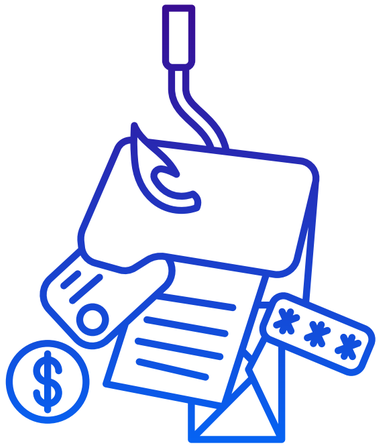
FRAUDES AUX OPÉRATIONS BANCAIRES

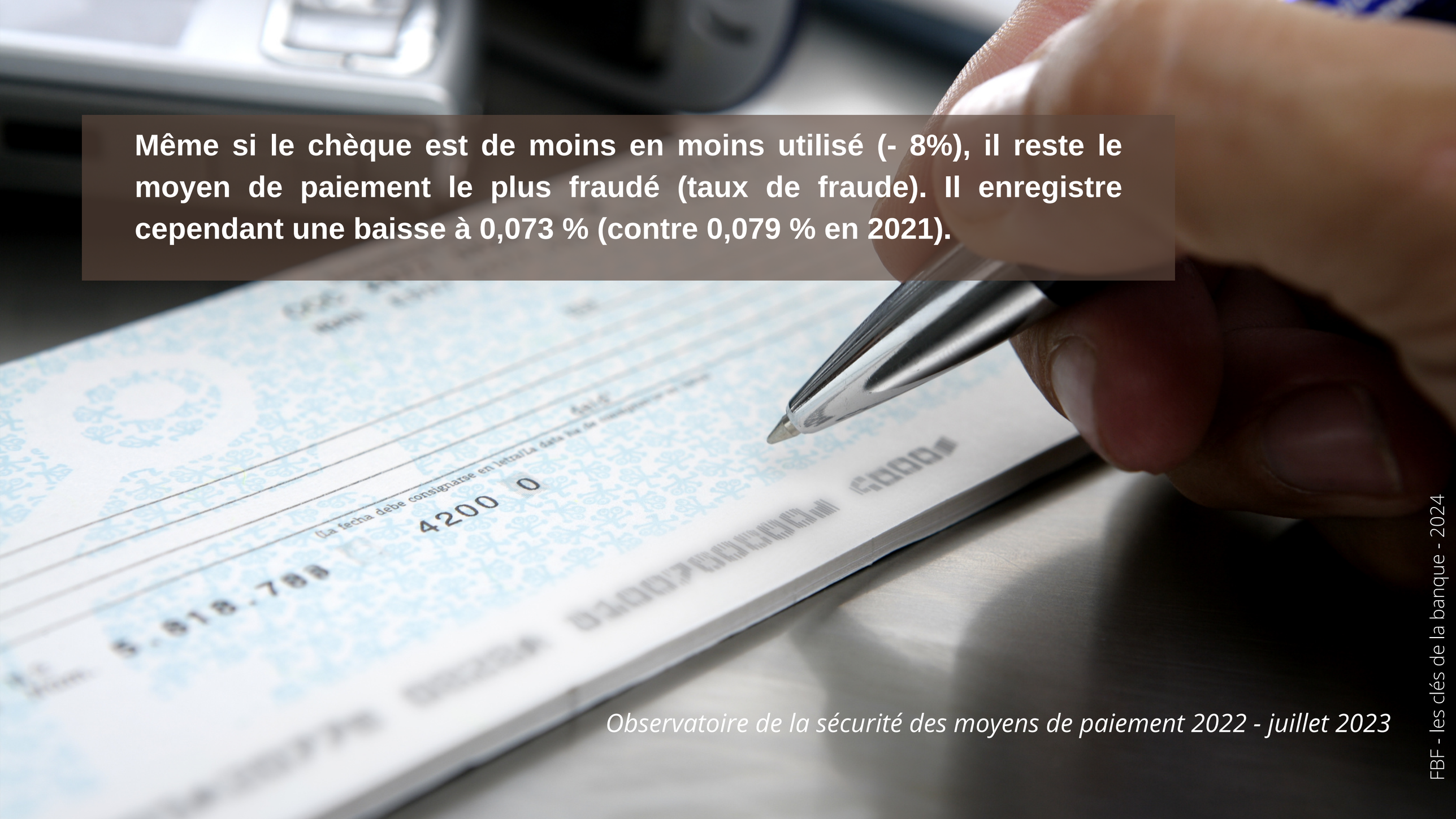
les clés de la banque

A votre avis ?

