

Levée de doute sur des opérations inhabituelles liées à la carte bancaire

Support de présentation



**CAISSE
D'ÉPARGNE**

Vous être utile.

CE QU'IL FAUT RETENIR SUR LA LEVEE DE DOUTE

En synthèse

Nouvelle fonctionnalité digitale qui permet au client de répondre à une alerte fraude carte bancaire

- Cette fonctionnalité vient en complément des processus actuels de gestion de la fraude : contact téléphonique et/ou sms **pour informer le client d'opérations cartes inhabituelles sur son compte depuis l'application bancaire « Banxo »**.
- Seuls les clients majeurs capables particuliers (< à 75 ans) et mineurs émancipés, utilisateurs de l'application Caisse d'Epargne et avec Sécur'Pass activé sont éligibles à ce nouveau parcours selfcare (alerte fraude automatique). Pour un client mineur ou plus de 75 ans, l'envoi de l'alerte carte en selfcare est à la main de la cellule fraude Caisse.

Le client est notifié sur son téléphone lorsqu'une alerte fraude carte est émise

- Cette alerte concerne une liste d'opérations inhabituelles (dont potentiellement certaines opérations ont été refusées)
- Le client a 3 choix :
 1. Il confirme qu'il est bien à l'origine de toutes les opérations, l'alerte est levée mais il devra renouveler ses achats (car certains refusés).
 2. Il signale une fraude car parmi la liste des opérations présentées, il n'est pas à l'origine d'une ou plusieurs opérations et fait opposition.
 3. Il souhaite mettre sa carte en usage limité pour pouvoir réaliser un retrait au DAB et/ou un paiement avec saisie du code avant de faire opposition. Dans ce cas, la carte est bloquée pour les paiements VAD et paiements mobile.

S'il ne répond pas à l'alerte, il continue d'utiliser sa carte, mais certaines opérations pourront encore à l'avenir être rejetées, si considérées comme inhabituelles par notre outil d'analyse de la fraude.

■ CONTEXTE

Objectifs de cette nouvelle fonctionnalité digitale

Grâce à la « Levée de doute », nos **Objectifs** sont de :



Satisfaire nos clients en leur proposant un parcours en selfcare en temps réel

Le client n'est plus systématiquement sollicité par contact téléphonique, il peut ainsi réagir plus vite et limiter la fraude.



Améliorer l'efficacité opérationnelle de lutte contre la fraude.

La gestion par le client en selfcare du traitement de la suspicion de fraude permettra de réduire les coûts de traitement côté middle office et d'améliorer l'expérience utilisateur.



Adresser environ une alerte fraude sur deux à ce nouveau parcours.

Parcours existant

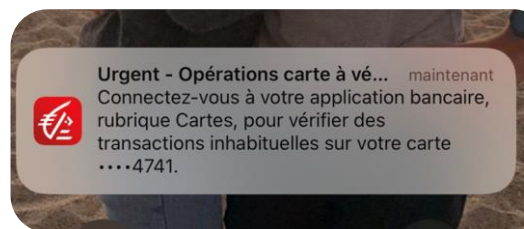
Comment le client constate-t-il une opération carte frauduleuse ?

- Soit en recevant **une alerte par SMS et/ou appel téléphonique** généré par la cellule fraude Caisse d'Epargne,
 - Soit en consultant le détail des opérations de son compte sur son **espace client Direct Ecureuil ou relevé de compte.**
- ⇒ Le Client peut mettre en opposition sa carte depuis l'espace client et/ou en sollicitant sa Caisse d'Epargne (Conseiller ou CRC).

QU'EST-CE QUE LA LEVEE DE DOUTE EN SELF CARE ?

Un nouveau parcours disponible depuis l'application Banxo

Un dispositif lutte contre la fraude permettant au client d'être informé et de réagir lorsqu'une ou plusieurs « **opérations cartes inhabituelles** » ont été détectées sur son compte.



Le client reçoit une **notification** sur son téléphone mobile l'invitant à se connecter à notre application Banxo



Le client pourra se prononcer pour une ou plusieurs **opérations inhabituelles** liées à sa carte bancaire

Maximum 5 jours pour réagir sinon l'alerte est clôturée !

