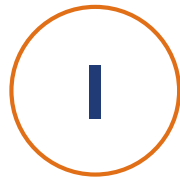


# LES ARNAQUES FINANCIÈRES : ÇA N'ARRIVE PAS QU'AUX AUTRES !



# SOMMAIRE



De quoi parle-t-on ?



Comment se protéger ?



Comment réagir ?

# DE QUOI PARLE-T-ON ?

## La Minute Cash – Épisode 5 : Arnaques



# LA FRAUDE AUX MOYENS DE PAIEMENT



Fraude aux  
virements



Fraude à la carte

Fraude aux chèques

# LA FRAUDE AUX MOYENS DE PAIEMENT

## Quelques chiffres

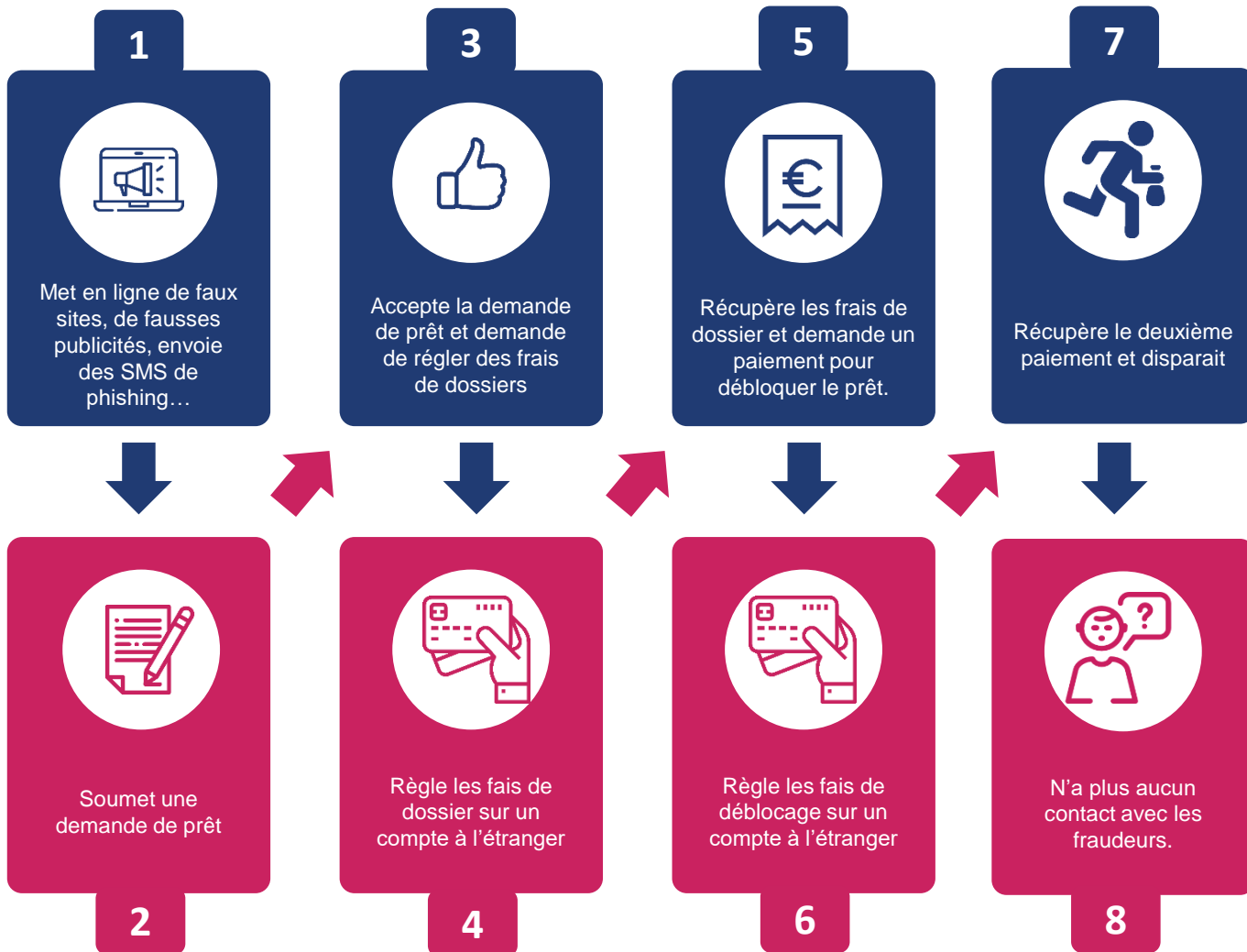
Une fraude annuelle sur les paiements scripturaux : **1,192 milliard d'euros**, soit l'équivalent de **18 € par habitant et par an**.