Quel moyen de paiement est le plus fraudé ?



- le chèque
- la carte paiement
- la carte retrait
- le prélèvement
- le virement



Même si le chèque est de moins en moins utilisé (- 8%), il reste le moyen de paiement le plus fraudé (taux de fraude). Il enregistre cependant une baisse à 0,073 % (contre 0,079 % en 2021).

Observatoire de la sécurité des moyens de paiement 2022 - juillet 2023

ÉVOLUTION DES FRAUDES EN 2022

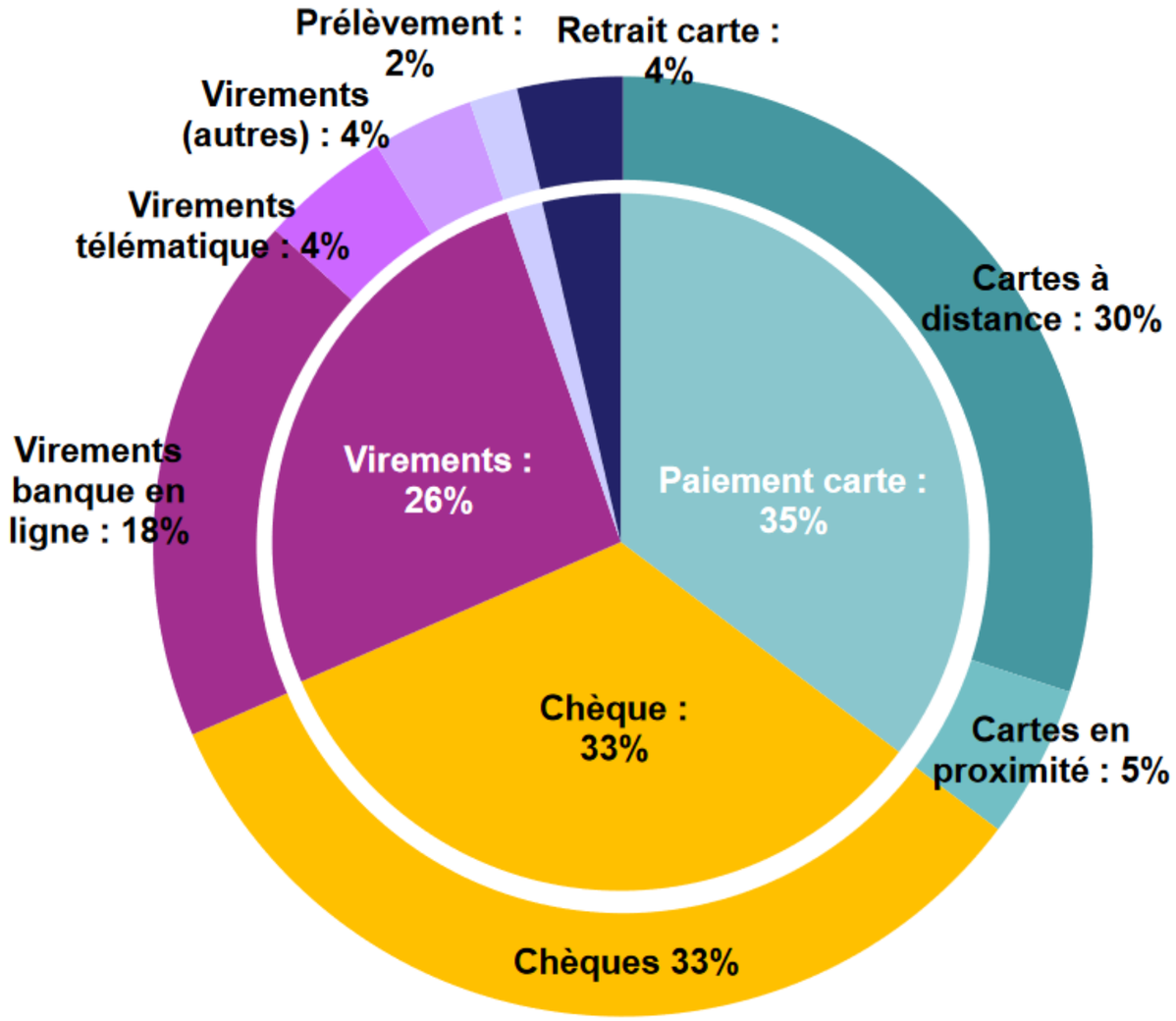
Au total, et malgré la croissance des flux, la fraude recule de 4 % en volume comme en valeur, pour revenir à 1,19 milliard d’euros de préjudice.

