BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

Fraudes aux opérations bancaires

Comment réagir ?

Guide client

Fraudes aux opérations bancaires

Comment réagir ?

Face à l'évolution des pratiques de paiement et des modes opératoires des fraudeurs, chaque acteur peut contribuer au renforcement du dispositif de prévention des fraudes. En tant que professionnel, vous trouverez ici les éléments utiles pour réagir en cas de fraude ou limiter dans votre activité les cas de fraude en sensibilisant vos équipes et vos clients aux bons réflexes à adopter.

Ce guide expose les cas de fraudes les plus représentatifs tels que :

- **la fraude au virement** (détournements et fraude aux coordonnées bancaires),
- **la fraude à la carte bancaire** (fausses cartes, cartes volées ou coordonnées piratées suite à achat sur un site non sécurisé),
- **la fraude au chèque** (falsifiés, volés),
- **la fraude au prélèvement** (utilisation de coordonnées d'un tiers pour y faire effectuer ses prélèvements).

Vous trouverez dans une seconde partie les services en ligne proposés par la Banque des Territoires répondant à l'ensemble des exigences réglementaires et garantissant un niveau de sécurité élevé pour toutes vos opérations bancaires.

Le virement

Les principaux cas

Attaque informatique : vol de données personnelles et de coordonnées bancaires via phishing et logiciels malveillants.

Détournement : manipulation d'une personne en lui faisant croire qu'elle a affaire à un interlocuteur légitime dans le but de lui faire réaliser une action ou une opération.

Point d'attention : aucune demande de virement n'est demandée par la banque à son client.

Comment réagir ?

- Demander au gestionnaire d'engager la procédure de récupération des fonds (il n'y a aucune garantie de remboursement car le virement a valablement été réalisé).
- Déposer plainte auprès de la police ou de la gendarmerie.

Préconisations

Prévenir les attaques informatiques

- S'équiper et maintenir à jour les systèmes de sécurité informatiques sur l'ensemble des outils professionnels, protéger ses mots de passe et identifiants de connexion (le cas échéant signalez le vol de vos données à la CNIL).
- Communiquer à votre banque vos nouvelles coordonnées lors de changements intervenus dans l'entreprise adresse postale ; mail , personnes habilitées…).
- Accentuer la vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir et les week-ends.

Prévenir les cas de détournement

- Garder tous les documents sensibles dans un endroit sécurisé, accessible aux seules personnes autorisées de l'étude (chèques, lettres chèques, courriers à en-tête, …).
- Renseigner son ordre de virement avec attention.
- Ne jamais communiquer ses coordonnées bancaires par téléphone.
- Ne pas faire figurer un RIB en pied de page d'un courrier, d'un courriel ou sur son site professionnel.
- En cas de communication d'un nouvel IBAN, assurez-vous auprès de votre créancier de la véracité des informations communiquées sur la base des renseignements détenus par l'étude (suspicion d'usurpation d'identité ou piratage de boîte mail).
- Réaliser une vigilance particulière sur les virements internationaux.

BON À SAVOIR

Emission d'un virement

Contrôler la source de l'IBAN destinataire d'un virement en réalisant un appel de contrôle par un canal de confiance.

Réception d'un virement:

Vos coordonnées bancaires comportent l'intitulé de la Caisse des Dépôts avec le **code banque 40031** et le **code BIC : CDCGFRPPXXX**

La carte bancaire

Les principaux cas

L'utilisation frauduleuse suite à la perte ou le vol de la carte bancaire ou le détournement des données.

Comment réagir ?

- Faites immédiatement opposition dès que vous constatez la perte, le vol ou toute utilisation non autorisée de votre carte ou de ses données en appelant le **centre national d'opposition** au **0892 705 705**. Un numéro d'opposition vous sera transmis.
- Déposer plainte auprès de la police ou de la gendarmerie.
- Contactez votre gestionnaire bancaire pour constituer le dossier de remboursement. Le délai de prévenance pour la prise en charge d'une opération non autorisée est de 13 mois pour un paiement dans l'Espace économique Européen et de 70 jours hors EEE).

L'utilisation frauduleuse sans dépossession de la carte bancaire

- Signalez la fraude bancaire auprès de la plateforme Percev@l du ministère de l'intérieur (service-public.fr) en fournissant le numéro d'opposition, le numéro de carte bancaire et les relevés bancaires. Cette demande sera traitée par la gendarmerie nationale et sert à simplifier les enquêtes.
- Uniquement dans ce type de fraude, la déclaration sous Percev@l est suffisante pour initier un dossier de remboursement.