Dont :

- Chèques : **395 millions d'euros**
- Cartes : **464 millions d'euros**
- Virements : **313 millions d'euros**



# LE MÉCANISME DE L'ARNAQUE AU CRÉDIT



# LES ARNAQUES À L'ÉPARGNE

Les livrets

Les investissements / les placements

Le trading en ligne

Bitcoin et autres crypto actifs

Les biens divers



# LES ARNAQUES À L'ÉPARGNE

**BOOSTEZ VOTRE ÉPARGNE**

INVESTIR EN TOUTE TRANQUILITÉ  
Rendement 8 fois supérieur au Livret A

**Demande d'informations**

Nom \*  
 Prénom \*  
 Email \*  
 Téléphone \*  
 Année de Naissance \*

**ENVOYER**

\* Conformément à la loi informatique et libertés de 08 janvier 1978, je précise que vos données et de renseignements que j'envoie en remplissant ce formulaire sont destinées à traiter votre demande.

**TRADEZ LES CRYPTO-MONNAIES !**

Les Crypto-Monnaies sont les instruments de trading les + rentables au monde à trader !

Tradez en toute sécurité sur une plateforme régulée dans l'UE (Autorité Européenne / Autorité des Aires)

Un Service Client 24h/24 dans + de 10 langues.

▶ Essayer la démo gratuite ▶ Tradez les Cryptomonnaies

Tradez en toute sécurité avec un Co-trading Régulé dans l'Union Européenne.

**TRADEZ L'OR**

999.9 FINE GOLD

NEWVT 000010000

**Boostez votre épargne**

Rendement **10** fois supérieur au livret A

**Demande d'informations**

Nom

Prénom

Adresse e-mail



**OBTENEZ VOTRE CRÉDIT DE 500€ À 1.000.000€ EN 48 HEURES EN EFFECTUANT VOTRE DEMANDE DÈS MAINTENANT**

UN CRÉDIT VOUS ENGAGE ET DOIT ÊTRE REMBOURSÉ. VÉRIFIEZ VOS CAPACITÉS DE REMBOURSEMENT AVANT DE VOUS ENGAGER.

**Obtenez jusqu'à 5 000 € de bonus**

**Investir maintenant**

\* Le trading implique des risques de pertes

**Tradez sur le Forex**

Bonus sur dépôt jusqu'à 200 €  
Les conditions générales s'appliquent

**Télécharger maintenant**

**Plus500**

**Solution Épargne à 3,92% par an pour remplacer votre livret A !**

Facile, rapide, sécurité 100% gratuite

Vérifiez votre éligibilité !

Recevez votre étude personnalisée en ligne !

**L'INVESTISSEMENT LOCATIF EN IMMOBILIER DE PARKING UN PLACEMENT QUI PEUT VOUS RAPPORTEER JUSQU'À 14% PAR AN**

**Devenir propriétaire d'une place de parking**

Contactez nous pour recevoir le guide et notre conseiller répondra à toutes vos questions.

Votre Nom \* Prénom \*  
 Votre Adresse Email \* Téléphone \*

**Je souhaite m'inscrire !**

**L'ÉPARGNE NOUVELLE GÉNÉRATION**

Profitez d'un taux exceptionnel sur votre Livret d'Épargne :

**6% ET 40€ OFFERTS** pour les 1500 premiers inscrits

**POUR BÉNÉFICIER DE CETTE OFFRE, INSCRIVEZ-VOUS MAINTENANT**



# LES ARNAQUES À L'ÉPARGNE

## Quelques chiffres

Montant estimé des pertes subies par les Français victimes d'arnaques aux faux placements : **500 millions d'euros /an**

Source : Parquet de Paris

En avril 2023, plus de **6200 sites internet ou mails** sont répertoriés sur les listes noires gérées par l'ACPR et l'AMF.