Les évolutions sont toutefois différenciées selon les moyens de paiement :

- 0,001% pour le virement (sur flux en hausse de 9%)
- 0,044 pour le virement instantané (sur flux en hausse de 85%)
- 0,053 % pour la carte (contre 0,059%)
- 0,073 % pour le chèque (contre 0,079%)

Observatoire de la sécurité des moyens de paiement 2022 - juillet 2023

Répartition de la fraude en valeur



A Noter :
Le taux de fraude le plus bas jamais enregistré sur les paiements internet, en baisse de 33% depuis 2019, grâce aux règles d'authentification forte

Observatoire de la sécurité des moyens de paiement 2022 - juillet 2023

Tendances 2023 - 1er semestre

Au premier semestre 2023, la fraude aux transactions scripturales s'est élevée à 628 millions d'euros pour 4,1 millions d'opérations frauduleuses, soit une augmentation en valeur de +5 % par rapport au premier semestre 2022.

Au 1er semestre :

- la carte reste le moyen de paiement le plus fraudé en valeur et sa part monte à 42 % (vs 35 %),
- la fraude sur le virement instantané progresse en valeur et représente aujourd'hui 5,2 %,
- le chèque reste l'instrument de paiement qui présente le taux de fraude le plus élevé et il remonte légèrement pour s'établir à 0,076 % (vs 0,073 %)

Observatoire de la sécurité des moyens de paiement 1er semestre 2023- janvier 2024

TYPOLOGIE

Les fraudes utilisent la palette d'émotions que peut ressentir tout individu...

la peur ...

de perdre de l'argent, perdre un droit, manquer une occasion...,

l'envie ...

de gagner de l'argent, faire mieux que les autres...,

la solidarité...

le besoin d'être utile, de participer à l'effort collectif...

Le canal utilisé peut être varié

Cumul possible + usage de l’IA (deepfake et clonage vocal)

- mail,
- faux site (phishing),
- appel vocal ou SMS, (vishing, spoofing, Smshing),
- QR Codes (quishing)
- réseaux sociaux...

Les escrocs profitent de l'actualité

- aide à l'Ukraine,
- prime carburant, chèque énergie,
- prime de rentrée, prime de partage de la valeur,
- promos, réductions et cartes avantages,
- placements garantis à haut rendement,
- prêt rapide et sans intérêt, etc.

Ils se font passer pour 1 organisme public ou 1 grande entreprise :

Pôle emploi (France Travail), CAF,
Total énergies, EDF,
les impôts ou encore la banque...

en usurpant leur d'identité :

logo, charge graphique, numéro de téléphone...

Tout message, appel ou publicité doit alerter s'il /elle présente :

1 caractère urgent,
1 gain rapide et/ou certain,
1 absence de risque,
1 facilité de mise en place,
1 gratuité, etc.

#1

LA FRAUDE AUX COORDONNÉES BANCAIRES

EN APPARENCE

VOUS RECEVEZ UN RIB

Un message de votre opérateur téléphonique ou fournisseur d'énergie... vous demande de faire désormais vos virements vers ses nouvelles coordonnées bancaires (RIB).

L'EXPÉDITEUR EST UN ESCROC

Il se fait passer pour votre bailleur, fournisseur ou autre créancier... et vous fait croire à un changement de RIB pour voler votre argent.
Il utilise souvent un mail proche de celui de votre interlocuteur habituel.