Préconisations

- Ne mentionnez jamais vos données personnelles ou vos numéros de carte bancaire dans un courriel, même envoyé à un proche.
- Ne répondez jamais à un courriel vous demandant des informations personnelles ou vos numéros de carte bancaire.
- Sauf si vous en avez absolument besoin, n'utilisez jamais d'ordinateur public pour faire un achat sur internet.
- Désactivez le sans contact hors de la zone SEPA.
- Regardez régulièrement vos relevés de compte pour vérifier les paiements qui y sont passés.
- Consultez fréquemment la situation de votre compte sur votre espace CDC-Net.

BON À SAVOIR

La commande d'une nouvelle carte bancaire après une mise en opposition pour perte ou vol est automatique.

Les chèques

Les principaux cas

- **La perte ou vol de chéquier**
- **La falsification d'un chèque** (montant, nom du bénéficiaire, signature…)
- **Faux chèque** (produit à partir d'un vrai chèque)

Comment réagir ?

- En cas de perte ou de vol de votre chéquier, vous devez faire opposition au plus tôt auprès de votre gestionnaire afin de refuser le paiement d'un chèque qui se présenterait.
- Déposez plainte pour utilisation frauduleuse au commissariat de police ou à la gendarmerie.

Cas spécifique du chèque falsifié non encore encaissé

Demander une lettre de désistement au bénéficiaire ou le cas échéant faire une lettre de garantie en plus des deux précédentes actions.

Préconisations

Prévenir la fraude

- Pour le règlement de montant élevés, privilégier un autre moyen de paiement que le chèque, tel que le virement.
- Sécuriser la conservation des formules de chèque.
- Ne pas signer par avance les formules de chèque vierge.
- Limiter le nombre de chéquiers.
- Signaler toute perte ou vol de chéquiers à votre gestionnaire.
- Tenir sa comptabilité à jour (ex : faire mensuellement les rapprochements bancaires, et consulter de façon régulière le relevé de compte …).
- S'assurer auprès du bénéficiaire de la bonne réception du chèque.

Se prémunir contre la falsification un chèque

- Privilégier l'utilisation d'un stylo à bille à encre noire.
- Ne laisser aucun espace devant les sommes en chiffres et en lettres et laissez le minimum d'espace entre les chiffres et les mots, tirer un trait horizontal pour compléter la ou les lignes.
- Si le chèque est rempli par une machine, vérifier et signer après s'être assuré de la lisibilité et de l'exactitude des mentions portées par la machine et de la présence du nom du bénéficiaire.
- En cas de doute sur un chèque, réaliser un examen des mentions portées, ainsi que de leur cohérence avec l'identité du payeur.

BON À SAVOIR

En raison du secret bancaire, les coordonnées de la personne qui a encaissé le chèque falsifié ne peuvent être communiquées.

Le prélèvement

Les principaux cas

- Le créancier fraudeur s'enregistre en tant qu'émetteur de prélèvement auprès d'un prestataire de services de paiement et émet massivement des prélèvements vers des IBAN qu'il a obtenus illégalement et sans aucune autorisation.
- Le débiteur fraudeur communique à son créancier les coordonnées bancaires d'un tiers lors de la signature du mandat de prélèvement et bénéficie ainsi du service, sans avoir à en honorer les règlements prévus.

Comment réagir ?

- Contestez le prélèvement non autorisé en contactant votre gestionnaire bancaire. Le délai de contestation pour un prélèvement sur lequel vous n'avez signé aucun mandat est de 13 mois dans l'espace économique européen.
- Déposer plainte auprès de la police ou de la gendarmerie.

Préconisations

Prévenir les attaques informatiques

- S'équiper et maintenir à jour la sécurité de vos systèmes informatiques sur l'ensemble des outils professionnels, protéger ses mots de passe et identifiants de connexion.
- Communiquer à votre banque vos nouvelles coordonnées lors de changements intervenus dans l'étude (adresse postale ; mail , personnes habilitées…).
- Accentuer la vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir et les week-ends.

