable pour payer des factures récurrentes ou ponctuelles. Il est plus particulièrement adapté aux paiements récurrents. Il permet à un créancier d'être à l'initiative de la mise en recouvrement de ses créances vis-à-vis d'un débiteur. Ce faisant, il dispense le débiteur de l'envoi d'un titre de paiement lors de chaque règlement ou échéance des opérations récurrentes.

Le prélèvement SEPA repose sur un mandat double, donné sur un formulaire unique par le débiteur à son créancier par lequel le débiteur autorise à la fois :

- Le créancier à émettre des ordres de prélèvement SEPA,
- Sa banque à débiter son compte du montant des ordres présentés.

Les données de ce formulaire de mandat sont formalisées dans un document intitulé « mandat de prélèvement SEPA ». Le formulaire de mandat complété et signé est l'expression du consentement du débiteur. L'absence de mandat (ou sa révocation ou sa caducité) signifie une absence de consentement.

Les mandats sont conservés sous la responsabilité du créancier. Ce dernier peut être amené à présenter un mandat en cas de demande de remboursement émanant de la personne débitée.

Le prélèvement SEPA est réalisé en euros ; il peut être émis de la France ou d'un autre pays de l'espace SEPA[23]. Les comptes impactés sont ouverts dans les livres des banques[24] situées dans ce périmètre. Le paiement doit respecter un certain nombre de caractéristiques techniques, en matière de format notamment.

---

[20] DIFFERENCES ESSENTIELLES entre le prélèvement SEPA Core et le prélèvement SEPA Interentreprises (cf. page 29 du présent document)

21 Brochure - Le Prélèvement SEPA – SEPA CORE Direct Debit - disponible sur le site Internet du CFONB (www.cfonb.fr) à la rubrique Espace documentaire > Instruments de paiement > Prélèvement

22 Brochure - Le Prélèvement SEPA Interentreprises – SEPA Business to Business Direct Debit - disponible sur le site Internet du CFONB (www.cfonb.fr) à la rubrique Espace documentaire > Instruments de paiement > Prélèvement

[23] Liste à jour des pays et des territoires de l'espace SEPA disponible sur le site de l'EPC (http://www.europeanpaymentscouncil.eu/)

[24] Le terme « banques » est utilisé au sens large « prestataires de services de paiement ».

De façon générale, il convient :

- Pour la banque du créancier, avant de mettre en place une « ligne » d'émission de prélèvement SEPA, de réaliser une analyse du dossier du client créancier puis d'en assurer le suivi.
- Pour la banque du débiteur, d'informer son client sur les modalités de fonctionnement de ce moyen de paiement.

ASPECTS PRINCIPAUX DU MOYEN DE PAIEMENT TANT LORS DE LA MISE EN PLACE ET LE SUIVI CHEZ LA BANQUE DU CREANCIER QUE CHEZ LA BANQUE DU DEBITEUR

BANQUE DU CREANCIER

La banque du créancier s'assure, selon ses critères d'appréciation, de l'aptitude de son client remettant à émettre des prélèvements SEPA.
La sécurité de ce moyen de paiement nécessite une grande vigilance de la part du banquier du créancier. Rappelons que les demandes de remboursement formulées par les débiteurs peuvent être formulées 13 mois après le paiement du prélèvement SEPA.

La banque doit se montrer prudente avant d'accepter un nouvel émetteur de prélèvements SEPA, que celui-ci dispose ou non d'un Identifiant Créancier SEPA (ICS).

➲ Les principes du KYC[25] sont applicables pour accorder ou refuser ce type de service.

Dès lors que la banque est d'accord pour que le client utilise ce moyen de paiement, elle doit lui faire part des règles de fonctionnement du prélèvement SEPA. De plus, un accord est formalisé sur la base, en particulier, des obligations à respecter pour pouvoir émettre cette catégorie d'opérations.

La banque du créancier assume l'entière responsabilité des prélèvements SEPA qu'elle présente au recouvrement. Elle s'assure donc du respect des règles par son client, y compris lors de leurs mises à jour.

➲ En cas de non-respect des règles professionnelles ou de manquements graves, il est possible à la banque du créancier d'aller jusqu'à interdire à ce dernier l'utilisation de ce moyen de paiement et de procéder à la radiation de l'ICS de celui-ci dans la base de données des Identifiants Créanciers SEPA tenue par la Banque de France.

BANQUE DU DEBITEUR

Les comptes des clients peuvent enregistrer des prélèvements SEPA émis depuis la France ou depuis n'importe quel autre pays de l'espace SEPA, par des créanciers français ou étrangers de l'espace SEPA.

➲ Les règles en vigueur prévoient le remboursement immédiat au débiteur d'une opération contestée. Concernant un SDD Core autorisé, le débiteur doit toutefois en formuler la demande auprès de sa banque dans un délai de 8 semaines maximum à compter de la date du débit de son compte.

➲ A l'expiration de ce délai de 8 semaines et dans les 13 mois maximum à compter de la date du débit du compte du débiteur, ce dernier ne peut contester que les opérations qu'il n'aurait pas autorisées. Dans ce cas, la banque du débiteur peut engager la procédure de recherche de preuve du consentement.

[25] Know Your Customer

A l'issue de cette procédure de recherche de preuve du consentement (copie du mandat par exemple), la demande effective de remboursement pourra être formulée auprès de la banque du créancier.

- La banque du débiteur a la possibilité de demander une copie des mandats, par exemple en cas de volumétrie inhabituelle rejets de SDD Core sur un créancier.

Le débiteur a le droit de donner des instructions à sa banque pour :

- bloquer tout prélèvement sur son compte
- bloquer tout prélèvement venant d'un ou plusieurs créanciers désignés (« black list »)
- autoriser seulement les prélèvements émis par un ou plusieurs créanciers désignés (« white list »)
- limiter le paiement des prélèvements à un certain montant et/ou une certaine périodicité, en fonction de l'offre de sa banque.

En général, ces services sont proposés par les établissements bancaires. La donnée de base utilisée dans le cadre de ces services est l'Identifiant SEPA du Créancier (ICS).

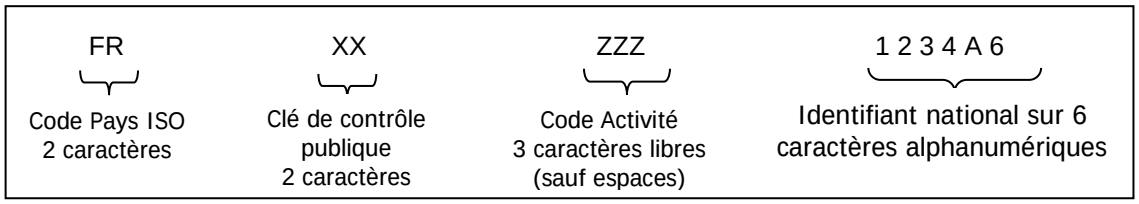
ATTENTION

La structure des ICS est propre à chaque pays. Il n'existe pas au niveau européen de base centralisée reprenant l'ensemble des ICS.[26]

En France, l'identifiant créancier SEPA délivré par la Banque de France est composé de 13 caractères. Il comprend les éléments suivants :

a) le code pays « FR » pour la France, « MC » pour la Principauté de Monaco, « NC » pour la Nouvelle Calédonie, « PF » pour la Polynésie Française et « WF » pour Wallis et Futuna.
b) une clé de contrôle calculée sur les éléments a) et d),
c) le code activité (« Creditor Business Code ») géré par le créancier à sa convenance, est obligatoirement renseigné; il ne doit pas comprendre d'espace,
d) l'Identifiant national sur 6 caractères alphanumériques (connu précédemment sous la terminologie NNE – Numéro National d'Emetteur sur 6 chiffres).

Représentation de la structure de l'identifiant créancier SEPA pour la France :



[26] Pour les créanciers étrangers, un contrôle de structure de l'ICS peut être réalisé. Il nécessite toutefois une interrogation au cas par cas auprès de l'Organisme en charge de l'enregistrement des ICS dans le pays concerné. Le site de l'EPC met à disposition une liste (document EPC262-08) reprenant la structure des identifiants créanciers SEPA et les points de contact pour les différentes communautés nationales de l'espace SEPA. https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC262-08%20Creditor%20Identifier%20Overview%20v4.0.pdf

DIFFERENCES ESSENTIELLES entre le prélèvement SEPA Core et le prélèvement SEPA Interentreprises

Afin de mieux appréhender les risques liés, le tableau ci-dessous restitue les différences essentielles entre les deux types de prélèvements SEPA CORE et Interentreprises.