EN RÉALITÉ

LES BONS RÉFLEXES

VÉRIFIEZ AVANT D'AGIR

... que cette information
est vraie en contactant la personne
(ou organisme) au numéro de
téléphone (ou adresse) que vous
utilisez habituellement et non
celui du message qui est faux.

EN CAS DE DOUTE, CONTACTEZ VOTRE BANQUIER.

LESCLESDELABANQUE.COM

#7

LA FRAUDE AU FAUX CONSEILLER BANCAIRE

EN APPARENCE

VOTRE CONSEILLER VOUS APPELLE PAR TÉLÉPHONE

Le numéro affiché semble bien être le sien. Il vous alerte sur des opérations qu'il dit "anormales". Pour les annuler ou procéder à des vérifications, il vous demande d'agir directement sur votre téléphone ou de vous donner certaines informations.

C'EST 1 ESCROC QUI VOUS FAIT RÉALISER DES OPÉRATIONS

Au lieu d'annuler les opérations, vous en réalisez vous-même des nouvelles à son profit. Et si vous lui donnez des informations (cryptogramme, codes d'accès de banque à distance, ou code SMS de validation...) il pourra les réaliser lui-même.

EN RÉALITÉ

LES BONS RÉFLEXES

NE DONNEZ JAMAIS SUITE À UNE TELLE DEMANDE

Jamais votre banque ne vous demandera :
ni vos codes d'accès,
ni votre cryptogramme visuel de carte,
ni vos codes de validation.

"CODES, MOTS DE PASSE ET IDENTIFIANTS BANCAIRES :
NE DONNEZ JAMAIS CES DONNÉES"

LESCLESDELABANQUE.COM

ATTENTION : LES MÉTHODES ÉVOLUENT...

Les messages font souvent pression :

urgence, action rapide requise, pour gagner de l'argent ou éviter de perdre un droit etc.

Ils sont de + en + souvent rassurants :

notamment avec des infos fournies par la victime elle-même sur les réseaux sociaux ou via phishing par exemple : date de naissance, adresse, numéro de compte...