# LES USURPATIONS D'IDENTITÉ

## Des individus

- **Voler une identité** pour souscrire des crédits, réaliser des opérations illégales
- Plus de **210 000 victimes par an en France** (Ministère de l'économie)

## Des institutions, banques, administrations

- **Tromper le destinataire** du message ou de l'appel téléphonique en prenant l'identité d'une entité officielle (CAF, impôts, banques, sociétés de livraison...) (« Spoofing »)



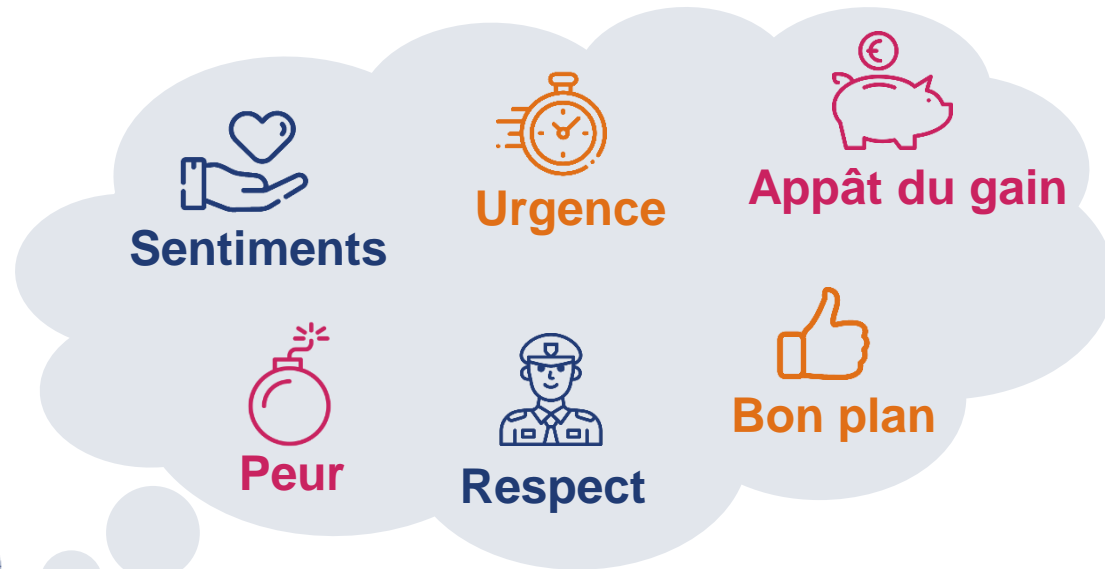
# LE PIRATAGE PSYCHOLOGIQUE OU « INGÉNIERIE SOCIALE »



- Le pirate tente de vous convaincre, par exemple:
  - De lui **remettre de l'argent**, par virement vers son compte
  - De **dévoiler des informations** qu'il exploitera ensuite, mot de passe, données personnelles etc.
  - De lui **donner accès à votre ordinateur** pour installer des logiciels malveillants.
- Il peut faire auparavant des recherches sur vous sur **les moteurs de recherche**, sur **les réseaux sociaux**.

# LE PIRATAGE PSYCHOLOGIQUE OU « INGÉNIERIE SOCIALE »

**Jouer avec vos émotions...**



**...pour vous empêcher de réfléchir**

# ET CE N'EST PAS FINI...

L'imagination des fraudeurs est sans limite...  
...et ils sont extrêmement opportunistes.



# SOMMAIRE



De quoi parle-t-on ?



Comment se protéger ?



Comment réagir ?

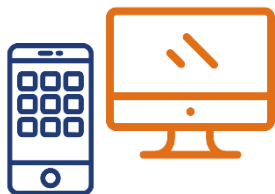
# PROTÉGER SES ÉQUIPEMENTS

- Installez les **mises à jour** (Windows, IOS, Android...)
- Installez des **logiciels de sécurité** (antivirus, anti spywares...)
- Activez le **pare feu** de votre équipement
- Faites des **sauvegardes** régulièrement
- Méfiez-vous des **WI-FI publics** !