Prévenir les cas de détournement

- Vérifiez vos comptes régulièrement. Si vous constatez un prélèvement douteux, contactez rapidement votre gestionnaire bancaire.
- Maitrisez vos autorisations de prélèvements en établissant des « listes blanches » et « listes noires » de créanciers. Les services bancaires vous adresseront un formulaire de demande de liste blanche et liste noire d'identifiant créancier SEPA (ICS).

Sécurisez vos opérations avec l'authentification forte HID Approve

HID Approve: l'authentification forte

HID Approve est la solution d'authentification forte privilégiée par la Banque des Territoires, pour répondre à l'ensemble des exigences de la réglementation DSP2.

- HID Approve garantit un niveau de sécurité élevé et contribue à lutter contre la fraude.
- HID Approve vous permet de vous authentifier et de valider vos opérations en toute simplicité.
- Authentifiez-vous en définissant le code de votre choix et activez si vous le souhaitez la fonctionnalité de reconnaissance digitale ou faciale de votre smartphone.

Pour vous enrôler à HID Approve

- Mettez à jour vos coordonnées sur la Banque en Ligne (courriel principal et téléphone principal).
- Téléchargez l'application HID Approve sur votre smartphone ou tablette via Google Play ou l'App Store.
- Enrôlez-vous à HID Approve depuis votre espace Banque en ligne CDC-Net dans le menu "Mon Authentification Forte".

Pour en savoir plus

Découvrez HID Approve en images

Consultez le mode d'emploi

Nos solutions d'encaissement en ligne par carte bancaire

Monétique accepteur : nos solutions d'encaissement en ligne par carte bancaire

Nous proposons des solutions monétiques simples vous permettant d'encaisser des flux de paiement par carte bancaire via un portail sécurisé. Vous pouvez ainsi offrir à vos clients et parties prenantes un paiement plus moderne, plus souple et plus sûr que les espèces ou le chèque, et cela que vous disposiez ou non d'un site Internet.

L'offre paiement en ligne comprend deux services distincts, au choix :

- SP Plus (module de paiement en ligne ajouté à votre site Internet),
- JPEL (lien vers un formulaire d'encaissement sécurisé, sans besoin de site Internet).

Ces services monétiques sont souscrits auprès de nos équipes implantées dans les territoires, et l'intégration informatique est prise en charge par votre direction informatique ou votre prestataire.

Paiement en ligne pour les professions juridiques

Afin de faciliter le quotidien des professions juridiques, nous avons prévu que l'offre monétique SP Plus puisse être directement intégrée au sein des plateformes utilisés dans les études :

- Prisme, Genapi pour la clientèle notariale,
- iQera pour les huissiers de justice,
- Fiducial / NeoPay pour les huissiers de justice et commissaires priseurs judiciaires.

Notre solution SP Plus est parfaitement compatible avec les sites internet des partenaires logiciels. Les fonds encaissés sont directement versés sur votre compte Caisse des Dépôts qui bénéficie des règles de sécurisation des fonds de tiers réglementés.

Contacter un interlocuteur

Sécurisez l'encaissement de vos chèques

Encaisser un chèque grâce à notre prestation de Télétransmission de Lignes Magnétiques Chèques

Notre solution de Télétransmission de Lignes Magnétiques Chèques (TLMC) vous permet d'encaisser un chèque rapidement et de manière totalement sécurisée.

Un traitement numérisé pour optimiser le délai de traitement des chèques

Notre solution TLMC vous permet d'optimiser le délai pour encaisser un chèque grâce à :

- une gestion en un seul fichier des remises à imputer sur un ou plusieurs comptes,
- une gestion intégrée à la banque en ligne,
- une numérisation rapide grâce à la location de scanner de chèques et son logiciel de capture haute précision,
- un endossement automatique et traitement des coupons en option.

Des remises de chèques archivées pour plus de sécurité

- Reconstitution facilitée des remises via le fichier télétransmis en cas de perte ou vol.
- Archivage et consultation en ligne des remises effectuées.
- Des fonds immédiatement visibles sur votre compte.

Les fonds sont visibles et utilisables dès la transmission du fichier TLMC

La date de valeur est garantie à J+1 à la remise du fichier TLMC.

Contacter un interlocuteur

BANQUE des TERRITOIRES

Caisse des Dépôts GROUPE

banquedesterritoires.fr

@BanqueDesTerr

Direction de la communication du groupe Caisse des Dépôts - octobre 2021 - 21 147