



BANQUE des
TERRITOIRES



Guide Client Fraudes aux opérations bancaires

Comment réagir ?



BANQUE des
TERRITOIRES



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.

[banquedesterritoires.fr](https://www.banquedesterritoires.fr)

  | @BanqueDesTerr



Les types de fraudes au virement

Le faux RIB

 Suite au piratage de l'une des boîtes mail le RIB envoyé par mail est falsifié par le fraudeur. Le virement est envoyé à tort vers le compte du fraudeur et le bénéficiaire initial du virement ne reçoit rien et se manifeste auprès de vous.

Le phishing et le malware

 Le phishing est l'envoi d'un mail ou sms contenant un lien ou une pièce jointe cachant un malware ou renvoyant à une fausse page de connexion dans le but de récupérer vos données personnelles

Le malware est un logiciel malveillant Il pénètre votre ordinateur à votre insu et il est capable de menacer la sécurité de l'appareil et des données qu'il contient

Préconisations :

- 
- Débranchez la clé Real systématiquement dès que l'ordinateur n'est pas utilisé.
 - Ne cliquez sur une pièce jointe que si l'émetteur est connu et que le contenu semble cohérent.
 - Les communications emailing envoyées depuis la Banque des Territoires, doivent toujours comporter dans le domaine (la partie à droite du @) :
 - ✓ @service.banquedesterritoires.fr
 - ✓ @information.banquedesterritoires.fr
 - ✓ @infos.banquedesterritoires.fr
 - ✓ @caissedesdepots.fr

Comment réagir ?

- 
- En cas de suspicion de fraude contactez votre gestionnaire pour que vos comptes puissent être mis sous surveillance (pour les débits). Cette surveillance pourra être levée quand dès que le danger sera écarté.
 - Demandez 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)



Les types de fraudes au virement



La fraude au faux technicien Caisse des dépôts

L'escroquerie au faux technicien CDC consiste pour l'escroc à se faire passer pour un agent de la CDC. Il prétexte un dysfonctionnement technique pour parvenir à récupérer les codes d'accès et de validation de la banque en ligne.



Préconisations :

- Ne communiquez pas vos codes d'accès de la Banque en ligne
- Ne réalisez pas de test à la demande d'un technicien qui n'a pas été sollicité, ne validez pas de transaction ou de remise à sa demande
- Refusez la prise en main à distance de son PC. La CDC ne vous en fera jamais la demande
- Ne cliquez pas sur un lien inconnu

La fraude au Président

Le fraudeur utilise l'usurpation d'identité pour faire pression sur un salarié en charge des finances de l'entreprise (ex. comptable) et en se faisant passer pour un supérieur hiérarchique. Il utilise le caractère urgent et confidentiel de sa demande pour éviter tout soupçon et envoyer un ordre de virement insoupçonnable.

Préconisations

- Sensibilisez vos collaborateurs au risque de fraude au virement bancaire
- Effectuez un contre appel en cas de doute
- N'effectuez pas de virement dans l'urgence
- Généralisez l'utilisation de mots de passe plus complexes

Comment réagir ?

- En cas de suspicion de fraude contactez votre gestionnaire pour que vos comptes puissent être mis sous surveillance (pour les débits). Cette surveillance pourra être levée quand dès que le danger sera écarté.
- Demandez 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)
- En cas d'e-escroqueries (phishing, malware...) signaler l'infraction sur [THESEE](#)





Les principaux cas

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

Préconisations

- Ne mentionnez jamais vos données personnelles ou vos numéros de carte bancaire dans un courriel, même envoyé à un proche
- Sauf si vous en avez absolument besoin, n'utilisez jamais d'ordinateur public pour faire un achat sur internet
- Ne validez pas un paiement dont vous n'êtes pas à l'origine
- Désactivez le sans contact hors de la zone SEPA

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**.
- Déposez 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.