	SDD Core	SDD B2B
Type de clientèle	Tous les acteurs économiques	Le débiteur est obligatoirement un « non-consommateur », c'est à dire que le débiteur est une personne morale, ou physique qui agit dans un cadre professionnel
Adhésion au service	Obligatoire pour les banques	Optionnel pour les banques
Données du mandat	La banque du débiteur ne dispose pas des données du mandat.	La banque du débiteur doit contrôler avant tout paiement la cohérence des données du mandat initial ou amendé et les instructions du débiteur avec les données de l'opération reçues de la banque du créancier. Ces données dûment confirmées ainsi que l'accord original du débiteur, sont conservées par la banque du débiteur avec les éventuelles instructions de paiement données par ce dernier (opposition, révocation…) ;
Délai de retour du paiement par la banque du débiteur (« return »)	5 jours ouvrés bancaires après la date de règlement.	3 jours ouvrés bancaires[27] après la date de règlement.
Droit à contestation du débiteur	Le débiteur peut via sa banque contester une transaction autorisée dans les 8 semaines qui suivent le débit.	En signant le mandat, le débiteur renonce à contester un prélèvement SEPA interentreprises autorisé.
Droit à contestation du débiteur pour absence de consentement	La banque du débiteur peut demander le remboursement dans les 13 mois à compter de la date de débit du compte du débiteur	Un prélèvement SEPA interentreprises contesté par un débiteur n'a pas lieu d'être remboursé par la banque du débiteur, dès lors qu'il s'agit d'une transaction autorisée. Un retour de fonds ne peut être exigé auprès de la banque du créancier. Toutefois, la banque du créancier est tenue d'étudier toutes les demandes présentées par la banque du débiteur suite à la contestation du débiteur pour opération non autorisée ou erronée (cf. procédure[28]).

Pour toute précision complémentaire,
n'hésitez pas à vous référer à la documentation CFONB !

[27] Au 20 novembre 2017 (précédemment le délai était de 2 jours ouvrés bancaires après la date de règlement)
[28] Cf. brochure CFONB « le prélèvement SEPA interentreprises » fiche 7

2. TYPES D'ATTAQUES

Le prélèvement SEPA a apporté une dimension européenne au prélèvement national. Le risque global de fraude apparaît amplifié par cet élargissement géographique.

Les principaux scénarios ci-dessous sont donnés à titre informatif et ne sont pas exhaustifs. Ils peuvent être issus d'usages ou de comportements émanant d'un créancier ou d'un débiteur :

- ***D'un créancier frauduleux***

Deux scénarios plus spécifiques sont repris *:*
Après avoir récupéré des IBAN, un fraudeur s'enregistre en tant qu'émetteur de SDD chez une banque afin d'envoyer un grand nombre de prélèvements sans mandat (ou avec des mandats qu'il aurait fabriqués lui-même) et ne reposant sur aucun contrat commercial avec le débiteur.

Des entreprises émettrices de prélèvements (déjà titulaires d'un ICS) ont été rachetées. La situation vis-à-vis de leur(s) banque(s) apparaît « dormante » sur une certaine période. Des prélèvements en masse sont émis et, quelques semaines plus tard, les sociétés sont déclarées en « faillite ».

- ***D'un créancier avec un mandat légitime***

Un fraudeur s'enregistre en tant que nouveau client comme un créancier chez une banque. Il obtient de manière légitime des mandats de la part de débiteurs et émet des premiers encaissements non frauduleux.
Puis, au bout de quelque temps, il envoie des prélèvements non causés par une vente de bien ou de service, de montants importants ou non. Le fraudeur transfère l'argent ainsi récupéré vers des comptes à l'étranger et disparaît.
Cette attaque peut être également réalisée par un créancier de longue date.

- ***D'un créancier qui fait de la cavalerie***

Un créancier, dans une situation financière fragile peut, afin de se faire de la trésorerie, envoyer un grand nombre de SDD vers des IBAN qu'il connaît. Voir partie « cavalerie » sur le prélèvement du présent guide

Certaines attaques peuvent trouver leur origine à partir d'un débiteur mal intentionné avec des pratiques liées à :

- ***Une compromission d'IBAN***

Un fraudeur vole (ou achète) une liste d'IBAN. Il se présente chez plusieurs créanciers et communique ces IBAN volés à la place de son IBAN lors de la création du mandat.

- ***une utilisation de faux IBAN dans un mandat***

Un fraudeur, lors de la création de son mandat, communique à son créancier un faux IBAN qui n'est lié à aucun compte ou qui appartient à une personne étrangère à la transaction.

- ***une contestation abusive***

Un débiteur conteste pendant le délai de 13 mois de manière non justifiée un prélèvement sous prétexte qu'il n'a pas signé de mandat.

EXEMPLES CONCRETS

- Des détournements de coordonnées bancaires ont permis la présentation de prélèvements SEPA. Le débiteur fraudeur a indiqué les coordonnées d'un tiers sur le mandat lors de la souscription du service, bénéficiant ainsi de biens sans avoir à en honorer les règlements prévus.

- Une société en activité dans le secteur informatique depuis plusieurs années, titulaire d'un compte dans un établissement A ouvre un compte dans un établissement B et demande rapidement un numéro ICS. A la suite de quoi, des prélèvements SEPA sont émis sur différents comptes dont celui d'un complice du créancier. Dès réception des fonds sur le compte ouvert dans l'établissement A, la société procède au transfert de ces fonds sur le compte ouvert dans l'établissement B. Au moment des rejets des prélèvements, le solde du compte du créancier ne permet plus le remboursement des opérations contestées. Sa banque subit donc une perte.
  Le cas peut se produire avec ou sans complicité.

- Un créancier mal intentionné :

  - a émis des prélèvements SEPA sur des comptes de tiers sans avoir obtenu des mandats. A partir des fonds reçus, il a tenté d'émettre un virement vers un pays étranger. Cette démarche inhabituelle pour cette relation a alerté la banque teneur de compte qui est intervenue afin d'éviter la poursuite des opérations.

  - va jouer sur la position de son compte jusqu'au terme du délai légal de rejet (soit 13 mois maximum après le débit en compte). Dès lors, les complices procèderont aux rejets de l'ensemble des prélèvements reçus sur ladite période. Voir également partie « Cavalerie » du présent guide.

NB : Certains scénarios décrits dans le paragraphe ci-dessus sont transposables aussi bien en prélèvement SEPA Core qu'en B2B.

3. MESURES PREVENTIVES

Rappel : en cas de suspicion, la réactivité des banques tant du créancier que des débiteurs peut permettre de limiter la portée des attaques.

CREANCIER

Une utilisation judicieuse de l'IDENTIFIANT CREANCIER SEPA (ICS), peut permettre une meilleure identification des flux pour le créancier.

Principales consignes à respecter par le créancier :

- recueillir les mandats signés des débiteurs, les conserver afin de pouvoir en fournir la preuve physique à tout moment sur sollicitation ainsi que celle concernant tous les amendements liés aux mandats,
- indiquer dans le libellé du fichier transmis à son banquier : sa dénomination sociale, les éléments concernant le produit ou le service vendu, la RUM (Référence Unique du Mandat), les références End to End…
- informer préalablement (au minimum 14 jours calendaires) les débiteurs avant l'exécution du prélèvement SEPA (ce au moyen d'une facture, d'un avis, d'un échéancier, etc…),
- mettre à disposition des débiteurs des coordonnées d'un point de contact disponible pour les consommateurs afin de modifier, de révoquer le mandat de prélèvement, obtenir des précisions,
- utilisation de toute solution permettant un contrôle des coordonnées numéro de compte/nom
- etc…

BANQUE DU CREANCIER

Les mesures préventives concernent essentiellement la CONNAISSANCE DU CLIENT CREANCIER[29] au travers de ses habitudes. Une identification poussée du créancier lors de sa souscription au service ainsi qu'une revue régulière des clients concernés peut être réalisée par la banque afin de détecter ou décourager les créanciers qui pourraient être indélicats.

Ainsi, de simples questions peuvent permettre de détecter une fraude

➲ Les modalités de présentation des prélèvements SEPA correspondent-elles aux habitudes du créancier pour le prélèvement ? L'opération est-elle en lien avec son activité (description, chiffres d'affaires, plan de développement commercial, secteur d'activité, KYC, locaux…) ? Est-elle conforme aux procédures habituellement utilisées par le créancier et portées à la connaissance de la banque ?

- L'objet du règlement : le libellé indiqué sur l'ordre correspond-il aux affaires traitées par le créancier ? S'agit-il d'un objet bien déterminé pour éviter tout risque de fraude ?
- Le pays de destination des prélèvements : le créancier est-il en relation d'affaires avec un pays autre que la France ? Avec les consommateurs de ce/ces pays plus spécifiquement ?

[29] KYC « Know Your Custumer »

- Le montant de l'opération : les ordres correspondent-ils au courant d'affaires habituel de ce créancier ?
- Le créancier aura-t-il la capacité financière suffisante pour rembourser totalement ou partiellement les prélèvements contestés 13 mois après leur date d'émission ? S'interroger face à toute situation spécifique, notamment en cas de décisions judiciaires.

➲ L'ordre est-il cohérent ?

- Les références reprises habituellement dans ce type d'ordre présenté par le créancier sont-elles présentes ?

➲ Le taux de rejets des prélèvements émis paraît-il inhabituel par rapport à l'activité du client ?

- Le suivi du taux de R transactions du créancier peut être le révélateur d'une activité anormale.
  - Se poser la question à propos des motifs des rejets à destination du créancier
  - S'interroger à propos des rejets pour motifs « contestation débiteur », « absence de mandat », par rapport à l'ancienneté de la relation, « comptes clos »...
  - Des rejets de prélèvements massifs ont-ils eu lieu concomitamment à une modification des habitudes clients, par exemples, virements vers l'étranger, remises de chèques de montant important … ?
- Le créancier sera-t-il capable de faire face à des retours d'impayés sur une période pouvant aller jusqu'aux 13 mois après l'émission des prélèvements ?

➲ L'ICS est-il valide ?

- Pour les créanciers français, l'ICS est-il valide dans la base des ICS détenue par la Banque de France ?