PRÉVENTION

LES MESSAGES CLÉS DE PRÉVENTION

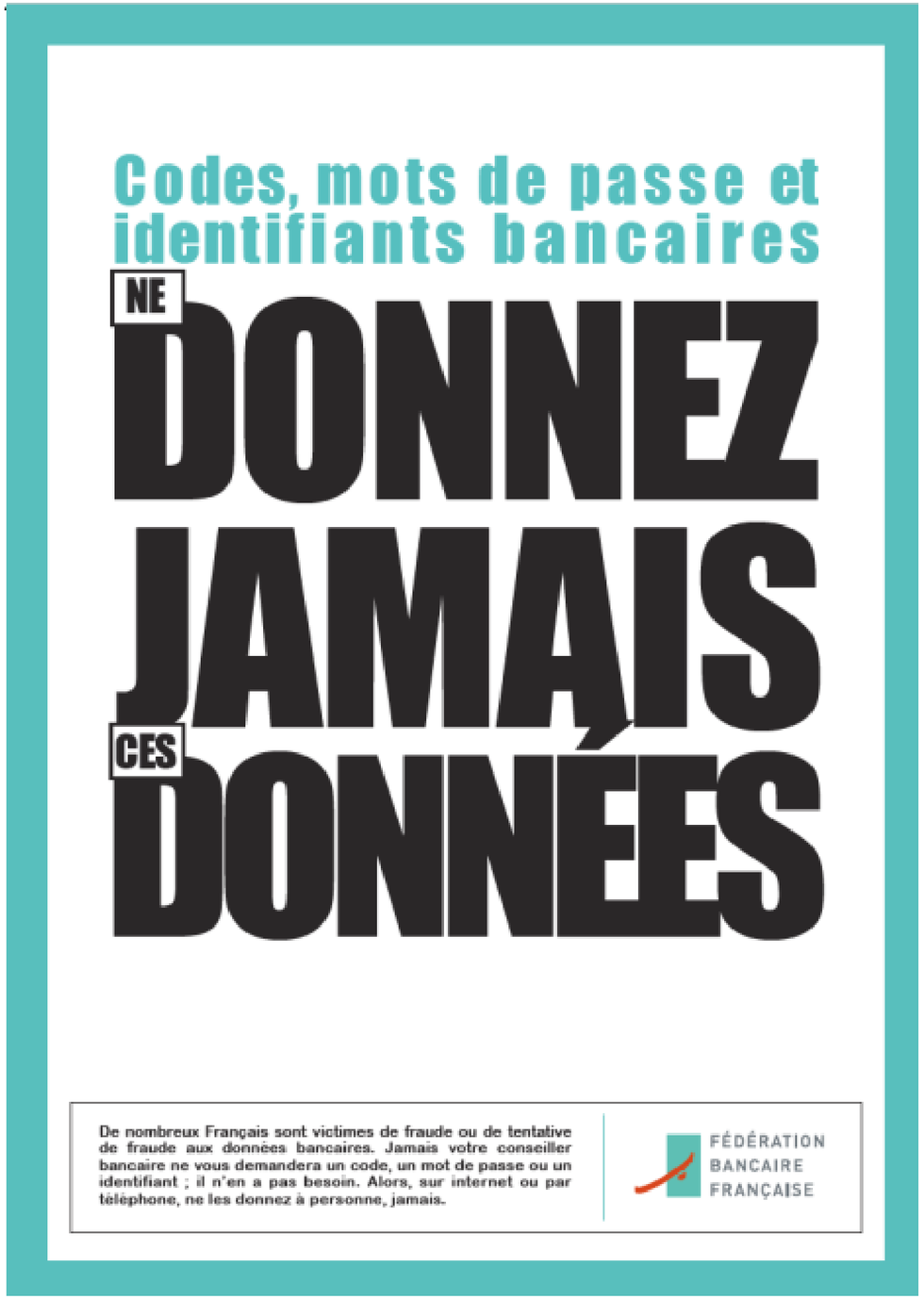
- Maîtriser la diffusion de ses **données personnelles**
- Ne pas donner ses **données bancaires,** ne pas noter ses **codes**
- Bien relire les **informations** avant de valider une opération : nature de l'opération, montant, bénéficiaire...
- Ne pas cliquer sur les **liens** surtout si mail inattendu et toujours utiliser la messagerie sécurisée de sa banque à distance
- Ne donnez jamais mots de passe, cryptogramme de carte, codes de validation...
- **consulter** régulièrement son **compte** pour repérer anomalie et contester

LES RÉFLEXES FACE AUX TENTATIVES DE FRAUDE

- garder **sang-froid** et **bon sens**, prendre le temps d'analyser
- **en parler** autour de soi, un regard extérieur peut éclairer rapidement
- se renseigner de son côté pour conforter l'information ou la démarche ex : sur son moteur habituel "mots clés clés + arnaque"
- ne pas divulguer de renseignements par téléphone si pas soi-même à l'initiative
- s'**abstenir** d'agir ou de répondre si le moindre doute subsiste
- **ne jamais donner codes d'accès à la banque, données carte, mots de passe**…
- contacter rapidement la banque via le canal habituel pour signaler

CAMPAGNE NATIONALE

en presse quotidienne régionale
en radio
2 vagues : avril et octobre 2023 /2024



LA PROFESSION BANCAIRE SE MOBILISE
NOTAMMENT CONTRE LE SPOOFING

Action en cours vis-à-vis des opérateurs télécom pour veiller à la bonne application de la loi Naegelen encadrant le démarchage téléphonique et à lutter contre les appels frauduleux.

- Amélioration des parcours clients avec des notifications claires sur les actions en cours.

- Revue des parcours : paiement carte, virement, augmentation de plafond, ajout de bénéficiaire. Chacun de ces parcours se conclut par :
  - « J’autorise ce [nom de l’opération] ex paiement carte »
  - « Je refuse ce [nom de l’opération] ex virement »

REMBOURSEMENT

COMMENT DEMANDER 1 REMBOURSEMENT ?