# PROTÉGER SES ÉQUIPEMENTS

- Faites régulièrement la mise à jour :



Du système d'exploitation de votre pc et de vos mobiles



De votre logiciel antivirus



De votre navigateur Web



De vos applications et jeux

- Afin de :

Profiter de nouvelles fonctionnalités



Prévenir les cyber menaces



Corriger les dysfonctionnements





# ÊTRE UN INTERNAUTE AVISÉ



Choisissez des mots de passe difficiles à deviner



Changez vos mots de passe régulièrement



Utilisez des mots de passe différents, en utilisant un « portefeuille » de mots de passe



Au besoin, créez une adresse mail « poubelle »

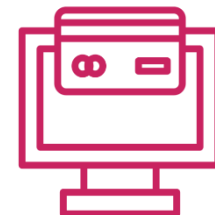
# ÉVITER LES FRAUDES À LA CARTE BANCAIRE

Protégez vos données (PIN, numéro, CVV)



Soyez vigilant sur un DAB, chez un commerçant

Utilisez prudemment votre carte en ligne



# ÉVITER LE PIRATAGE DE SON COMPTE BANCAIRE EN LIGNE





- **Privilégiez** les applications pour mobiles mises à disposition par les banques
- **Saisissez directement l'adresse** de la page d'identification de la banque dans le navigateur
- **Ne donnez jamais vos coordonnées bancaires** lorsque vous n'êtes pas à l'initiative d'une transaction

**Votre banque ne vous demandera **jamais** vos codes de sécurité ou mots de passe**

# APPRENDRE À DÉJOUER LE PHISHING



## Attention au phishing (hameçonnage par courriel)

- Observez bien l'email, l'adresse de réponse, celle des liens présents ...
- Évitez de cliquer sur des liens provenant de sources inconnues (préférer aller sur les sites internet directement par leur adresse url)
- Vérifiez la présence du cadenas et du « s » de https
  - Google Chrome :  google.fr
  - Firefox :  https://www.google.fr

## Mais prenez garde également :

- Aux liens dans les SMS (« Smishing ») ou sur les réseaux sociaux
- Aux appels téléphoniques frauduleux (« Vishing »)

# PHISHING : UN MESSAGE-TYPE

De : MaBanque <[securpass.MaBanque@orange.fr](mailto:securpass.MaBanque@orange.fr)> ? Attention à l'adresse mail !  
Objet : Avertissement  
Date : 25 juin 2023 à 9h23



Bonjour,

Grâce au service Secur'pass, vous pouvez sécuriser vos données de cartes bancaires.  
Ainsi, les risques d'utilisation frauduleuse de vos données lors de transactions en ligne sont limités.

Selon vos choix et vos besoins.

[Activez maintenant.](#)



Attention aux liens (Faire apparaître l'adresse en passant le curseur sur le lien SANS CLIQUER !)

Cordialement,  
Ma Banque



Situation de compte.pdf



Attention aux pièces jointes

MaBanque est une Société anonyme à directoire et conseil de surveillance au capital de 1 678 876 667 €  
Siège social : 45, rue Stine- 75002 Paris –  
RCS Paris N°345 628 019, Intermédiaire d'assurance immatriculé à l'Orias sous le N° 498 543 (www.orias.fr).



Même s'il n'y a pas de fautes, le niveau de langage du mail peut vous alerter

# COMMENT ÉVITER LA FRAUDE AUX CHÈQUES ?

Vol et détournement

Encaissement pour le compte de tiers



# LES USURPATIONS D'IDENTITÉ

## Comment protéger votre identité ?



- Ne jetez pas vos documents qui pourraient servir de justificatifs
- Vérifiez bien le destinataire à qui vous envoyez des documents
- Évitez de publier des informations personnelles sur internet et les réseaux sociaux
- Marquez les documents transmis en indiquant l'usage pour lequel vous les transmettez

Pour le marquage des documents, le service **filigrane.beta.gouv.fr** permet d'insérer un filigrane dans votre pièce d'identité ou tout autre document

Source image : <https://beta.gouv.fr/>



# DEJOUER LE PIRATAGE PSYCHOLOGIQUE

Jouer avec vos émotions...