En cas de doute, prendre contact
avec le client créancier à partir des coordonnées figurant au fichier de la banque

DEBITEURS

La meilleure parade pour les clients débiteurs est de réaliser un suivi régulier de leurs opérations bancaires de débit.

- Le créancier est inconnu (ICS, NOM, RUM). L'opération ne semble pas correspondre à l'achat d'un bien ou d'un service effectué par le client.
  Attention toutefois à l'utilisation de la raison sociale et de la marque commerciale qui peuvent être différentes du libellé de l'opération.

- Les données du créancier sont connues mais l'opération paraît anormale, le montant du débit ne correspond pas à celui annoncé dans la pré-notification.

- Le créancier est connu mais la RUM n'est pas connue, l'opération ne correspond pas à un mandat signé avec ce créancier.

Dès lors qu'une opération paraît suspecte, les clients ont :

- Soit à prendre contact auprès de leur créancier afin de vérifier le bien-fondé du prélèvement.
- Soit à intervenir au plus tôt auprès de leur banque respective dans les conditions prévues par les textes réglementaires. Ainsi, le débiteur a la possibilité :
  - avant le règlement interbancaire, de refuser le prélèvement SEPA auprès de sa banque.
  - après cette date, de contester l'opération et de demander le remboursement auprès de sa banque sous certaines conditions, sachant notamment que la procédure est différente en fonction du délai dans lequel la contestation est reçue par la banque.[30]

De même, les clients doivent être vigilants sur les « mandats » qu'ils signent. Ces documents doivent respecter une certaine formalisation [31] et être en cohérence avec les engagements contractuels du fournisseur. En cas de désaccord, il est toujours possible à un débiteur d'intervenir immédiatement auprès de son créancier pour que ce dernier sursoie à la transmission de l'ordre de prélèvement SEPA ou émette une instruction en vue de la révocation de l'ordre de prélèvement initial.

Les coordonnées bancaires et la signature d'un client débiteur peuvent être obtenues par le vol ou la ruse sous des prétextes divers en récupérant tout document ou tout support contenant ces informations.

Cela s'applique aux principaux moyens de paiement (méthodes décrites en particulier en page 60 du présent document).

[30] Brochure « La migration prélèvement national vers le prélèvement SEPA » disponible sur le site Internet du CFONB (www.cfonb.fr) à la rubrique Espace documentaire > Instruments de paiement > Prélèvement

[31] Brochure « Le Prélèvement SEPA - SEPACORE Direct Debit » et les modèles de mandats disponible sur le site Internet du CFONB (www.cfonb.fr) à la rubrique Espace documentaire > Instruments de paiement > Prélèvement

SPECIFICITES LIEES AU PRELEVEMENT SEPA INTERENTREPRISES

RAPPEL

Le prélèvement SEPA interentreprises[32] (SEPA Business-To-Business Direct Debit ou B2B), est destiné aux « non-consommateurs » souhaitant régler tout ou partie de leurs créances selon des conditions particulières.[33]

POINTS DE VIGILANCE CONCERNANT LE PRELEVEMENT SEPA INTERENTREPRISES – SEPA BUSINESS TO BUSINESS DIRECT DEBIT »

- Les règles du prélèvement SEPA interentreprises en matière de remboursement sont différentes de celles du prélèvement SEPA Core[34], sachant que la banque du débiteur a la connaissance de la signature d'un mandat B2B afin de pouvoir mener les contrôles de son ressort. Ainsi, le débiteur a obligation de lui communiquer les données du mandat qu'il a signé auprès de son créancier avant la présentation au paiement du premier prélèvement. A défaut, le SDD fera l'objet d'un rejet.

  Les données du mandat, dûment confirmées par le débiteur, sont conservées par la banque du débiteur avec les éventuelles instructions de paiement données par ce dernier. Pour les prélèvements SEPA interentreprises récurrents qui suivent, la banque du débiteur vérifie notamment la validité des coordonnées bancaires du débiteur non consommateur, l'absence d'instruction de non-paiement, la cohérence des données du mandat validées par le débiteur et des éventuelles instructions de paiement de ce dernier, avec les données de l'opération reçue.

  Le prélèvement SEPA interentreprises exclut tout droit à remboursement des transactions autorisées par le débiteur « non-consommateur ». Cela étant, le débiteur, après règlement et dans un délai maximum de 13 mois, peut contester un prélèvement SEPA interentreprises qu'il estime erroné.

  Il s'agit d'une procédure exceptionnelle, notamment en cas d'action frauduleuse du créancier ou de ses préposés.

- Les mesures préventives déclinées pour le SDD Core dans le présent document sont bien évidemment à respecter pour le SDD B2B.

- En tant que banque du débiteur, du fait de la réception du mandat, en cas de doute, prendre contact avec la relation (à partir des coordonnées détenues dans les bases de la banque).

- La banque du créancier peut toutefois être amenée à supporter des débits en cas de contestation du débiteur face à un créancier escroc, le débiteur pouvant être complice ou non. Voir partie « cavalerie » du présent guide.

---

[32] Brochure « Le Prélèvement SEPA Interentreprises – SEPA Business to Business Direct Debit » disponible sur le site Internet du CFONB (www.cfonb.fr) à la rubrique Espace documentaire > Instruments de paiement > Prélèvement

[33] Cf. paragraphe : « DIFFERENCES ESSENTIELLES entre le prélèvement SEPA Core et le prélèvement SEPA Interentreprises. »

[34] La banque du débiteur reçoit, dans l'ordre de prélèvement SEPA Core, les données dématérialisées du mandat transmises par le créancier. Elle n'a pas d'obligation de contrôler ces données.

Compte-tenu des particularités du prélèvement SEPA Interentreprises, en cas de contestation liée à une fraude, la situation peut notamment être la suivante :

- Le créancier (ou l'un de ses employés) est un escroc et le débiteur est particulièrement négligeant ;
- Le débiteur est complice du créancier (voire il s'agit de la même personne) ;
- L'IBAN à créditer ne correspond pas au compte du créancier officiel (mandat détourné) ;
- L'IBAN du créancier indiqué sur le mandat est différent de l'IBAN à créditer contenu dans l'opération, cela étant, l'ICS est valide° ;
- L'ICS contenu dans l'opération est différent de l'ICS associé au mandat du compte à débiter…

CAS CONCRETS DE TENTATIVE DE FRAUDE

➲ Les banques des débiteurs reçoivent des mandats, qui s'avèrent être des faux, aux fins d'enregistrements dans leurs bases.

Ces mandats sont accompagnés de lettres à l'entête de grandes entreprises multi bancarisées ; ces correspondances comportent souvent des irrégularités.

Les entreprises en question ne sont pas à l'origine de la demande d'enregistrement : leur nom, ICS et signature ont été usurpés pour effectuer des prélèvements B2B.

➲ Un fraudeur crée une société et la fait immatriculer puis fait signer légitimement des mandats B2B à ses débiteurs ou rachète une société avec récupération de mandats légitimes. Après une période d'activité sans difficulté particulière, le créancier change de comportement et envoie des prélèvements illégitimes. Le fraudeur transfère les fonds encaissés vers des comptes à l'étranger puis disparaît.

Bien que la banque du débiteur ait effectué ses contrôles, elle n'a pas pu détecter la fraude.
La Banque du créancier doit alors assumer la perte financière liée à cette fraude.

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LES FRAUDES DITES TRANSVERSALES

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

L'UTILISATION DE LA BANQUE EN LIGNE

1. PRESENTATION

DEFINITIONS DES PRINCIPALES ATTAQUES SUR INTERNET

Les techniques de fraude :

- *Hameçonnage ou « phishing » :* technique utilisée par les fraudeurs visant à obtenir des données personnelles, principalement par le biais de courriels non sollicités renvoyant les utilisateurs vers des sites frauduleux ayant l'apparence de sites de confiance.

- *Piratage de systèmes automatisés de données, de serveurs ou de réseaux :* intrusion frauduleuse sur de tels systèmes.

- *Virus :* certains virus s'installent « discrètement » sur l'ordinateur utilisé via un courrier électronique reçu ou un téléchargement. Celui-ci peut donc avoir un fonctionnement « défaillant », sans que l'utilisateur ne s'en aperçoive. Des informations peuvent être détruites ou être récupérées et retransmises à distance.

- *Cheval de Troie :* il s'agit d'un virus qui peut installer des logiciels espions permettant de mémoriser et restituer l'activité de l'ordinateur (exemple : des frappes au clavier pour les envoyer à un serveur tiers). Un programme se substitue à un autre programme, ce de façon complétement transparente pour l'utilisateur.

- *Pharming (contraction des mots anglais « farming » « culture fermière » qui consiste pour les jeux en ligne à récolter de l'argent) et « phone phreaking » (piratage des lignes téléphoniques).* L'utilisateur est redirigé automatiquement vers un site pirate ressemblant au vrai site. Les pirates peuvent alors récupérer toutes vos informations.

- *Malware :* Logiciel installé sur le PC à l'insu de l'utilisateur pour y réaliser des opérations malveillantes.

- *SWAP de SIM :* activation frauduleuse d'une carte SIM par un pirate auprès d'un opérateur.

- *« Rançongiciel » / rançonnage :* Un programme malveillant chiffre les données du poste compromis. A travers la boîte de dialogue ou par téléphone, la victime est ensuite soumise à un chantage consistant à verser de l'argent afin de récupérer la clé permettant de déchiffrer les documents.