Le client aura **5 jours calendaires** à compter de la réception de l'alerte pour se prononcer, à défaut il sera relancé à deux reprises via push + sms, puis via push + email.



Le client peut également accéder à son alerte fraude via la rubrique "**Carte**" dans l'application mobile, sur le visuel il est précisé « **limitée** », il pourra se prononcer.

QUELS CHOIX POSSIBLES ?

Illustration avec Margot qui vient d'être notifiée par notification push (hors application)



Choix 1

Margot déclare qu'elle est bien à l'origine des opérations carte.

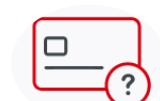
NB : Si certaines opérations sont refusées, il faudra qu'elle les renouvelle.



Choix 2

Margot déclare qu'elle n'est pas à l'origine des opérations et met sa carte en opposition

NB : Même si une seule opération est suspecte, il faut faire opposition !



Choix 3

Margot déclare qu'elle n'est pas à l'origine des opérations et décide de conserver un usage limité de sa carte. Cette limitation s'arrêtera lorsque la carte sera mise en opposition ou lorsque la date de fin de validité de la carte sera atteinte si Margot ne met pas sa carte en opposition.

(utilisation limitée qu'aux paiements et retraits avec saisie du code et opérations sans contact)

Cas d'une personne en voyage ou en déplacement, il est préconisé de faire opposition très rapidement si à minima une opération est suspecte.



Clients éligibles

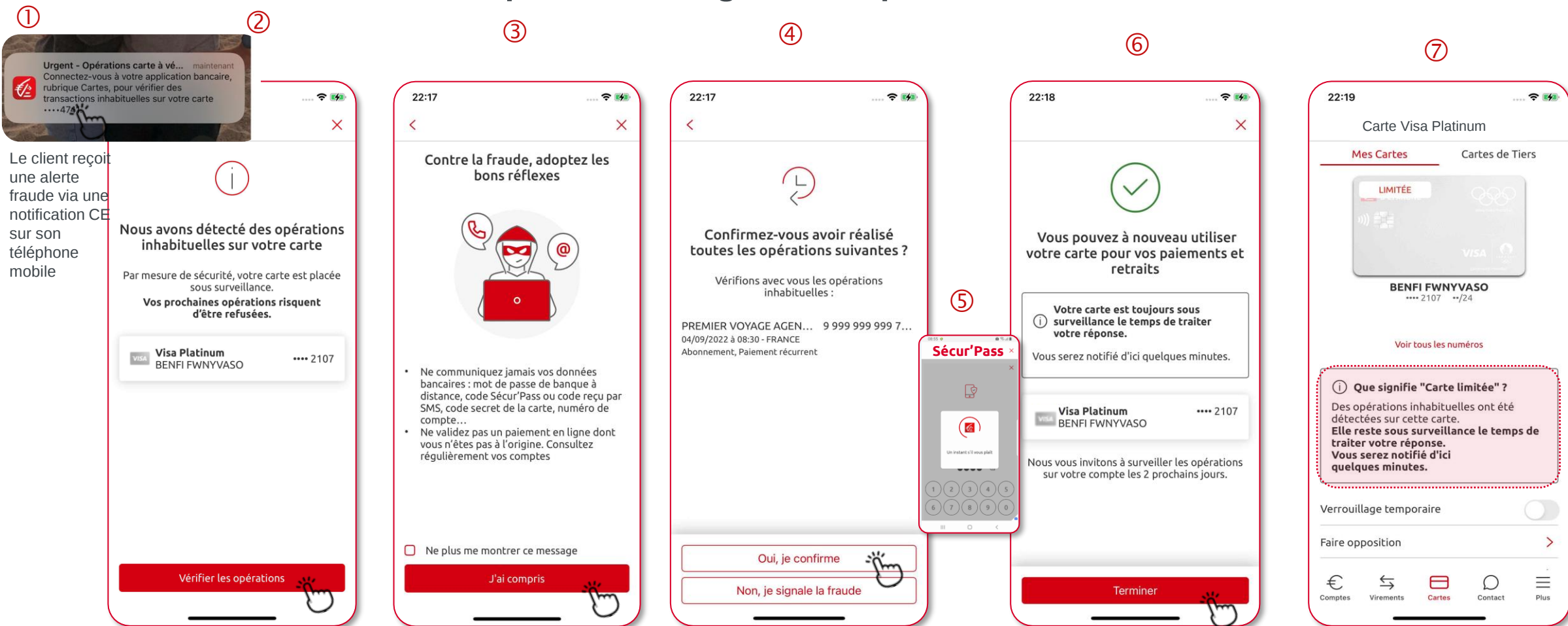
- ✓ Clients **Particuliers majeurs capables** < à 75 ans avec CB particuliers
- ✓ **Abonné Direct Ecureuil**, utilisateur de notre application Banxo
- ✓ Avec **Sécur'Pass** activé

