Cybercriminalité et fraudes
La chasse aux intermédiaires solvables

Lorsque les intermédiaires financiers deviennent la cible des victimes en quête d'indemnisation

Association luxembourgeoise des Juristes de Droit Bancaire

Arendt House

4 juin 2025

CONFIDENTIALITY REMINDER
This document is confidential and is intended solely for its recipient.
Do not distribute outside your organisation.

Cybercriminalité et fraudes

La chasse aux intermédiaires solvables

Vos contacts

Jean-Luc Putz

Partner
Business Crime

Stéphanie Lhomme

Partner ARC
Forensic
Investigations,
Corporate Intelligence
& Litigation Support

Noémie Haller

Counsel
Business Crime

Clara Bourgi

Counsel
Banking & Financial
Services

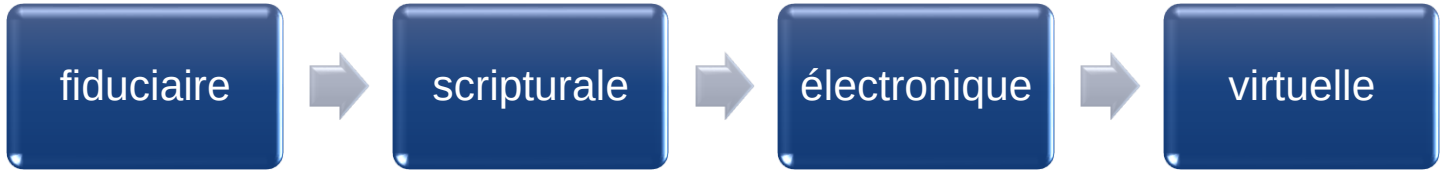
Vue d’ensemble

1. Le paiement et son encadrement juridique
2. Les typologies de risques de cybercriminalité pour les banques
3. Les qualifications pénales en matière de cybercriminalité
4. Les obligations du banquier
5. L’engagement de la responsabilité civile du banquier
6. Aspects procéduraux
7. Les moyens de défense
8. Conclusion

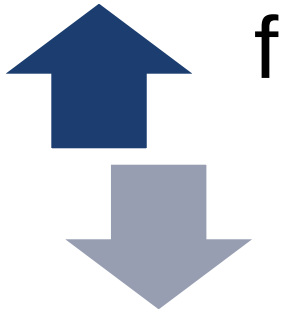
Le paiement et son encadrement juridique

Introduction

- **Rôle et importance du paiement**
- **Le banquier, en tant qu'intermédiaire**
- **Evolution de la monnaie & des moyens de paiement > évolution des techniques criminelles**



Introduction



fraude humaine

fraude technique

Confiance

Les typologies de risques de cybercriminalité pour les banques

1. Introduction

- Les risques de fraude, interne et externe, y inclus la cybercriminalité, ne cessent de croître, en particulier dans un contexte de dématérialisation croissante des échanges, notamment économiques et bancaires. Les banques peuvent en être les victimes directes ou indirectes si leurs clients (personnes physiques ou morales) sont visés. Leur responsabilité est dans ces situations souvent recherchée par les victimes finales, d'une part car elles **apparaissent comme les plus solvables dans l'écosystème mais aussi parce qu'elles sont soumises à diverses et nombreuses obligations.**

- Les banques continuent de faire face à des **fraudes dites « classiques », bien connues, mais toujours redoutablement efficaces**. Celles-ci exploitent le facteur humain notamment par des techniques de manipulation psychologique combinées à des techniques d'ingénierie sociale; ceci afin d'obtenir des informations personnelles et/ou confidentielles et/ou un accès à des systèmes.

- Les fraudes ont évidemment évolué avec **la numérisation et la digitalisation des échanges et des outils** : phishing, vishing, smishing, SIM swapping, spoofing, quishing, etc… Ces méthodes sont plus ou moins sophistiquées, avec un volet technique plus ou moins complexe, mais leur multiplication les rend efficaces.

- Il existe par ailleurs des **attaques plus techniques** (cyberattaques), qui connaissent une recrudescence. Elles ciblent tant les clients que les banques elles-mêmes ou autres parties prenantes (maillon faible). Les hackers / criminels tentent d'infiltrer les systèmes informatiques (serveurs bancaires, boîtes mail, plateformes d'e-banking, smartphones), dans le but d'exfiltrer des données sensibles, de mener des attaques de type « man-in-the-middle », mais surtout dans les situations qui nous préoccupent aujourd'hui de procéder à des paiements frauduleux.