EN
A
SAVOIR

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

L'utilisation frauduleuse sans dépossession de la carte bancaire

- Signalez la fraude bancaire auprès de la plateforme Percev@I du ministère de l'intérieur en fournissant le numéro d'opposition, le numéro de carte bancaire et les relevés bancaires. Cette demande sera traitée par la gendarmerie nationale.
- Dans ce type de fraude, la déclaration sous Percev@I est suffisante pour initier un dossier de remboursement



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)

Préconisations

Prévenir la fraude

- Pour le règlement de montant élevés, privilégier un autre moyen de paiement que le chèque, tel que le virement
- Signalez toute perte ou vol de chèquiers à votre gestionnaire
- Tenez votre comptabilité à jour
- Assurez-vous auprès du bénéficiaire de la bonne réception du chèque

Se prémunir contre la falsification un chèque

- Privilégiez l'utilisation d'un stylo à bille à encre noire
- Ne laissez 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, vérifiez et signez 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, réalisez un examen des mentions portées, ainsi que de leur cohérence avec l'identité du payeur

BOB À SAVOIR

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



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. Vous disposez d'un délai de 60 jours pour le contester. La banque de contre partie a l'obligation de rembourser la CDC et votre compte sera recredité.
- Déposez plainte pour utilisation frauduleuse au commissariat de police ou à la gendarmerie.

Cas spécifique du chèque falsifié non encore encaissé

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



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.

Préconisations

Prévenir les attaques informatiques

- Equipez-vous et maintenez à jour les systèmes de sécurité informatiques sur l'ensemble des outils professionnels, protégez vos mots de passe et identifiants de connexion
- Communiquez à votre banque vos nouvelles coordonnées lors de changements intervenus dans l'étude (adresse postale, mail, personnes habilitées...)
- Accentuez 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.
- Maîtrisez 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)

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
- Déposez plainte auprès de la police ou de la gendarmerie

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

Sécurisez vos paiements en ligne avec AKARI

AKARI : réglez vos achats en ligne par carte en toute sécurité

AKARI est une application mobile qui vise à valider avec une sécurité renforcée vos paiements en ligne réalisés au moyen d'une carte bancaire Caisse des Dépôts. L'authentification forte permet ainsi de sécuriser davantage les opérations et se substitue au code à usage unique reçu par SMS sur mobile. Cette solution garantit l'authentification renforcée, participe à lutter contre la fraude et vient fluidifier et sécuriser votre expérience de paiement.

[Téléchargez le guide de l'application
AKARI](#)

[Téléchargez la notice AKARI](#)

Validlban
solution SEPAm@iDIAMOND

Validlban (solution SEPAm@iDIAMOND) : un service de vérification des coordonnées bancaires.

Face à la recrudescence des fraudes, **Validlban** vous permet de sécuriser vos virements et vos émissions de prélèvements grâce à l'authentification des coordonnées bancaires

Notre offre pour sécuriser vos virements et prélèvements

Le service en ligne **Validlban** permet de vérifier l'authenticité des coordonnées bancaires en assurant un contrôle du format du relevé d'identité bancaire et de sa correspondance avec le nom du titulaire du compte.

L'outil interroge directement la source la plus fiable disponible, à savoir les référentiels des banques adhérentes. Avec ce système, vérifier un identifiant bancaire devient simple et rapide. Un service de vérification par lot est également disponible.

Validlban vous sécurise ainsi dans vos transactions au quotidien :

- Lutte contre la fraude (usurpation d'identité)
- Exécution des virements avec des coordonnées bancaires fiabilisés
- Diminution des rejets de prélèvements bancaires
- Fiabilisation des bases clients, bénéficiaires
- Réduction des erreurs de saisies
- Diminution du risque d'être appelé en responsabilité (en cas de litiges).



Seule les notaires et les administrateurs et mandataires judiciaires ont accès au service pour le moment. Validlban sera déployé auprès des autres professions en 2024.

Pour en savoir plus

[Découvrez Validlban](#)

[Consultez notre guide utilisateur](#)

Encaisser un chèque grâce à notre prestation Chèque+

Chèque+ 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 Chèque+ 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 Chèque+
- La date de valeur est garantie à J+1 à la remise du fichier Chèque+

Pour en savoir plus

[Découvrez Chèque+](#)

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)



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.

Pour en savoir plus

[Découvrez nos solutions d'encaissement en ligne](#)