Et si Margot ne réagit pas aux notifications ou ne consulte pas son application bancaire ?

⇒ Au bout de 5 jours, sans action de Margot, l'alerte est clôturée, sa carte n'est plus en statut limité. Elle pourrait être à nouveau notifiée en cas d'opérations inhabituelles à venir.

PARCOURS CLIENT

Cas 1 : client confirmant qu'il est à l'origine des opérations carte



Le client se connecte à son espace client via l'application Banxo et prend connaissance que sa carte est placée sous surveillance.

Le client est sensibilisé aux bons réflexes à adopter contre la fraude.

Le client doit confirmer les opérations ou déclarer une fraude.

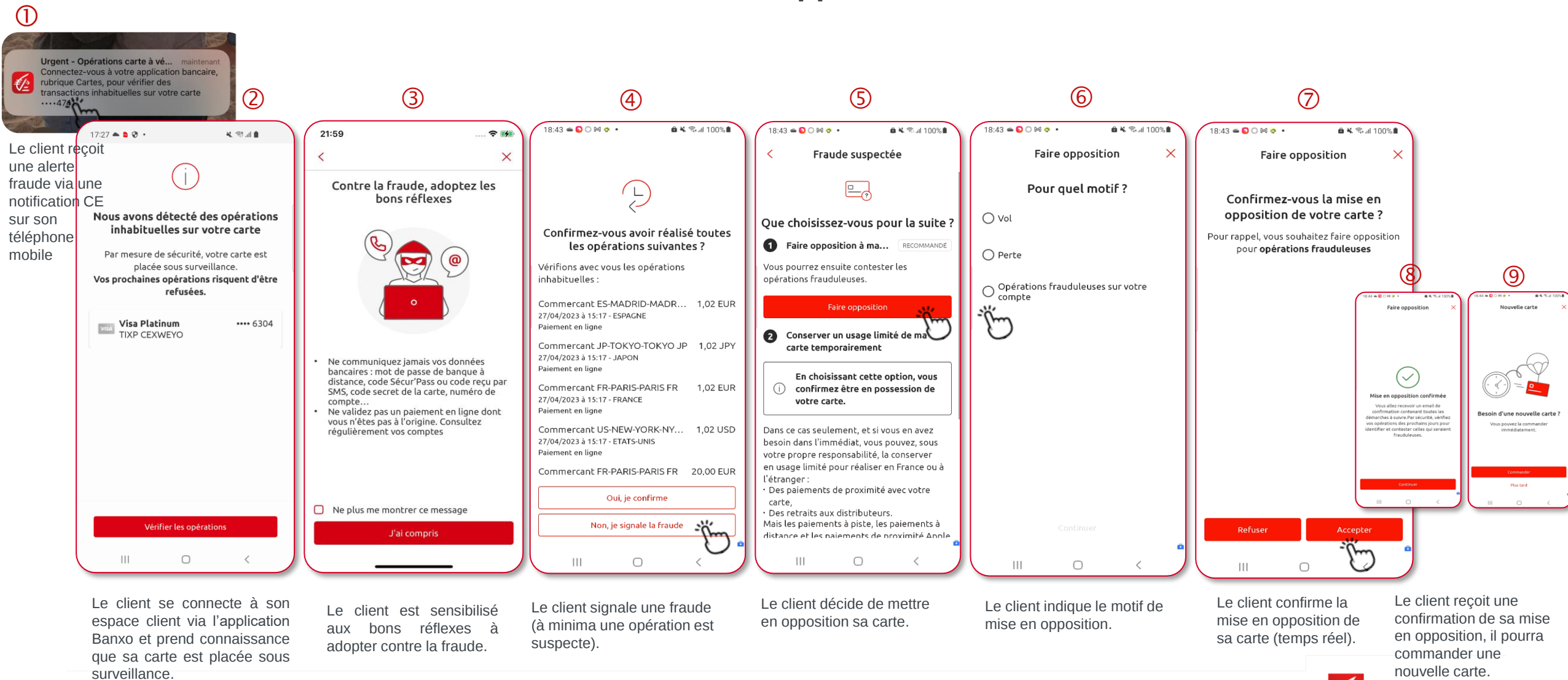
Le client devra s'authentifier pour confirmer la réactivation de sa carte.