- Enfin, la digitalisation des services financiers et l'émergence de **nouveaux moyens de paiement électroniques** (cryptomonnaies, actifs numériques, etc.) exposent également les banques et leurs clients à de nouveaux types de risques : ghost tap (NFC), vol de clés privées, exploitation de vulnérabilités dans des smart contracts, failles de sécurité dans des plateformes d'échanges collaborant avec les banques, pour ne citer que quelques exemples.

Définitions

- **Ghost Tap** - Interception et réémission de signaux de paiement NFC (near field communication) / sans contact pour exécuter des transactions sans autorisation.

- **Phishing** (email) : Usurpation d'identité par email pour inciter la victime à cliquer sur un lien malveillant ou à fournir ses identifiants.

  Ex: Emails frauduleux redirigeant les clients vers une fausse interface d'authentification, entraînant le vol d'identifiants LuxTrust.

- **Quishing** (QR code) : QR code frauduleux redirigeant vers des pages piégées ou de faux services de paiement.

- **SIM swapping** : Transfert frauduleux du numéro de téléphone vers une carte SIM contrôlée par un cybercriminel pour contourner l'authentification 2FA.

- **Spoofing** : Imitation technique d'un numéro de téléphone, d'une adresse email ou d'une URL

  Ex : Cour de cassation 23 octobre 2024 / Mécanisme d'authentification des numéros (MAN)

- **Vishing** (message vocal) : Appel d'un faux conseiller bancaire pour soutirer des codes d'accès ou initier une opération frauduleuse.

- **Smishing** (SMS) : Faux SMS incitant à cliquer sur un lien malveillant.

  Ex: Luxtrust – un SMS incite un client à renouveler son certificat LuxTrust via un URL qui le redirige vers une fausse interface bancaire où les identifiants LuxTrust lui sont dérobés.

2. Fraude interne avec détournement d'actifs de clients

- Les banques ne sont pas immunes aux **fraudes internes, c'est-à-dire commises par des employés ou collaborateurs internes**. Ces fraudes peuvent impacter les clients de la banque lorsque les actifs de ces clients sont détournés.

- Ce n'est pas l'objet premier de cette conférence mais pour rappel voici les schémas de fraudes internes les plus fréquents (liste non exhaustive), avec certains exemples récents.

Type de fraude (non exhaustif)	Exemple

Détournement	• Vol des actifs (fonds) du client:
	  • Détournement de fonds des comptes de multiples clients par un gestionnaire de fortune
	  • Prélèvements frauduleux sur les comptes de clients: « *Procès Indexia : des victimes qui avaient fait confiance à leur assureur* », Le Monde 26.09.2024
	• Transferts depuis des comptes inactifs:
	  • Utilisation de l'argent « dormant » sur des comptes inactifs