- **Ne jamais agir avec empressement ou sous le coup de l'émotion**
- **Ne pas communiquer d'informations personnelles**
- **Appeler le numéro de téléphone officiel de la banque, de l'administration...**



# RECONNAÎTRE DES SIGNES DE FRAUDE À L'ÉPARGNE OU AU CREDIT



- Une offre trop belle
  - Rendements élevés, peu de risques
  - Taux faibles, pas de caution, pas de conditions de ressource
- Peu de renseignements précis sur le produit
- Une décision à prendre rapidement
- Des informations privilégiées
- Demande d'informations personnelles ou bancaires



→ L'AMF met à disposition du public, une application pour mobile et un site internet, destinés, entre autres, à vérifier si le consommateur est face à une arnaque.



# CONNAÎTRE QUELQUES VÉRIFICATIONS

## Les listes noires de l'AMF et de l'ACPR

- Crédits, livrets d'épargne, services de paiement ou contrats d'assurance ;
- Investissements sur le Forex (marché des changes) ;
- Produits dérivés sur crypto-actifs ;
- Options binaires ;
- Investissements dans des biens divers (diamants, vin, crypto-actifs,...).

## Les registres des acteurs autorisés

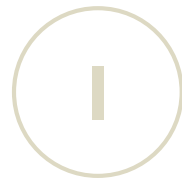
- Registre ORIAS : les intermédiaires CIF, IA, IOB
- Registre REGAFI : les agents financiers
- Registre REFASSU : les organismes d'assurance



## En cas de doute

- Prendre contact avec les autorités compétentes (ACPR, AMF, BDF)

# SOMMAIRE



De quoi parle-t-on ?



Comment se protéger ?



Comment réagir ?

# COMMENT RÉAGIR ?

## Face à des opérations frauduleuses



- **Réagissez rapidement**
  - Une consultation régulière de votre compte peut permettre de détecter un incident ou une anomalie
- **Faites opposition** à la carte bancaire piratée ou aux chèques falsifiés
- **Contestez rapidement** auprès de votre banque les opérations non autorisées ou mal exécutées, y compris des virements ou prélèvements
- **Portez plainte**

# COMMENT RÉAGIR ?



Si vous avez versé des fonds à un escroc

- **Contactez immédiatement votre banque**
  - Pour **bloquer le virement** s'il n'est pas trop tard;
  - Ou pour **demander le retour des fonds versés**, procédure dite de « recall » (Attention, le résultat n'est pas du tout garanti.)
- **Cessez tout contact avec votre interlocuteur**
  - Même si vous êtes relancés
- **Portez plainte en cas de montant important**
  - Pour maximiser les chances de retrouver les fonds détournés

# COMMENT RÉAGIR ?

Qu'est-ce que le « chargeback » ?



Une possibilité de **remboursement** en cas d'insatisfaction pour un **service ou un produit** acheté sur internet.



De nombreuses **conditions** :

- Avoir **payé par carte bancaire**,
- Disposer d'un **contrat prévoyant cette garantie**,
- Demander le remboursement **moins de 8 semaines** après le débit

# COMMENT RÉAGIR ?



## Face à une usurpation d'identité

- **Conservez** toutes les preuves en votre possession (captures d'écran, messages, adresses des pages Internet concernées, documents...) et **déposez plainte** (<https://www.pre-plainte-en-ligne.gouv.fr>)
- **Produisez une attestation sur l'honneur** disant que vous n'êtes pas l'auteur d'éventuels faits reprochés en joignant copie de la plainte.
- **Prévenez** tous vos établissements financiers et **signalez** l'usurpation aux plateformes sur lesquelles elle a eu lieu
- **Annulez et renouvelez** vos pièces d'identité utilisées par les escrocs.
- **Contactez** la Banque de France pour savoir si des incidents ont été déclarés à votre nom au FCC et/ ou au FICP
- **Consultez** le fichier FICOBA (auprès de la CNIL)

# COMMENT RÉAGIR ?



## Face à une usurpation d'identité

- Si un usurpateur **laissé un découvert** ou n'a **pas remboursé un crédit** souscrit en votre nom
  - Il faudra **démontrer votre bonne foi** à chaque établissement concerné, éventuellement en fournissant des **justificatifs additionnels**
  - **Alors seulement** votre responsabilité sera dérogée et une mention « usurpation » sera apposée sur d'éventuelles inscriptions FICP et/ou FCC
- **Une décision de justice peut établir l'usurpation, mais c'est une décision qui peut prendre beaucoup de temps**