Le client termine le parcours.

La carte reste sous surveillance le temps de traitement de sa demande. A réception de l'email de confirmation, la carte redevient active.

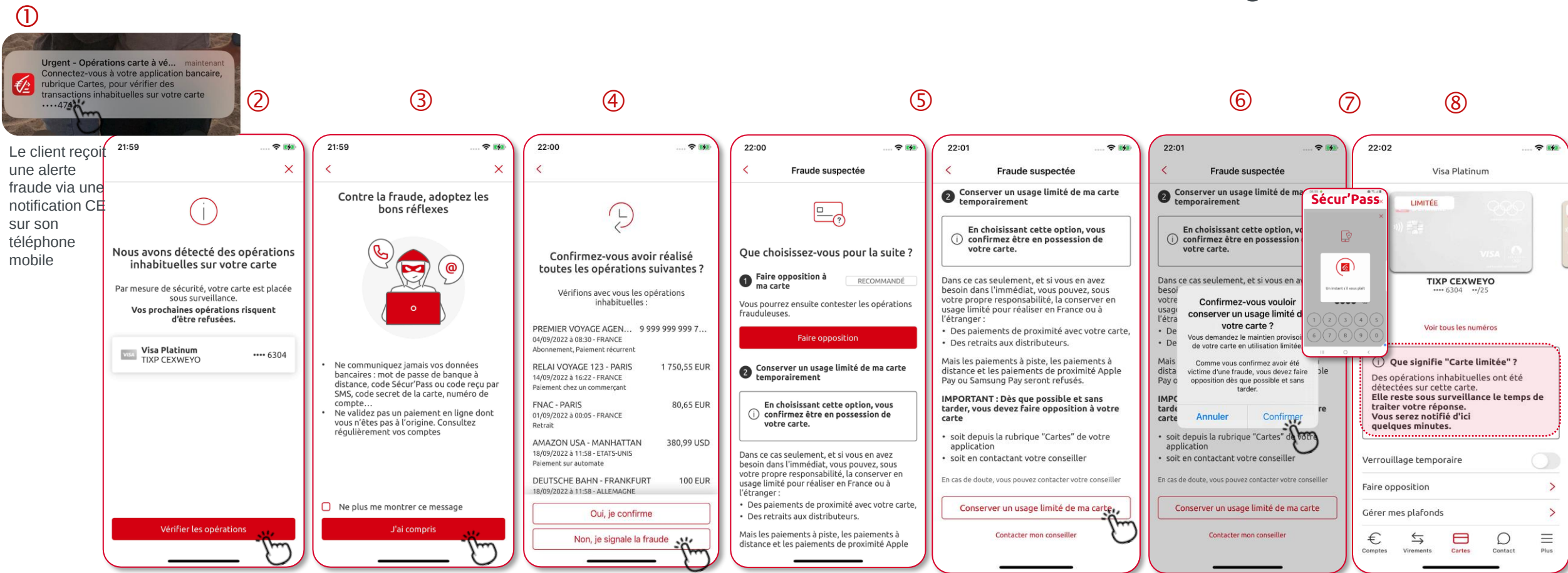
PARCOURS CLIENT

Cas 2 : client confirmant une fraude et faisant opposition à sa carte



PARCOURS CLIENT

Cas 3 : client confirmant une fraude carte mais souhaitant conserver un usage limité



Le client se connecte à son espace client via l'application Banxo et prend connaissance que sa carte est placée sous surveillance.