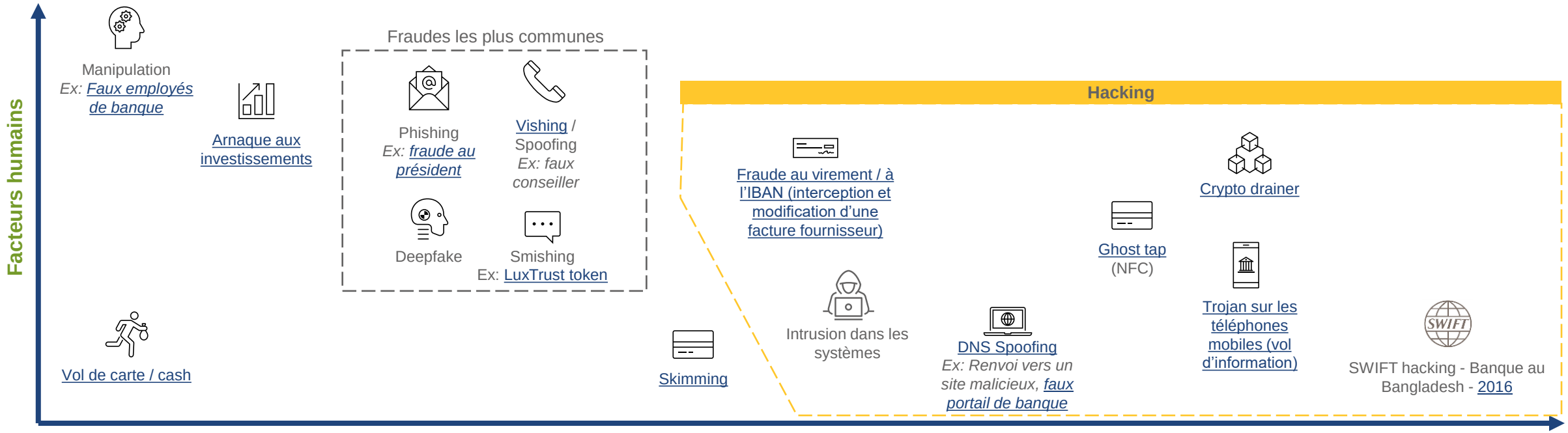
Transaction non autorisée	• Arrondissement des montants des transactions dans le but de détourner une partie des montants • Ajout de frais bancaires fictifs: « *Bank of America to pay $250 millions for illegal fees, fake accounts* ». NPR 11.07.2023
Vol d'informations personnelles / complicité	• Complicité d'un employé de banque dans le vol d'informations personnelles de clients afin de les vendre ou donner à un complice qui détourne ensuite des fonds

3. Typologie de fraudes externes (non exhaustif)

- Les banques de par les fonds qu'elles gèrent sont évidemment la cible de criminels externes. Ces criminels peuvent **cibler la banque directement ou ses clients**.

- **Le degré de sophistication et de technicité des fraudes varie**. Les plus classiques – mais encore redoutablement efficaces – ont un faible volet technologique et utilisent la manipulation humaine. Elles exploitent la **psychologie humaine** via des biais cognitifs, d'émotions, et de comportements. Certains aspects de la psychologie humaine utilisés dans ce type de fraudes sont l'autorité (fraude au président), la confiance (faux conseiller bancaire), l'urgence (expiration de votre token LuxTrust), l'avidité (promesse d'un retour sur investissement), la routine (fraude à l'IBAN, paiement d'une facture), parmi d'autres. Ces fraudes, bien que connues, sont encore en évolution constante et s'adaptent aux nouveaux moyens de communication ainsi qu'aux nouvelles technologies telles que GenAI, Deefakes, etc., et aux nouveaux moyens de paiement.

- On constate en effet que la majorité des fraudes **combinent facteurs humains et technologie.** Nous avons traité ces 2 dernières années de nombreux cas de hacking dans des fonds d'investissements. Les banques n'étaient pas la cible directe car elles sont plus matures en termes de cybersécurité. Les hackers se sont introduits dans les systèmes du "maillon faible" (beaucoup de petites parties prenantes dans l'écosystème des fonds à Luxembourg: AIFM, investment advisors, GP, avocats...), ont pris le temps d'analyser les échanges, d'identifier les informations nécessaires et ont avec succès fait des demandes de virements (faux capital calls...).



4. Typologie de fraudes externes (non exhaustif)

Nous détaillerons ensuite les implications juridiques et judiciaires des différents cas de figure. Mais voyons rapidement ici les cibles.

Clients

- Les criminels ciblent souvent les clients des banques afin de compromettre leur compte (p.ex. via phishing, smishing, etc.) ou leurs moyens de paiement (p.ex. carte NFC, Apple Pay, Google Wallet), pour ensuite effectuer des transferts / paiements frauduleux. En effet, les individus ou petites structures sont moins protégés et souvent encore moins alertes.

- Le client victime cherchera souvent la responsabilité de la banque, arguant que celle-ci a manqué à ses obligations de vigilance, diligence, contrôle... qui auraient dû bloquer la transaction frauduleuse.

- Il revient ensuite à la banque de se défendre, par exemple en mettant en évidence son environnement de contrôle interne (transaction monitoring) et en arguant en retour de la négligence / responsabilité du client.