2. TYPES D'ATTAQUES

Note au lecteur : dans cette partie, nous nous limiterons à illustrer deux types d'attaques : l'hameçonnage et le rançonnage.

HAMECONNAGE ou PHISHING

Un courrier électronique propose à l'utilisateur de se connecter à son site bancaire à distance au moyen d'un lien.
L'utilisateur est routé sur un site factice. Celui-ci va permettre au fraudeur de récupérer les codes d'accès de la victime (identifiant et mot de passe) via la réception d'un courriel, d'un téléchargement ou autre…

En fonction des services ouverts par le Prestataire de Services de Paiement, le fraudeur, après avoir « pris la main » sur le compte du client, va pouvoir par exemples :

- Ajouter un compte sur la liste des bénéficiaires de virement
- Changer l'adresse du titulaire de compte…

Le fraudeur cible ces opérations dites engageantes[35] (cf. supra) effectuées par le canal « banque en ligne » et faisant l'objet d'une authentification renforcée[36]. L'un de ces dispositifs consiste à envoyer un code par SMS au client.
L'objectif, pour le pirate, est de récupérer ce code de validation envoyé au client.

« Rançongiciel » / RANCONNAGE

La victime souvent contactée par téléphone et/ou courriel exécute les manipulations demandées par l'escroc. Ce dernier va ainsi pouvoir prendre le contrôle de l'ordinateur, le bloquer ou chiffrer des données personnelles.
Une pression est ensuite exercée sur la victime pour qu'elle :

- Effectue elle-même une opération de paiement
- Fournisse au fraudeur ses coordonnées bancaires, permettant à celui-ci de réaliser des opérations de paiement….

A défaut selon les dires de l'escroc, la victime ne récupérera pas l'accès à son ordinateur.

POINTS D'ATTENTION

Des dispositifs mis en place par les banques peuvent conduire les fraudeurs à se détourner de l'opération virement Banque En Ligne (BEL). Ainsi, grâce à l'identifiant/mot de passe du client victime et aux techniques décrites ci-dessus, le fraudeur peut, en fonction des services proposés par le Prestataire de Services de Paiement :

- Changer d'adresse et commander un carnet de chèque ou une nouvelle carte
- Souscrire à un e-wallet et effectuer des achats en ligne
- …

[35] Contenu du service variable d'un établissement à un autre

[36] Il s'agit généralement de la saisie d'un code à usage unique par le client, en plus de ses identifiant/mot de passe. Le fraudeur doit donc récupérer ce code à usage unique pour ajouter un bénéficiaire et exécuter un virement frauduleux.

EXEMPLES CONCRETS via la Banque En Ligne (BEL)

Pour récupérer les identifiant/mot de passe BEL d'un client, qui sont des données « statiques », le fraudeur utilisera du phishing ou du vol de courrier. Mais ces informations sont insuffisantes pour exécuter un virement vers un bénéficiaire inconnu du client. L'ajout du bénéficiaire nécessite la saisie d'un code à usage unique (donnée dynamique, avec une durée de vie limitée). L'objectif pour le fraudeur est de récupérer ce code, les exemples suivants présentent les techniques qu'il peut utiliser.

Le client se connecte au site frauduleux en pensant accéder au site de sa banque en ligne. Parallèlement, le fraudeur se connecte au site officiel et prépare l'ajout d'un bénéficiaire.

Ensuite, le fraudeur via le site frauduleux demande au client de saisir le code SMS, intercepte celui-ci et valide l'ajout du bénéficiaire sur le site officiel.

- Si le code est mis à disposition du client par un autre dispositif que le SMS (c'est-à-dire par courrier), le fraudeur demandera au client d'activer ce dispositif. Le fraudeur est très convaincant, le client est persuadé que s'il ne donne pas ce code, il sera victime d'une fraude qui sera à sa charge. L'appel du fraudeur peut être effectué également durant la nuit.
- Si le code à usage unique est envoyé par courrier. Le fraudeur pourra, par exemple, usurper l'identité du client et demander un changement d'adresse pour se faire envoyer le courrier directement chez lui. Il peut également dérober dans la boite aux lettres du client le courrier envoyé.
- A noter : lors du phishing, les N° de téléphone (fixe et mobile) sont parfois demandés au client.

Quelques techniques de fraude plus élaborées

- Swap de SIM

Une fois le Swap de SIM (Cf. page 39) effectué, le mobile du client n'est plus opérationnel. Toutefois le client peut mettre quelque temps avant de réagir et d'appeler son opérateur.

- Malware sur l'ordinateur du client

Il existe plusieurs scénarios, mais l'objectif est toujours le même, permettre au pirate d'être « logiquement » entre l'ordinateur du client et le site de la banque.

- Le client pense se connecter à sa banque en ligne, il entre ses identifiant/mot de passe. Le malware récupère ces données, se connecte à la banque en ligne du client et fait une demande d'ajout de bénéficiaire. Il affiche un message à destination du client indiquant que pour des raisons de sécurité, il doit saisir son code à usage unique (qu'il vient de recevoir par SMS, par exemple). Le client saisit le code, le malware ajoute un bénéficiaire, exécute un virement frauduleux et permet au client d'accéder à son espace sécurisé ou invoque un problème (demande de se connecter plus tard).
- Les clients étant de plus en plus sensibilisés au phishing, ils répondent de plus en plus rarement à ce type de courriel. Les pirates se sont adaptés en développant des malwares permettant de récupérer ces informations. Par exemple, le questionnaire correspondant au phishing ne va s'activer qu'au moment où le client sera dans son espace sécurisé de la banque en ligne. Il peut alors penser que ces demandes sont légitimes (le numéro de la carte, la date de fin de validité et le cryptogramme seront demandés).

- Un malware peut modifier toutes les informations saisies par le client avant qu'elles ne soient envoyées au Système Informatique (SI) de la banque et afficher d'autres données que celles provenant de ce SI. Le client demande l'ajout d'un bénéficiaire, le malware modifiera ces données et fera donc ajouter un autre bénéficiaire. Ainsi, le client saisira le code à usage unique pour ajouter le bénéficiaire indiqué par le malware, tout en voyant à l'écran les coordonnées bancaires de son bénéficiaire effectif. Il pensera effectuer le virement vers ce dernier, alors que celui-ci sera effectué vers le bénéficiaire ajouté par le malware (le montant pouvant également être modifié).
- Le malware peut également affecter le smartphone du client. Ce dernier recevra tous les SMS qui lui sont destinés, sauf ceux qui contiennent le code à usage unique (le malware opère en fonction de l'émetteur du SMS).

Autre typologie

Dans certains cas, les escrocs appellent directement les clients par téléphone et cherchent, par exemples, à se faire passer pour un « service de répression des fraudes de la banque» ou un « service sécurité de la banque **»** en charge de la surveillance des paiements.

Prétextant la détection d'une opération frauduleuse d'achat en ligne, ils expliquent au client être en mesure de bloquer cette opération par le biais d'une manipulation sécurisée qui nécessite l'envoi d'un SMS sur le téléphone portable du client.
Ce SMS correspond en réalité à la création d'un nouveau bénéficiaire de virements effectuée en ligne par le pirate.

Les malfaisants insistent particulièrement sur le fait que cette opération est indispensable au blocage de la transaction frauduleuse. Ils demandent ensuite au client de leur communiquer le code qu'il a reçu. Ils sont ainsi en mesure de valider la création de l'IBAN du nouveau bénéficiaire de virements et de l'utiliser pour « vider » les comptes du client.

3. MESURES PREVENTIVES

QUELQUES CONSEILS AUPRES DES CLIENTS CONCERNANT L' ACCES A LA BANQUE EN LIGNE

Protégez vos connexions

- Vérifiez que la connexion est sécurisée : présence de https devant l'adresse du site, icône d'une clé ou d'un cadenas dans la fenêtre du navigateur internet.
- Contrôlez qu'aucune autre fenêtre internet n'est ouverte. Pour accéder à votre banque en ligne, tapez uniquement l'adresse exacte fournie par votre banque.
- N'activez la fonction Bluetooth[37] ou WI-FI que lorsque c'est nécessaire et désactivez-là dès la fin d'utilisation.
- Utilisez exclusivement des équipements (ordinateur – smartphone) dont vous maîtrisez le niveau de sécurité.
- Evitez de vous connecter depuis un ordinateur ou un réseau WI-FI public.
- Ne téléchargez que des programmes et contenus provenant d'une source fiable. Cela peut concerner tout type de photos, vidéos, jeux, thèmes pour mobiles, etc…
- Déconnectez-vous de façon sécurisée et effacez l'historique en fin d'utilisation.
- Effacez le contenu de la corbeille dès lors que vous avez supprimé des documents.
- Activez régulièrement les scans de vos anti- virus.
- Changez vos mots de passe régulièrement.