Le client est sensibilisé aux bons réflexes à adopter contre la fraude.

Le client signale la fraude (à minima une opération est suspecte).

Le client décide de conserver un usage limité de sa carte et de ne pas faire opposition immédiatement. Il souhaite réaliser un dernier paiement et/ou retrait avec saisie du code.

Le client confirme l'usage limité de sa carte et s'authentifie par Sécur'Pass.

La carte est limitée; son usage est restreint (les paiements VAD et mobile sont exclus). La carte **reste limitée**, le client devra à terme faire opposition.

PARCOURS CLIENT

Le client visualise le statut de sa carte sur l'écran Synthèse carte de l'application

Ecran synthèse carte

Cas client confirmant qu'il est à l'origine des opérations carte

Lors de l'alerte



La carte est « limitée » en utilisation.
Le client est informé que des opérations inhabituelles sont détectées sur sa carte.

Après action client



La carte reste « limitée » jusqu'à réception de l'email de confirmation de prise en compte de la réactivation de sa carte.

Ecran synthèse carte

Cas client confirmant une fraude et faisant opposition à sa carte

Lors de l'alerte



La carte est « limitée » en utilisation.
Le client est informé que des opérations inhabituelles sont détectées sur sa carte.

Après action client



La carte est « en opposition ».
Le client peut commander une nouvelle carte suite à son opposition.

Ecran synthèse carte

Cas client confirmant une fraude carte mais souhaitant conserver un usage limité de sa carte

Lors de l'alerte



La carte est « limitée » en utilisation.
Le client est informé que des opérations inhabituelles sont détectées sur sa carte.

Après action client



La carte reste « limitée » en utilisation, le client doit rapidement faire opposition.

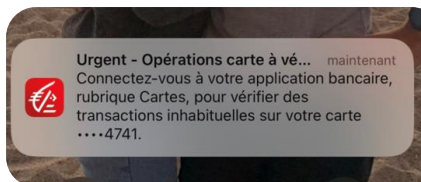
COMMUNICATION CLIENT

Le client est relancé à deux reprises post notification et au maximum au bout de deux heures



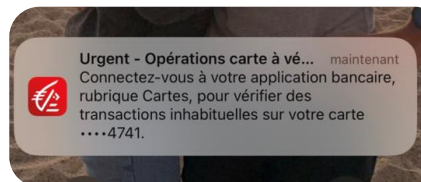
Notification émise en temps réel 24h24 et 7 jours sur 7

Notification push hors application



Notification + 30 minutes

Notification push hors application

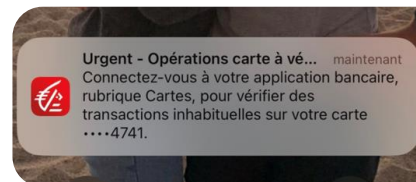


+
SMS

Caisse d'Epargne Aquitaine Poitou-Charentes : Merci de vous connecter à votre application bancaire, rubrique Cartes, pour vérifier des transactions inhabituelles sur votre carte4741.

Notification + 2 heures

Notification push hors application



+
Email



Opérations inhabituelles sur votre carte

Bonjour Mlle BECAC BANOE,

Des **opérations inhabituelles** ont été détectées sur votre carte bancaire0736.

Veillez vous connecter à votre application au plus tôt pour les vérifier dans votre rubrique Cartes.
Vous pouvez également contacter votre centre relation Fraude au 02 47 36 51 18 du lundi au samedi entre 8H et 22H (appel non surtaxé, coût selon votre opérateur).

Bien cordialement,
Caisse d'Epargne Loire Centre

Information sécurité



Soyez vigilant si vous êtes contacté par téléphone / e-mail / sms / chat.
Dans tous les cas, ne communiquez jamais vos codes confidentiels, codes sécurité reçus par sms ou mots de passe, même pour annuler un paiement.

Mentions légales
Caisse d'Epargne et de Prévoyance Loire-Centre

Notification + 5 jours

L'alerte est clôturée

COMMUNICATION CLIENT

A chaque action, le client reçoit un email

Le client a confirmé en selfcare qu'il est à l'origine des opérations carte.