# COMMENT RÉAGIR ?

## Quand porter plainte ?



- **En cas d'usurpation d'identité**
  - Pour être protégé en cas d'utilisation frauduleuse de votre identité
- **En cas de virement frauduleux d'un montant important**
  - Pour maximiser les chances de retrouver les fonds détournés
- **Et en tout cas**
  - Pour établir votre bonne foi
  - Pour faciliter l'identification des fraudeurs

# COMMENT RÉAGIR ?

## S'informer

- [www.mesquestionsdargent.fr](http://www.mesquestionsdargent.fr)
- [www.abe-infoservice.fr](http://www.abe-infoservice.fr)
- [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)



## Signaler

- [www.signal-spam.fr](http://www.signal-spam.fr)
- [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) (Pharos)
- [www.bloctel.gouv.fr](http://www.bloctel.gouv.fr)
- [www.signal.conso.gouv.fr](http://www.signal.conso.gouv.fr)



## Porter plainte

- [www.service-public.fr/](http://www.service-public.fr/) (THESEE)
- [www.pre-plainte-en-ligne.gouv.fr](http://www.pre-plainte-en-ligne.gouv.fr)



# COMMENT RÉAGIR ?

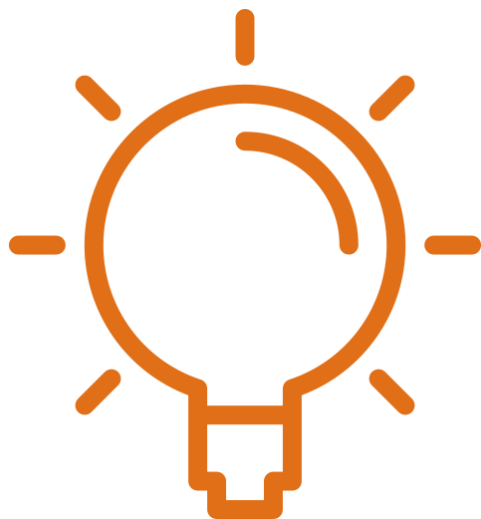
## Téléphones utiles



- **01 53 45 62 00** : « Épargne Info Service marchés »
  - Plateforme créée par l'AMF : du lundi au vendredi de 9h à 12h30 et de 13h30 à 17h (prix d'un appel local).
- **08 09 540 550** : DGCCRF, (appel gratuit)
- **0 805 805 817** : Info Escroqueries (appel gratuit)
- **116 006** : Aide aux victimes (appel gratuit)
  - Service qui permet aux victimes d'infractions, d'accidents ou catastrophes de bénéficier d'informations et d'une écoute par des professionnels.

# Face aux arnaques, ne manquez pas d'**R** !

**R**alentissez



**R**egardez

**R**éfléchissez

**R**éagissez



# Mes questions d'argent

Le portail national de l'éducation économique, budgétaire et financière



mesquestionsdargent.fr

# LA BANQUE DE FRANCE A VOTRE SERVICE :

## UN CORRESPONDANT INCLUSION FINANCIÈRE (CORIF) DANS CHAQUE DÉPARTEMENT

- Pour toute question ou de besoin de contact sur des cas individuels relatifs à :
  - La procédure de surendettement
  - La procédure de droit au compte
  - Les fichiers d'incidents
  - Le plafonnement des frais bancaires ou l'offre clientèle fragile
  - Les questions de réglementation bancaire ou d'assurance
  - Le microcrédit



Contactez le  
**CORRESPONDANT  
INCLUSION  
FINANCIÈRE**  
de votre  
département



PAR COURRIEL  
corifXX@banque-france.fr  
(XX : n° du département)



**3414** dites « CORIF »  
du lundi au vendredi de 8 h à 18 h  
Prix d'un appel local

Retrouvez ces informations sur notre site Internet : [www.banque-france.fr](http://www.banque-france.fr) (Espace particuliers)



**MERCI DE VOTRE  
ATTENTION**

*Ce document est la propriété exclusive de la Banque de France, opérateur national EDUCFI. Il est fourni gratuitement à titre purement informatif sans que cette mise à disposition entraîne un quelconque transfert des droits de propriété intellectuelle sur ledit document. Toute représentation ou reproduction intégrale ou partielle du document sans le consentement de la Banque de France constitue un délit de contrefaçon sanctionnée par les articles L 335-2 et suivants du Code de la propriété intellectuelle.*