Protégez vos codes d'accès à la Banque en Ligne

- Ne communiquez jamais des données sensibles (numéro de cartes, mot de passe, code d'accès) en cliquant sur un lien envoyé par courrier électronique ou par téléphone.
- Ne divulguez à personne vos identifiants et mots de passe (ni à votre banque, ni à la police…) car personne n'a besoin de les connaître. Conservez les en sécurité et hors de portée de quiconque.
- Ne gardez pas dans la mémoire de l'ordinateur vos codes d'accès même s'il vous le propose,

  En cas de doute ou de problème d'accès au site de votre banque en ligne, prenez contact directement avec le conseiller clientèle de votre banque.
- Ne communiquez jamais un code reçu par SMS.
- Ne répondez pas à toute demande de manipulation sur votre ordinateur émanant d'un interlocuteur que vous n'auriez pas sollicité ou sous prétexte d'une quelconque mise à jour.
- N'ouvrez pas un message « douteux » avec un objet et un contenu passe-partout surtout si une pièce jointe est attachée. Dans ce cas, détruisez-la sans l'ouvrir.
- Si vous constatez des anomalies avec votre téléphone mobile (perte prolongée de réseau, carte SIM invalide…), il peut s'agir d'une attaque de fraudeur. Dans ce cas, contactez immédiatement votre opérateur téléphonique pour l'en informer et prévenez votre interlocuteur bancaire habituel.
- N'effectuez aucune opération de banque à distance (connexion, virement, opposition…) si vous pensez avoir un virus sur votre ordinateur et contactez votre agence pour demander de nouveaux codes d'accès.

[37] Technologie de réseau sans fil de faible portée permettant de relier des appareils entre eux (par exemples imprimante, téléphone portable, souris, clavier…)

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

L'INGENIERIE SOCIALE

1. PRESENTATION

Les Autorités et la Presse se font fréquemment écho d'escroqueries aux « faux » ordres de virement.

Les escrocs utilisent les techniques basées sur

- L'utilisation de technologies actuelles (plateforme de dématérialisation des numéros de téléphone, de cartes de paiement prépayées « anonymisées »…)
- La constitution de dossiers d'informations sur les entreprises via par exemples, leurs sites internet, la presse, les commandes de statuts de sociétés et d'extraits K Bis sur infogreffe, autres…

L'ingénierie sociale (ou « social engineering » en anglais) **est une technique qui consiste à faire croire à une personne qu'elle a à faire à un interlocuteur légitime, ceci en vue**

- d'obtenir des informations
- ou de lui faire réaliser des opérations (par exemple, un virement).

2. TYPES D'ATTAQUES

LE PROCESSUS DE CERTAINES ATTAQUES ACTUELLES

Généralement, la technique adoptée se déroule en deux étapes :

- d'une part, la collecte d'informations
- d'autre part, la réalisation d'un transfert de fonds.

Une équipe de malfaiteurs prépare des dossiers étayés sur des entreprises, leurs dirigeants et certains membres de leur personnel. L'objectif est d'obtenir un maximum de renseignements au-delà des informations génériques de l'entreprise (par exemples, informations concernant la vie privée des dirigeants recherchées sur des réseaux sociaux, des collaborateurs, manifestations internes…) afin d'être en mesure de rendre encore plus plausible l'escroquerie.

Des membres de la société victime, par exemples, Directeurs financiers, comptables… sont ensuite contactés par téléphone ou/et par courriel par une autre équipe de malfaiteurs. Grâce aux plateformes de dématérialisation de numéros, le numéro d'appel correspond à un numéro de la région d'où est censé provenir l'appel, ce afin de mettre en confiance l'éventuelle victime.

Ce fraudeur se fait passer pour le Dirigeant (par exemples, le PDG ou le DG de la maison-mère de la société victime), allant parfois jusqu'à imiter la voix du Dirigeant… Il demande l'exécution d'un ou de plusieurs virements souvent conséquents à destination d'un pays étranger. Il explique la nécessité et l'urgence de l'opération par une attaque prochaine de la concurrence, un contrôle fiscal ou autre….

Le collaborateur de la société victime, mis en confiance, très souvent relancé par le malfaiteur qui exerce très fréquemment une pression psychologique sur son interlocuteur (de type « je ne vous oublierai pas lors des prochaines augmentations individuelles car vous êtes un collaborateur de confiance »…) peut ainsi faire exécuter l'opération.

EXEMPLES CONCRETS

Le fraudeur recueille de nombreuses informations tant sur l'entreprise (organigramme, signatures des dirigeants, modèles de papier à entête, …) que sur l'organisation et le dispositif de la banque (il connaît le nom du conseiller de clientèle, les numéros de fax, le mode de passation et de validation des virements convenu entre le client et la banque….). Comme il est extrêmement bien renseigné et d'un aplomb sans faille, il se fait passer pour un interlocuteur variable en fonction du scénario choisi. Ainsi, il peut s'agir, par exemples, du Directeur des Affaires Financières, ou d'un policier chargé d'une enquête, d'un technicien de la banque suite au passage aux normes SEPA de virement et de prélèvement, ou d'un cabinet de conseil… . De même, la cible des collaborateurs contactés peut être variable, Directeur financier, comptable, secrétaire… de l'entreprise victime.

PLUSIEURS SCENARIOS IDENTIFIES

Note au lecteur : des coquilles/fautes d'orthographe sont contenues dans ces exemples issus de cas concrets.

LA « FRAUDE AU PRESIDENT »

Une comptable aurait été manipulée, sous le sceau de la confidentialité et sur instructions (supposées) du PDG pour effectuer des virements à destination de l'étranger, ceci dans le cadre d'opérations de croissance externe. La comptable aurait reçu de la part du PDG (par courriel notamment), des informations selon laquelle elle aurait été choisie pour ses qualités professionnelles et de discrétion pour l'assister dans diverses missions d'acquisition et réceptionner des ordres de virement urgents à destination de l'étranger (ces ordres devant rester strictement confidentiels y compris vis-à-vis du directeur financier et du deuxième comptable de l'entreprise). Les documents ayant servi d'instructions pour les virements comportaient la signature conforme du PDG.
Il peut être fait référence à un cabinet d'avocat ou à l'AMF également.

Exemples d'usurpation d'adresse courriel du PDG et OPA confidentielle.

De : monPDG@monEntreprise.com [mailto:**monPDG@s487846204.onlinehome.fr**]
Envoyé : mercredi 20 novembre 2013 11:37
À : XXXX
Cc : michel.polac@amf-transactions.com
Objet : Confidentiel

Madame XXX,

Voici l'OPA en cours,

Nous effectuons en ce moment une opération financière concernant un rachat de société basé en Chine.

Cette OPA doit rester strictement confidentielle, personne d'autre ne doit être au courant pour le moment.

L'annonce public de cette OPA aura lieu le 11 Décembre 2013 dans nos locaux avec la présence de toute l'administration.
Je vous ai donc choisi pour votre discrétion et votre travail irréprochable au sein du groupe pour le traitement de cet OPA.

Merci de prendre contact de suite avec Monsieur Polac de l'AMF (michel.polac@amf-transactions.com) pour la remise des coordonnées bancaires afin d'effectuer le virement dans l'immédiat.

Par mesure de sécurité, merci de dialoguer uniquement sur mon mail personnel (monPDG@gmail.com) pour ce type d'opération confidentielle où nous pourrons discuter sans risque de divulgation afin de respecter la norme de cette OPA .

Merci de ne faire aucune allusion sur ce dossier de vive voix, ni même par téléphone uniquement sur mon mail personnel selon la procédure imposée par l'AMF (autorité des marchés financiers).

Cordialement.

NOM du PDG

De : XX <axxxx.dxxxxx@asahlm.com>
Envoyé : mardi 22 juillet 2014 11:25
À : xx xxx
Objet : Re: Dossier actes
Nous effectuons en ce moment une opération financière concernant un rachat de société étrangère basée en Chine.
Je souhaite que cette opération soit traitée uniquement par vos soins.

Cette OPA doit rester strictement confidentielle, personne d'autre ne doit être au courant pour le moment et cela afin de préserver nos avantages face aux offres concurrentes.

L'annonce publique aura lieu le Mardi 29 Juillet 2014 dans nos locaux en présence de toute l'administration.

Merci de prendre contact de suite par mail avec Me Fortin du cabinet Bresson (m.fortin@cabinet-bresson.com) pour la remise des coordonnées bancaires de la partie adverse afin d'effectuer un virement d'un premier acompte d'un montant 976'260 euros (Valeur jour).

(Référence du dossier a mentionner sur le mail REF# JT46B25)
PS: Par mesure de sécurité, merci de dialoguer uniquement sur mon mail sécurisé (xxx.xxxx@hushmail.com) sur ce type d'opération confidentielle afin de discuter sans risque de divulgation et de respecter la norme de cette OPA.

Merci de ne faire aucune allusion sur ce dossier de vive voix, ni même par téléphone et de ne tenir aucun propos a ce sujet avec tiers personne, uniquement sur mon mail personnel selon la procédure imposé par le cabinet.
J'aviserai personnellement les personnes concernées en temps voulu.

Dès l'ordre de virement rédigé, merci de me le faire parvenir sur mon mail personnel afin que j'y appose ma signature si nécessaire.
Cordialement,

« LES FAUX TESTS SEPA »

Quelques groupes de fraudeurs ont utilisé des scénarios similaires durant plusieurs mois. Depuis le 1er août 2014, le scénario évoque généralement une mise à jour des versions des logiciels. Quasiment à chaque fois, les fraudeurs se présentent en tant que « service connectique » ou « service télématique » de la banque, voire de la Banque de France. L'objectif est de convaincre les comptables des entreprises de réaliser de soi-disant virements « tests » SEPA. Ils travaillent uniquement à distance, principalement via des usurpations d'identité par téléphone, et dans certains cas, avec de faux courriels et des fausses télécopies.