Vous avez confirmé des opérations



Validation des opérations de votre carte

Bonjour MLE MINEUR TEST NPS LDD,

Vous venez de confirmer que vous êtes bien à l'origine des opérations inhabituelles détectées sur votre carte bancaire **** 5738.

Vous pouvez donc continuer à utiliser votre carte.

Bien cordialement,
Caisse d'Epargne Loire Centre

Vous n'êtes pas à l'origine de cette confirmation ?

 Contactez dans les plus brefs délais

Mentions légales

Le client a confirmé en selfcare qu'il n'est pas à l'origine des opérations carte et met en opposition sa carte.

Bonjour Monsieur SEIT MAMYTYEX,

Nous vous confirmons la prise en compte de votre demande de mise en opposition de votre carte Visa Infinite.

- N° de la carte : xxxx xxxx xxxx 4309

- Date d'opposition : 23 juin 2023

- Motif : Vol

- N° d'opposition : 775849

Information à nous retourner :
- Le PDF qui vous a été envoyé dans votre messagerie sécurisée. Vous pouvez la consulter sur <https://www.caisse-epargne.fr>

Si vous n'êtes pas à l'origine de cette demande, contactez votre conseiller dans les plus brefs délais.

Merci de votre confiance,
Votre Caisse d'Epargne.

Le client a confirmé en selfcare qu'il n'est pas à l'origine des opérations carte et souhaite conserver un usage limité de sa carte avant de la mettre en opposition.

Vous avez signalé des opérations frauduleuses



Opérations frauduleuses sur votre carte

Bonjour MR ETMEC HAINBCJ

Nous avons pris en compte que vous n'êtes pas à l'origine de certaines opérations inhabituelles sur votre carte bancaire **** 7009.

Vous avez choisi de conserver votre carte à usage limité(*).

Afin d'éviter d'autres opérations frauduleuses, vous devez la **mettre en opposition** dès que possible et sans tarder à partir de votre application mobile ou en contactant votre conseiller.

Bien cordialement,
Caisse d'Epargne Loire Centre

(*) Par mesure de sécurité, elle est placée sous surveillance. Rendez vous dans votre application pour plus de détails sur l'usage limité.

Mentions légales

Le client a confirmé par téléphone avec la cellule fraude la mise en opposition de sa carte.

Vous avez mis votre carte en opposition



Carte en opposition suite à des opérations frauduleuses

Bonjour MR NABEY SOXYZU,

Vous avez confirmé que des opérations frauduleuses ont été réalisées avec votre carte bancaire **** 3008.

Suite à nos échanges et conformément à votre demande, nous vous confirmons que votre carte a bien été mise en opposition(*).

Bien cordialement,
Caisse d'Epargne Loire Centre

(*) Rendez vous dans votre application ou votre espace sécurisé internet pour plus de détails sur la commande d'une nouvelle carte.

Mentions légales
Caisse d'Epargne et de Prévoyance Loire-Centre

VISION CONSEILLER

Poste de travail – Ecran Gérer la carte

Dès la suspicion d'une fraude carte bancaire et donc l'envoi d'une alerte, la carte est automatiquement en usage limité :

- . le temps de la réponse du client
- . ou si le client souhaite déclarer la fraude mais tout en continuant à utiliser sa carte

Portail MySys (Version 23.5.2249.259 Build : 583008 Source : 672457 / 108.0.5359.125) pro

MME Natacha - 0614 Fin Client

13335 - CEAPC 2262090 - MAITRISE OUVR...

Appeler

Vue client

Ma journée

Mes favoris

Recherche

Identification client

Natacha

Déconnexion

Gérer la carte n°4978 (04/2026)