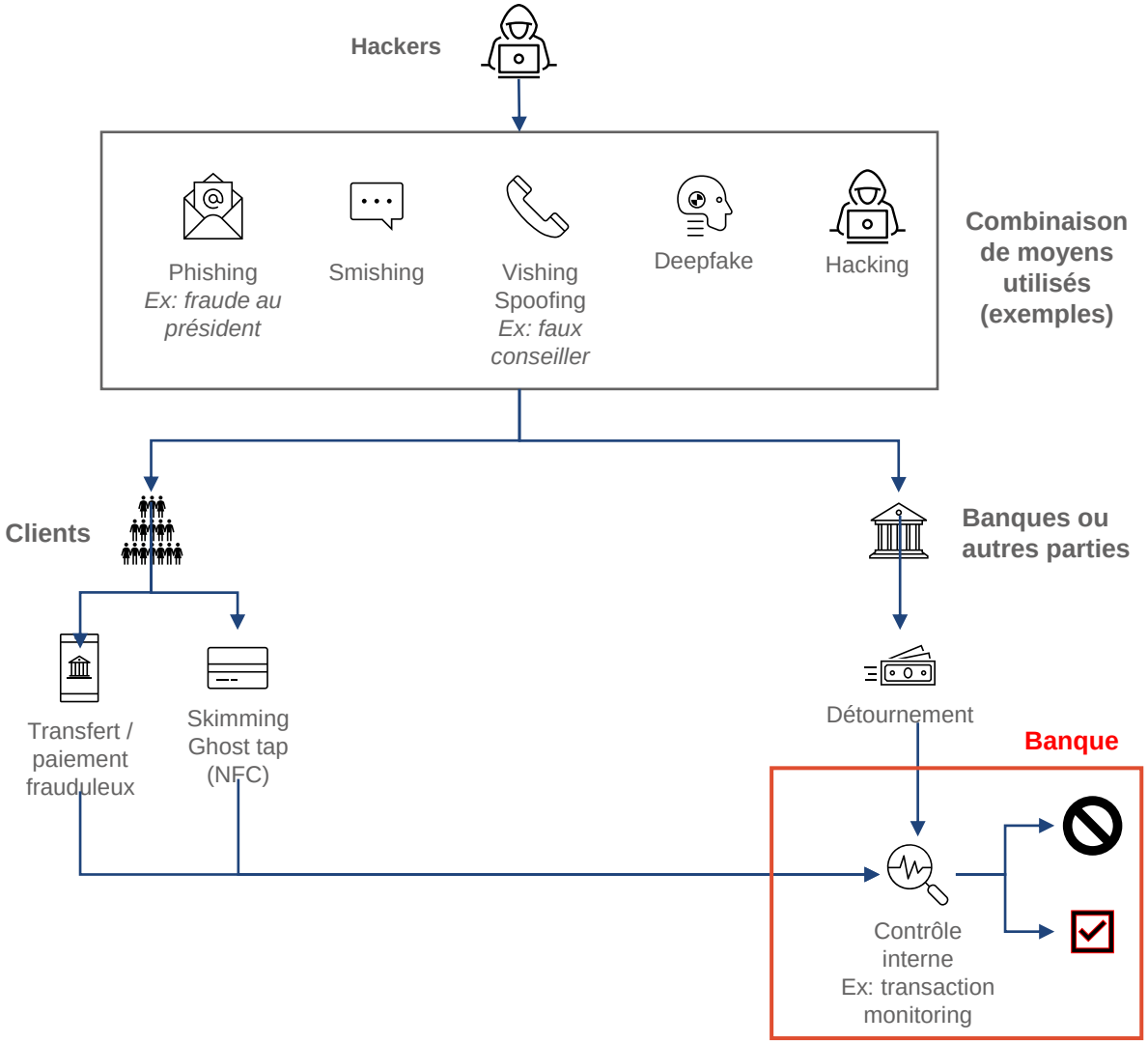
Banques

- Les banques sont parfois attaquées directement. Les criminels utilisent ainsi une défaillance, humaine (ingénierie sociale) et/ou technique (hacking) pour s'introduire dans le système, et tenter de détourner des fonds, ou d'obtenir des informations qui permettent ensuite de détourner facilement des fonds.

- Ici, les moyens techniques utilisés sont souvent plus sophistiqués.