Plusieurs « variantes » ont été constatées, notamment :

- Prise de contrôle du PC /de l'ordinateur du client via des sites internet légitimes de dépannage informatique.
- Suivant les cas :
  - Souvent, le fraudeur essaie de convaincre le client de saisir lui-même le virement via ses outils habituels et dans l'éventualité où le site de banque en ligne serait indisponible de lui transmettre toute information ou fichier relatifs au virement afin qu'il le fasse à sa place.
  - Plus rarement, le fraudeur saisit le virement en profitant de la prise de contrôle du PC.
- Si une confirmation de fax est nécessaire, le fraudeur demande au client de lui envoyer une ancienne confirmation. Il lui reste alors à modifier ce fax et à le transmettre à la banque.
- Dans certains cas, les fraudeurs ont aussi infecté les PC de plusieurs victimes avec des logiciels espions.

Ou

Le fraudeur contacte le comptable d'une entreprise en se faisant passer pour un collaborateur de la banque (service connectique) afin de lui faire réaliser des tests dans le cadre de la mise en conformité avec les normes SEPA. Dans certains cas, Il peut adresser un courriel pour confirmer la véracité de l'opération. L'usurpateur peut demander au client de lui communiquer par fax un modèle d'ordre de virement vierge ou un exemplaire utilisé récemment en précisant dessus la mention « test ». Dans certains cas, le fraudeur a convaincu la victime d'installer un logiciel sur son [PC]. Ce logiciel permet de piloter le PC à distance.
Au final, l'escroc réussit à convaincre la victime d'exécuter un virement test pour une somme souvent à six chiffres.

3. MESURES PREVENTIVES

Les fraudeurs exploitent les faiblesses des organisations des entreprises qu'ils ciblent et, en particulier, l'absence éventuelle de coordination entre les différents acteurs d'un processus.

Voici quelques règles de bonnes pratiques[38] qui sont des règles de bon sens :

Pour le client

- vérifier l'identité et la légitimité de toute personne demandant une information ou initiant une opération sensible / urgente /confidentielle / exceptionnelle,
- être conscient de la capacité des fraudeurs à usurper des identités par courriel et par téléphone, à détourner des lignes téléphoniques,
- veiller au strict respect des procédures internes et réaliser les contrôles prévus,
- protéger les informations personnelles et confidentielles, diffusées notamment sur internet.

Pour le(s) Collaborateur(s) de la banque

- en cas de doute, ne pas hésiter à procéder à des contre appels vers plusieurs points d'entrée du client,
- connaître ses clients et ses habitudes (montants, pays destinataires, canaux d'acquisition…).

[38] qui ne sont pas des mesures exhaustives

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LA « CAVALERIE »

1. PRESENTATION

La cavalerie est une escroquerie financière reposant sur un circuit d'opérations sans raison commerciale dans le but de couvrir des problématiques de trésorerie. Ce système repose sur des décalages de dates et de montants entre les encaissements et les décaissements.

De façon générale, le fraudeur, personne physique ou personne morale, va agir à partir de plusieurs comptes, ouverts dans le même établissement ou non, en utilisant un ou plusieurs moyens de paiement.

De nombreuses combinaisons sont possibles :

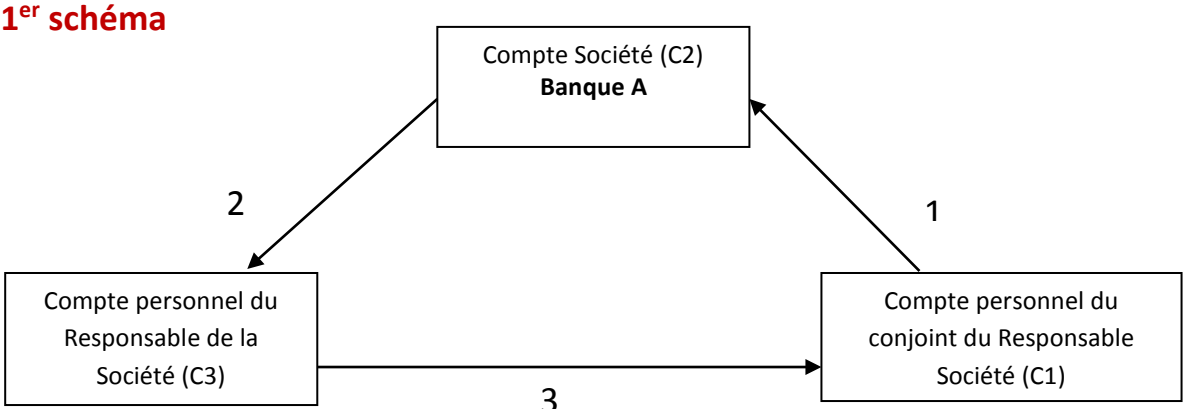
- cavalerie associée à une ouverture de compte réalisée avec des documents justificatifs faux,
- encaissement de chèques à partir de plusieurs comptes détenus par une même personne dans des établissements bancaires différents
- utilisation du même compte pour percevoir un salaire émanant d'une entreprise A
  - avec émission immédiate d'un chèque de même montant à l'ordre de l'entreprise B ;
  - ou avec émission de prélèvements à destination de l'entreprise B.
- rejets des prélèvements à l'issue du délai règlementaire des 13 mois maximum.

L'explication de la mise en œuvre de ce type de fraude répond souvent à une problématique de trésorerie dans laquelle les parties mettent en jeu le différentiel de traitement accordé sur les remises de chèques et/ou d'effets de commerce et les opérations de débit (par exemples, virement, utilisation du chéquier…).

2. TYPES D'ATTAQUES

Pour une meilleure compréhension de la technique, deux exemples de schéma sont présentés ci-dessous.

1er schéma

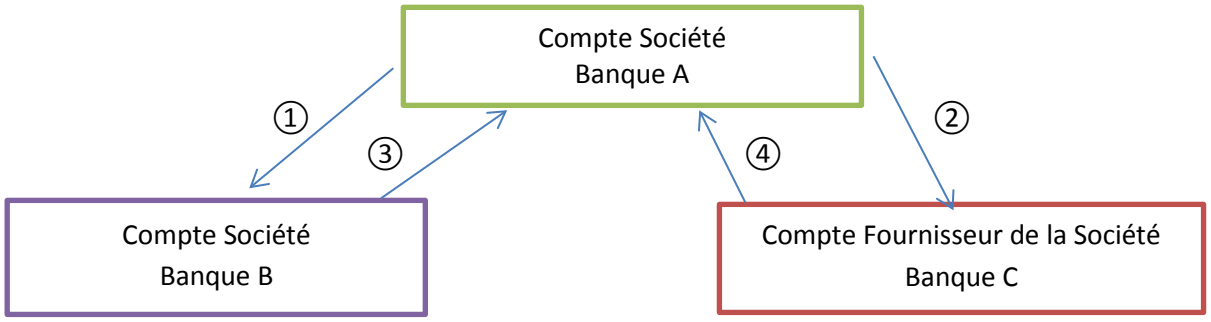


Il s'agit d'un cas basique :

1. Des chèques émis depuis le compte personnel du conjoint (C1) sont remis à l'encaissement sur le compte de la Société (C2) à fréquence journalière.
2. Des ordres de virement sont ensuite réalisés depuis le compte (C2) à destination du compte du responsable de la société (C3) et ce, à fréquence quotidienne également.
3. Consécutivement, des ordres de virement sont immédiatement opérés depuis le compte (C3) avec pour bénéficiaire, le compte (C1).

Ce type de fonctionnement est l'illustration d'une fraude assortie d'un risque de crédit.

2ème schéma



① et ② Des prélèvements sont émis vers les comptes tenus chez les banques B et C. Le compte de la société fonctionne sans difficulté particulière tant chez la banque A que chez la banque B

13 mois plus tard

③ et ④ Des rejets de prélèvements (motif opération non autorisée) arrivent massivement vers le compte de la société chez la Banque A. Les demandes de mandat aboutissent ou non et le client a disparu en laissant un solde très faible sur son compte.

EXEMPLES CONCRETS

1. Technique basée sur le retour de chèques impayés

Compte ouvert à la banque A en octobre 2012, sans mouvement pendant de nombreux mois. L'extrait de compte ci-dessous permet d'appréhender le fonctionnement du compte.