- Se rapprocher de son **conseiller bancaire** pour démarches selon moyen de paiement

- **Fournir tous les éléments** de la fraude à la banque comme aux autorités de police ou gendarmerie > Caractère « non autorisé » de la transaction déterminant pour obtenir remboursement

- Réaliser démarches de **blocage** du moyen de paiement, **signaler** la fraude via Perceval ou Thésée (site service public), **déposer plainte** pour participer aux efforts de lutte et interpeller les escrocs

Absence de plainte = absence d'enquête = impunité pour les fraudeurs
= Poursuite des activités frauduleuses au détriment d'autres victimes

TRAITEMENT DE LA DEMANDE PAR LA BANQUE

- Chaque banque s'organise pour apprécier la situation **au cas par cas** (circonstances et type de fraude) et en assurer le traitement.

- En 1 jour ouvré : **1ère analyse** de l’opération pour déterminer si l’opération doit faire l’objet d’un remboursement (ou pas).

- La banque peut être amenée à approfondir ses recherches pour valider sa décision. Elle peut donc être amenée à récupérer les fonds si elle avait remboursé à J+1.

- Examen des éléments susceptibles d’avoir altéré l’authentification forte, tels que origine de la transaction, terminal utilisé, localisation géographique... pour apprécier le consentement

QUIZ

VRAI / FAUX

	V	F
Pour ne pas se faire avoir, une bonne formation suffit	☐	☐
Les escrocs utilisent le plus souvent des failles techniques.	☐	☐
L'authentification forte ou "double" a supprimé tous les grands types de fraude.	☐	☐
Le dépôt de plainte n'est pas obligatoire pour pouvoir être remboursé par la banque.	☐	☐

VRAI / FAUX

	V	F
Pour ne pas se faire avoir, une bonne formation suffit	☐	☒
Les escrocs utilisent le plus souvent des failles techniques.	☐	☒
L'authentification forte ou "double" a supprimé tous les grands types de fraude.	☐	☒
Le dépôt de plainte n'est pas obligatoire pour pouvoir être remboursé par la banque.	☑	☐

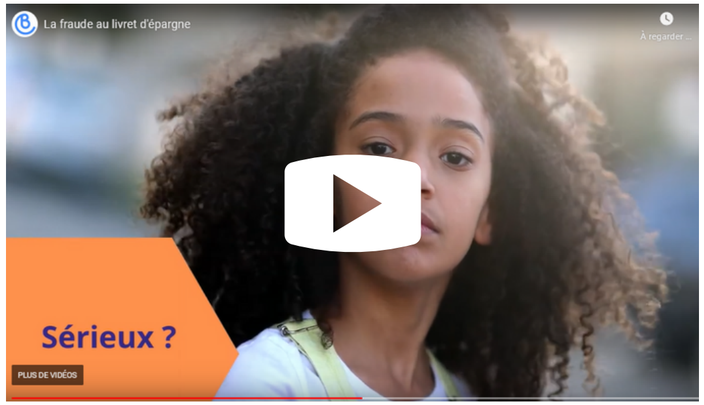
Mini-guides

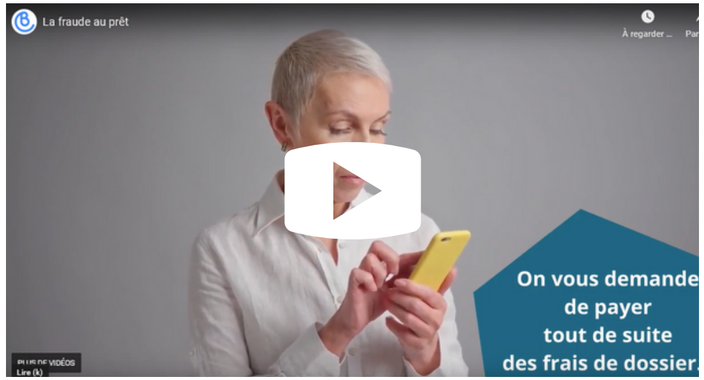
Vidéos

Infographies

Modèles de lettres

Liens utiles





LESCLESDELABANQUE.COM

Ce module a été conçu par les clés de la banque, le programme d'éducation financière de la Fédération bancaire française.
A vocation pédagogique, il ne constitue pas une référence juridique. Toute reproduction totale ou partielle est subordonnée à l'accord formel de la FBF.