MME NATACHA - N° compte : 13335

Envoi code confidentiel Courrier

Synthèse

Opposition

Actions / Modifications

Porteur en déplacement

Plafond dérogatoire

e-Carte Bleue

Alertes/Contestations

Détails / Historiques

Visuel

VISUEL SANS CONTACT JO

LIMITÉE

VISA

Nom sur la carte Nom de naissance

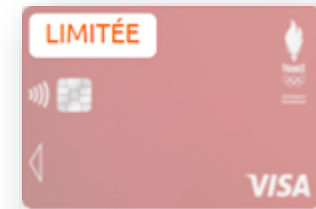
Lieu de livraison Domicile

Plafond STANDARD - PAIEMENT 2400 - RETRAIT 1000

Situation de la carte Alerte Fraude

Informations

Annuler Enregistrer



Usage limité

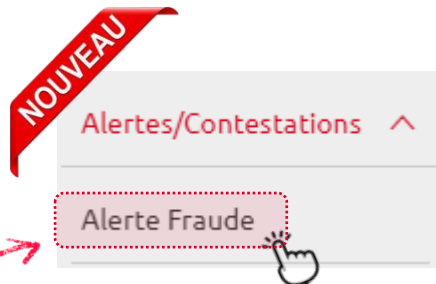
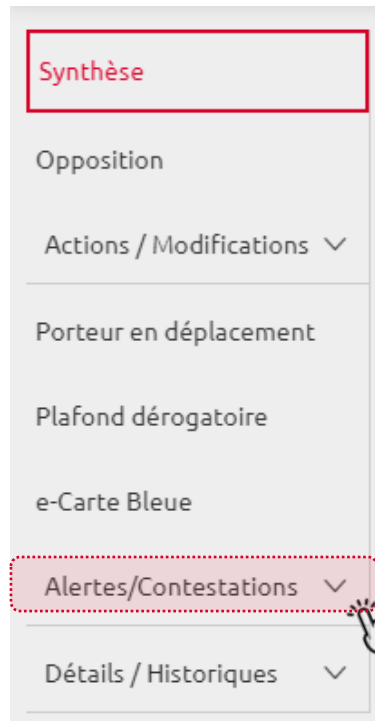
- > Paiements de proximité
- > Retraits aux distributeurs

La situation de la carte indique qu'elle est soit en :

- Alerte Fraude
- Usage Limité par le Client

VISION CONSEILLER

Poste de travail – Ecran situation de la carte



NOUVEAU

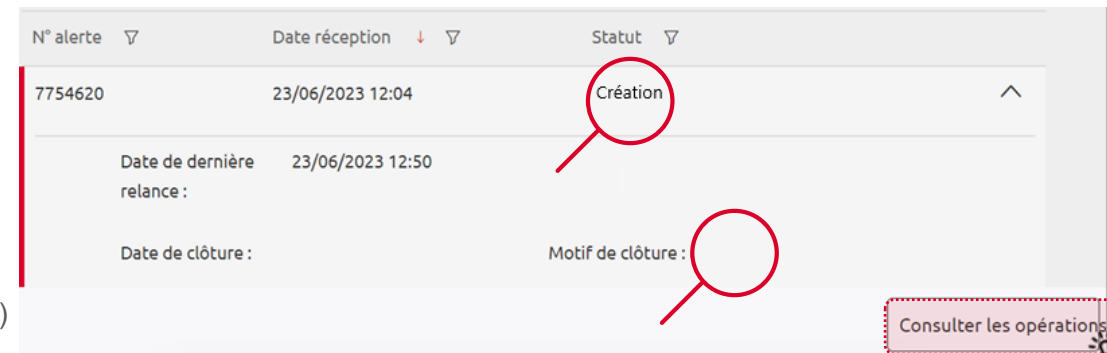


Le statut change en cas de relance(s)

- . Première relance
- . Deuxième relance
- . Alerte fraude traitée en Selfcare
- Alerte Clôturée

Le motif de clôture change en cas de traitement

- . Carte saine (le client est à l'origine des opérations)
- . Opposition (le client a fait opposition sur sa carte)
- Fraude sans opposition (usage limité choix client)
- Sans réponse client



Consulter les opérations

Détail des opérations concernées par l'alerte

Opérations de l'alerte N°7754620			
Date opération ▾	Libellé ▾	Montant ▾	Num Autorisation ▾
23/06/2023 11:18	LA SOCIETE GENERALE-PARMAIN-95620 FR	20,00 €	