BANQUE A

Extrait de compte simplifié

Date	Opération	Débit	Crédit	Solde
oct-12	Ouverture du compte avec Dépôt d'espèces		100	100
27 01 2014	Remise 2 chèques (compte frère titulaire compte chez **banque B**) : 1 500 et 3 500 euros		5 000	5100
30 01 2014	Facture carte : Achat matériel informatique	4 700		400
31 01 2014	REJET Chèques déposés le 27 01 : compte soldé	5 000		-4 600
03 02 2014	Remise 1 chèque (compte titulaire compte chez **banque B**)		6 000	1 400
03 02 2014	Facture carte : Achat d'essence	50		1 350
04 02 2014	Facture carte : Achat de meubles	4 300		-2 950
10 02 2014	REJET Chèque déposé le 3 02 (motif : défaut de provision)	6 000		-8 950
24 02 2014	Facture carte : Achat de vêtements	1 500		-10 450
25 02 2014	Facture carte : Achat matériel Hi-fi	2 100		-12 550
01 03 2014	Remise 1 chèque (compte d'une SCI chez **banque C**)		12 000	-550
05 03 2014	REJET Chèque déposé le 01 03 (motif : défaut de provision)	12 000		-12 550

- Remise de chèque de 12K € émis par la SNC X, gérée par la mère du client, et dans le même temps émission d'un chèque de même montant par le client à l'ordre de ladite société aboutissant à un tirage de chèques croisés, sans aucune justification économique.
- Le client se faisait de la trésorerie en émettant des chèques croisés entre son compte professionnel ouvert à la Banque A et son compte de particulier ouvert à la Banque B.
- La cliente a procédé à l'ouverture de 5 comptes à vue dans des établissements bancaires différents. Elle s'est fait délivrer des moyens de paiement qui lui ont permis d'alimenter ces comptes et qu'elle a utilisés de façon abusive : chéquiers et CB. Elle a, au final, émis 157 chèques (toutes banques confondues) sur une période [de 20 jours] pour un montant total de 40 969 €.
- Suite aux retours d'impayés de deux chèques tirés sur la société X (domiciliée à Toulon), le client "régularise" le débit par la remise d'un chèque tiré sur la SARL Y (domiciliée à Rouen) pour continuer à utiliser ses moyens de paiement. Ce chèque revient également impayé. Après enquête, il est noté que les deux sociétés ont la même gérante, enregistrée à deux adresses différentes. De plus, le client laisse entendre qu'il se verse des salaires de ces deux structures, dont il semble être le gérant de fait. Enfin, il est constaté que la cavalerie dure manifestement depuis quelque temps.

- En deux jours, le client a effectué 5 remises de 1 chèque dans 5 guichets de Tours, montants compris entre 1.216 € et 1.276 €. Ces chèques, émis sur son propre compte à la Banque A sont revenus impayés pour "compte clôturé".
- Dans la foulée, il a utilisé sa CB et émis 2 virements via ses outils de banque à distance (1.000 et 2.500 €) vers les comptes d'un tiers à la banque B.
- Un client détient un compte de particulier dans une agence de la banque et un compte professionnel dans une autre agence de cette même banque. Il a remis le 26/11 sur son compte professionnel des chèques tirés sur son compte de particulier (6.524 €+3.650€), alors que la veille se présentaient au paiement des chèques tirés sur son compte professionnel au profit de son compte de particulier.

2. Technique basée sur des rejets de prélèvements

a) Principe de fonctionnement

Dans la cadre du prélèvement, le principe de fonctionnement reste identique. Le créancier pourra « jouer » sur la position de son compte jusqu'au terme du délai légal de rejet (soit 13 mois maximum après le débit en compte). Dès lors, les complices procèderont aux rejets de l'ensemble des prélèvements reçus sur ladite période. Souvent, les prélèvements effectués ne correspondent à aucune fourniture de biens ou de services.

Une variante consiste en une utilisation du délai des 13 mois par le débiteur lui-même.

b) Mode opératoire

Le mode opératoire de ce type de fraude se décline en 3 étapes :

- **Etape préparatoire**

Le fraudeur va procéder à la création d'une société en apparence légitime. Son discours commercial vis-à-vis de son banquier s'avère être bien préparé et convaincant. Il s'appuie sur la technicité du produit commercialisé et sur le développement de solides partenariats.
Dans cette première phase, le fraudeur met en place son schéma de fraude, il définit son organisation et le rôle de ses acolytes dans cette connivence (ils peuvent être, par exemple, des clients fictifs).

- **Etape d'endormissement**

Afin de tromper la vigilance de son banquier, le créancier frauduleux émet régulièrement des prélèvements, souvent de petit montant, sans caractère singulier. Tout ou partie de ceux-ci sont sans objet.
Dans cette deuxième phase, l'objectif de l'escroc est de leurrer la vigilance de sa banque. Il est d'ailleurs observé très peu de rejets sur les prélèvements émis.

- **Etape finale, réalisation de la fraude**

A une date proche des 13 mois légaux de rejet, la banque du créancier reçoit massivement des demandes de vérification de mandats, documents qui sont produits par le créancier.

Après vérification par les banques des débiteurs, il s'avère que les signatures ont été falsifiées. De ce fait, les débiteurs, parfois complices, demandent à être remboursés. Leurs banques retournent donc les prélèvements pour motif « pas d'autorisation ».

Parallèlement, le créancier avait réalisé des virements issus de ces encaissements vers par exemple une société écran située en dehors de la zone SEPA, ou sur son propre compte situé dans un autre établissement teneur de compte.
Par conséquent, à réception des retours de prélèvements, le compte ne présente plus la provision suffisante. Le créancier est généralement devenu injoignable.

En conclusion
Ce type de fraude présente un risque financier élevé pour la banque du créancier d'autant qu'il peut être aggravé par un système de blanchiment des fonds au moyen d'une société fictive.

Le fraudeur va utiliser la totalité de la période maximum de 13 mois afin de maximiser son gain financier. L'objectif est d'avoir le plus de temps possible pour émettre ses prélèvements afin :

- que le montant de la fraude soit le plus élevé ;
- de passer sous certains seuils d'alerte de la banque en évitant d'émettre des SDD de montant trop important ;
- d'éviter d'alerter sa banque qui pourrait surveiller de manière plus attentive les nouveaux créanciers seulement sur les tous premiers mois.

De son côté, la Société débitée du prélèvement (parfois complice) va procéder à une demande de remboursement d'une opération non autorisée (après 8 semaines et au maximum 13 mois suivant la date du débit).[39]

Observation
Ce type de fraude semble plus compliqué à reproduire sur le prélèvement B2B en raison des règles et des contrôles imposés dans ce contexte.

[39] Les procédures entre PSP sont détailles dans le rulebbok SDD Core – voir également la Brochure CFONB – SDD core (et plus spécifiquement la fiche 7)

3. MESURES PREVENTIVES

Les mesures préventives concernent essentiellement la connaissance du client à travers ses habitudes afin de détecter des comportements atypiques.

L'analyse du fonctionnement du compte doit permettre de juger de la cohérence des opérations :

- Hausse soudaine des dépenses après une remise de chèque(s) ou la réception de virement(s) sur un compte peu approvisionné,
- Remise(s) et émission(s) de chèque(s) ou virement(s) d'un même montant concomitamment,
- Opérations en sommes rondes,
- Emetteurs et bénéficiaires de chèques ou virements croisés,
- Escompte (qualité des tirés, montants…) Suivi spécifique du volume des prélèvements émis, des rejets, en particulier pour les nouveaux créanciers sur une période d'au moins 13 mois après la date d'émission des prélèvements,
- Les contreparties du client créancier …

Il peut être utile d'appeler le client au moindre incident (alertes à ne pas négliger : retours de chèques impayés, d'effets escomptés, tensions de trésorerie… par exemples) ou en cas de réactivation d'un compte inutilisé pendant longtemps. La cohérence de ses explications pourra rassurer ou alerter son conseiller.

CFONB
Comité Français d'Organisation et de Normalisation Bancaires

LES AUTRES ESCROQUERIES DIVERSES

1. PRESENTATION

De façon générale, quelles que soient les arnaques, les escrocs utilisent la dissimulation et l'imitation afin d'arriver à leurs fins. Il s'agit donc pour eux de tromper le ou les interlocuteur(s) et de faire en sorte que ceux-ci procèdent à un transfert de fonds.

Dans ce chapitre, différentes catégories d'attaques frauduleuses sont reprises, le moyen de paiement utilisé n'est pas fraudé. Sont ainsi présentées,

- des attaques via des « petites annonces »,
- des fraudes de type loterie ou de type « nigérianes ». Désormais, les malfaiteurs utilisent le canal internet, sachant que précédemment, ces types d'arnaques étaient réalisés sous forme d'envoi de lettres ou de fax ou de communications téléphoniques,
- des usurpations de fournisseur, de bailleur…
- des ouvertures de comptes frauduleuses,
- des arnaques au crédit, …

Cette liste n'est pas limitative et les techniques des fraudeurs évoluent dans le temps.

Note au lecteur : compte-tenu de la diversité des cas, la présentation de ces fiches a été adaptée par rapport au document global.

2. TYPES D'ATTAQUES

Cas types (non limitatifs)

ATTAQUES VIA DES PETITES ANNONCES

Un particulier ou un professionnel met en vente un bien via internet (auto, moto, animal …). Le vendeur est contacté par un acheteur potentiel et se met d'accord sur le prix.

Dans certains cas, le vendeur fournit ses coordonnées bancaires afin que le règlement se fasse sous forme de virement. En fait, un faux chèque est adressé par "l'acheteur" à la banque teneur de compte. Constatant un crédit sur son compte, le vendeur remet à l'acheteur le bien objet de la vente. Dans d'autres cas, le montant proposé par l'acheteur est supérieur à celui du bien vendu. La majoration est justifiée par la rémunération d'un service demandé en complément (elle couvre par exemple des frais de transports). Le vendeur dépose donc à l'encaissement un chèque du montant convenu et règle la différence soit par virement, soit par transfert d'espèces.

Cette typologie de fraude peut également être utilisée pour les locations saisonnières.

Sous un prétexte quelconque, le montant adressé au loueur est supérieur au montant de la location, à charge pour lui de rembourser la différence au locataire.

➲ Quel que soit le cas, le chèque revient impayé quelques jours plus tard.

Il convient :

- En cas de doute, de se reporter à la partie du guide sur les chèques ;
- D'appeler à la prudence les clients qui feraient part de leur intention de procéder à ce type de transactions.

FRAUDES DE TYPE LOTERIE

A la base, le client va recevoir un courriel lui annonçant qu'il a gagné un gain important à une loterie. Afin de recevoir la somme, le destinataire du courriel se voit réclamer ses coordonnées bancaires afin qu'un virement lui soit adressé. Par ailleurs, sous prétexte de couvrir des frais ou autre, il est demandé un chèque ou un virement, ce avant que les gains lui soient adressés.

Après avoir adressé les fonds, le client sera dans la situation suivante :

- Absence d'information, avec un chèque adressé encaissé ou les fonds transférés récupérés par le fraudeur
- Réception d'un chèque (souvent faux), au lieu du virement annoncé.

FRAUDES DE TYPE « NIGERIANES »

Généralement après piratage de l'ordinateur d'une relation, l'escroc se substitue à une relation du/des destinataire(s). Il utilise la boîte mail de celle-ci et adresse un message important, confidentiel relatant une affaire secrète concernant très souvent cette relation. A titre d'exemples, citons un besoin d'argent d'un ami à l'étranger, pour des frais d'hospitalisation ou autre… un grave problème personnel… un décès… la situation catastrophique dans le pays…
La coopération du destinataire est attendue afin d'effectuer un transfert d'argent à destination du pays étranger ou de la France. En échange, une rémunération importante peut être proposée.

FRAUDES « A L'AMITIE »

L'escroc fait connaissance avec le client sur un site de rencontre ou sur des réseaux sociaux et se lie d'amitié avec cette personne.
L'escroc qui vit dans un autre pays propose de venir rencontrer la personne mais prétextant ne pas détenir de compte bancaire en France demande au client d'encaisser un chèque sur son compte (émis par l'escroc lui- même mais le plus souvent par un ami). Il demande en retour que lui soit adressé la somme par virement ou mandat.

➲ Le chèque revient impayé quelques jours plus tard.

URSURPATION D'UN FOURNISSEUR/BAILLEUR OU Fraude au changement de RIB (règlement factures ou loyers)

Une cible privilégiée des fraudeurs a été constatée sur les bailleurs, les professionnels de l'immobilier… Se faisant passer pour un fournisseur, un bailleur de la victime,… le fraudeur demande un changement de coordonnées bancaires. Cette demande peut se présenter via un courriel, un support papier, un appel téléphonique… Cette modification permettra à l'escroc de recevoir des fonds indus. Le client reçoit un appel téléphonique et un mail du bénéficiaire avec qui il entretient un courant d'affaires régulier l'informant que désormais, il faudrait virer les fonds à un factor à l'étranger (par exemple, en Pologne[40]). A réception de la facture, le client s'exécute. Quelques jours après, le bénéficiaire « véritable »[41] reçoit un appel l'informant que les fonds auraient un peu de retard mais qu'il ne fallait pas s'en inquiéter. Ne voyant toujours rien arriver, ce dernier contacte le client, c'est ainsi que la fraude est découverte.

[40] Cette destination n'est toutefois pas exclusive.
[41] La personne ayant assuré ou assurant véritablement la prestation fournie au Client et en attente d'un paiement. Par exemples, un fournisseur, un bailleur…

3. MESURES PREVENTIVES

FRAUDE AUX PETITES ANNONCES

- Etre vigilant, ne jamais conclure une transaction dans la précipitation en particulier avec des Inconnus.
- Se méfier d'une offre de prix supérieure au montant demandé ou d'une offre au contraire trop attractive.
- N'accepter que des paiements correspondants au montant de la transaction.
- S'assurer que le paiement est réalisé pour le montant et selon les modalités convenues avec l'acheteur (chèque ou virement).
- Ne pas oublier que le chèque, y compris le chèque de banque, n'est pas un moyen de paiement garanti : un rejet est toujours possible.
- En cas de doute, ne pas se dessaisir du bien, préférer reporter la transaction afin d'effectuer les vérifications nécessaires.

FRAUDES DE TYPE « LOTERIES » OU « NIGERIANES » OU «A L'AMITIE »

- Avant tout envoi de fonds, vérifier le bien-fondé de la demande. Il est par exemple, rarissime de « gagner » à une loterie à laquelle le destinataire du courriel n'a pas participé.
- De même, il convient de s'interroger sur le lieu de villégiature de la relation évoquée dans le courriel reçu : est-elle actuellement à l'étranger ? Contacter la personne sur la base d'autres coordonnées déjà utilisées.
- Se méfier des offres trop alléchantes. Ne jamais agir dans la précipitation.
- Garder son sang-froid, évoquer le sujet avec un tiers de confiance avant d'envisager tout envoi de fonds.

USURPATION D'UN FOURNISSEUR/BAILLEUR

- Ces acteurs changent peu fréquemment de coordonnées bancaires. La demande émane-t-elle bien de votre relation ?
- S'interroger si la nouvelle domiciliation bancaire est située à l'étranger.

4. AUTRES

DES FRAUDES D'AUTRES NATURES SONT AUSSI CONSTATEES…

OUVERTURE DE COMPTES POUR EMETTRE DES VIREMENTS NON PROVISIONNES

Cette fraude repose sur des ouvertures de comptes récentes réalisées par des étudiants européens, âgés de 18 à 35 ans, souvent d'origine africaine. Ces entrées en relation sont réalisées dans plusieurs Etablissements bancaires. Durant les premiers mois les moyens de paiement sont délivrés et le fonctionnement des comptes est sans incident. Les moyens de paiement ainsi récupérés permettront de renouveler ces arnaques dans d'autres régions.

Les individus déposent ensuite plusieurs chèques dans différents Points de Vente dont les montants sont souvent compris entre 1.000 et 2.000 €. Parallèlement, ils initient des virements domestiques ou internationaux via la banque en ligne. Ce type d'escroquerie est principalement réalisée à partir de la fin de semaine laissant aux individus 48 heures pour vider les comptes.

Une variante consiste à approcher des clients dont la trésorerie est tendue afin d'exécuter ces opérations. On parle alors de « compte de mule ».

Conseils
Vigilance renforcée dès lors que les événements repris ci-dessus sont constatés.

ARNAQUES AU CREDIT

L'arnaque consiste, au moyen de messages publiés sur internet, à proposer à la future victime un prêt d'argent à un taux extrêmement bas et à lui demander des frais avant de débloquer les fonds. Ceux-ci ne sont jamais débloqués et les frais avancés sont perdus. Par ailleurs, les informations fournies par la victime, par exemple ses coordonnées bancaires, peuvent être utilisées à son insu.

Mode opératoire
Les escrocs se font passer soit pour un particulier, soit pour un établissement bancaire. Ils utilisent les publicités ou la messagerie de réseaux sociaux pour proposer aux internautes une offre de prêt à un taux très bas.
Le message comporte des coordonnées (email et/ou numéro de téléphone). Ces coordonnées peuvent ressembler aux coordonnées officielles d'une banque (avec logo et image de la banque). Les escrocs demandent aux internautes de les recontacter.

Le message contient une offre de prêt d'une somme d'argent remboursable sur une durée définie à l'avance ou à convenir entre les deux parties, à un taux très inférieur à ceux pratiqués sur le marché.

L'objectif du fraudeur est d'amener le « souscripteur du prêt » à lui verser des frais pour la mise en place du dossier. Ces frais (frais d'assurance, de dossier, de notaire, d'avocat, de déblocage, de timbres, etc…) sont payables avant le déblocage des fonds et, généralement doivent être expédiés via une société de transfert d'argent.

Par ailleurs, le fraudeur va également demander de lui transmettre un certain nombre de renseignements et de documents pour constituer le dossier de prêt. Ces éléments à caractère personnel pourront être réutilisés dans d'autres arnaques (par exemple, usurpation d'identité).

Mesures visant à déjouer ce type de fraude

- Si le message semble être émis par votre établissement de crédit, téléphonez à votre conseiller bancaire pour vérifier l'authenticité de l'information.
- Ne transmettez jamais d'informations à caractère personnel sans vérifier le bien-fondé de la demande.
- Ne répondez pas directement aux mails ou aux adresses figurant sur ces messages.
- Soyez circonspect, la loi française réglemente les prêts, y compris pour ceux entre particuliers. Un contrat doit notamment préciser les conditions d'un crédit de gré à gré.
- Ne payez rien à l'avance. De façon générale, la somme réclamée (quel qu'en soit le motif, par exemple : frais de dossier, assurance pour le crédit…) sera réglée lors de la mise à disposition du prêt. La banque aura préalablement respecté des formalités légales : analyse de la solvabilité du futur client avant fourniture de l'accord du prêt, offre préalable de crédit mentionnant le respect des délais légaux de réflexion/rétractation… Un contrat aura été formalisé et accepté….
- Rester prudent et vigilant face aux messages reçus en particulier d'inconnus.

Soyez attentifs

- aux fautes d'orthographe, à la syntaxe.
- à la présentation du site bancaire (connaissez-vous ces logos ? appartiennent-ils au même groupe bancaire ?).
- à des demandes d'informations que votre banquier connaît déjà … Dans le cas où il s'agirait d'une autre banque vous proposant un prêt, celle-ci réclamerait un ensemble de documents pour constituer un dossier de crédit.

Que faire face à ce type d'attaque ?

- Informez votre banquier. Celui-ci procédera à un signalement auprès du réseau social concerné.
- Communiquez le contenu du message et votre présomption d'escroquerie au réseau social concerné.
- Signalez le courriel à INFO ESCROQUERIES (source : www.internet-signalement.gouv.fr).