ANNEXE - FOIRE AUX QUESTIONS

Principales interrogations

Questions	Réponses
Comment le client accède-t-il à son alerte fraude ?	Le client accède à son alerte fraude via la notification reçue sur son mobile l'invitant à se connecter à l'application Banxo (si le client a activé les notifications) ou en se connectant à l'application Banxo et en consultant l'écran "Carte".
Comment le client lève le doute de l'alerte ?	Le client lève le doute en répondant à une alerte fraude carte depuis l'application Banxo, soit en opposant sa carte, soit en indiquant l'absence de fraude, soit en choisissant l'usage limité de sa carte. Si le client déclare qu'il n'y a pas de fraude, la carte bancaire du client est considérée comme saine.
Quelles sont les actions possibles pour répondre à l'alerte ?	Les actions possibles pour le client sont de : 1. Confirmer la réalisation de toutes les opérations. La carte bancaire du client est saine et l'alerte est clôturée au poste de travail. 2. Confirmer la fraude (le client n'est pas à l'origine d'une ou plusieurs opérations présentées) et mettre en opposition sa carte. La carte bancaire du client est opposée et l'alerte est confirmée. 3. Confirmer la fraude mais ne pas mettre en opposition immédiatement sa carte (le client doit réaliser un dernier achat ou retrait), La carte restera limitée jusqu'à sa mise en opposition ou jusqu'à la fin de validité de la carte s'il ne l'oppose pas. L'alerte est clôturée au poste de travail. 4. Ne pas répondre à l'alerte.
Que se passe-t-il si le client ne répond pas à l'alerte fraude ?	Si le client ne répond pas à son alerte fraude carte via la notification push, il sera relancé • Au bout de 30 min = par SMS et à nouveau par notification Push mobile (hors app) • Au bout de 2 heures = par email personnel et à nouveau par notification push mobile (hors app) Dans tous les cas, au bout de 5 jours, l'alerte est clôturée, le client continue d'utiliser sa carte. Certaines opérations pourront encore à l'avenir être rejetées, si considérées comme inhabituelles par notre outil d'analyse de la fraude

ANNEXE - FOIRE AUX QUESTIONS

Principales interrogations

Questions	Réponses
Quelles opérations sont autorisées en cas de demande d'usage limité de la carte par le client?	Le client ayant demandé un usage limité de sa carte bancaire peut réaliser des paiements avec code secret ou paiements sans contact et des retraits aux distributeurs en France et à l'étranger. Les paiements à piste, les paiements à distance et les paiements de proximité Apple Pay ou Samsung Pay seront refusés.
Comment savoir si le client a été concerné par une alerte fraude sur sa carte bancaire ?	Le conseiller peut voir sur l'écran Mysys « Détails contrat carte », rubrique Alertes Contestation, choix Alerte fraude dans le totem de gauche. Le liste des alertes fraudes du client s'affichera et le détail de chacune pourra être consulté en cliquant dessus. Si le client a été concerné par une alerte fraude sur sa carte bancaire, la situation de la carte est indiquée en « Alerte Fraude ».
Lorsqu'on présente la liste des opérations inhabituelles au client via l'alerte. Sur cette liste, est-ce que toutes les opérations auront été rejetées ?	Il y aura à minima une opération rejetée (celle qui déclenche l'alerte fraude). Mais toutes les opérations de la liste n'ont pas nécessairement été rejetées.
Si parmi les opérations inhabituelles, une opération a été rejetée, si le client indique qu'il est bien à l'origine de l'opération, l'opération sera-t-elle au final acceptée ?	Non, le client devra, à nouveau, réaliser son achat.
Si le client décide de ne pas faire opposition tout de suite et de conserver un usage limité de sa carte, que se passe-t-il s'il ne fait pas opposition ?	Si le client ne fait pas opposition, sa carte ne fonctionnera pas en vente à distance, en paiement mobile et en paiement par piste. Le client pourra continuer d'utiliser sa carte qu'en paiement et retrait avec saisie du code ou en sans contact.
Si le client n'a pas répondu à l'alerte, peut-il tout de même contester l'opération ?	Oui, pour rappel, en cas « d'opération non autorisée » ou « mal exécutée », le client peut contester : - jusqu'à maximum 13 mois suivant la date du débit au compte pour un paiement dans l'EEE, - 70 jours suivant la date du débit au compte pour un paiement hors de l'EEE



**CAISSE
D'ÉPARGNE**

Vous être utile.