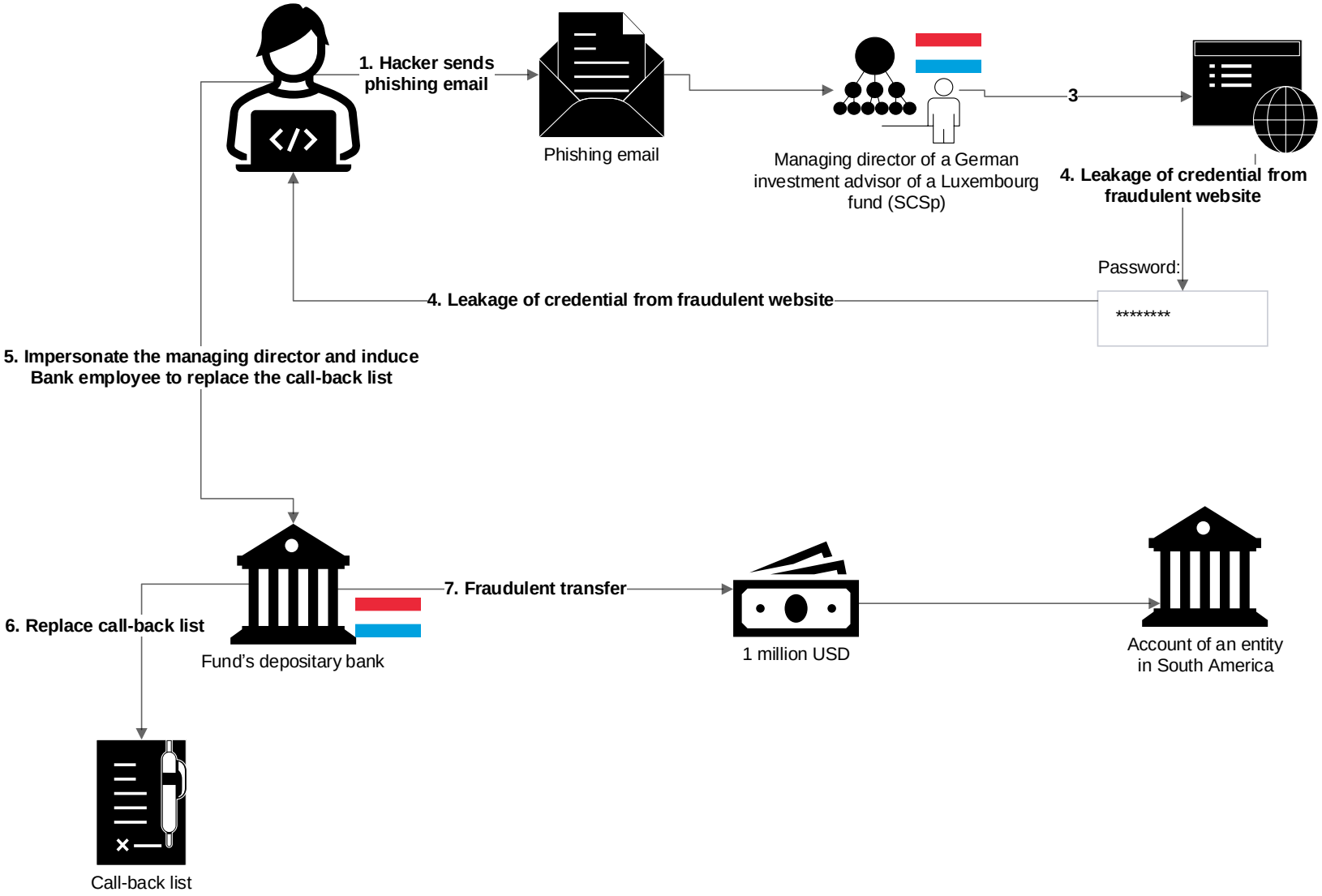
Intermédiaires et parties tierces

- Les intermédiaires et parties tierces, si structures plus petites, sont souvent moins bien protégés que les banques, et peuvent donc être une cible alternative pour les criminels, qui tentent ainsi de s'infiltrer dans leurs systèmes pour récolter de l'information ou pour émettre des demandes de paiement auprès de la banque (cas récents de hacking dans les fonds d'investissements à Luxembourg).



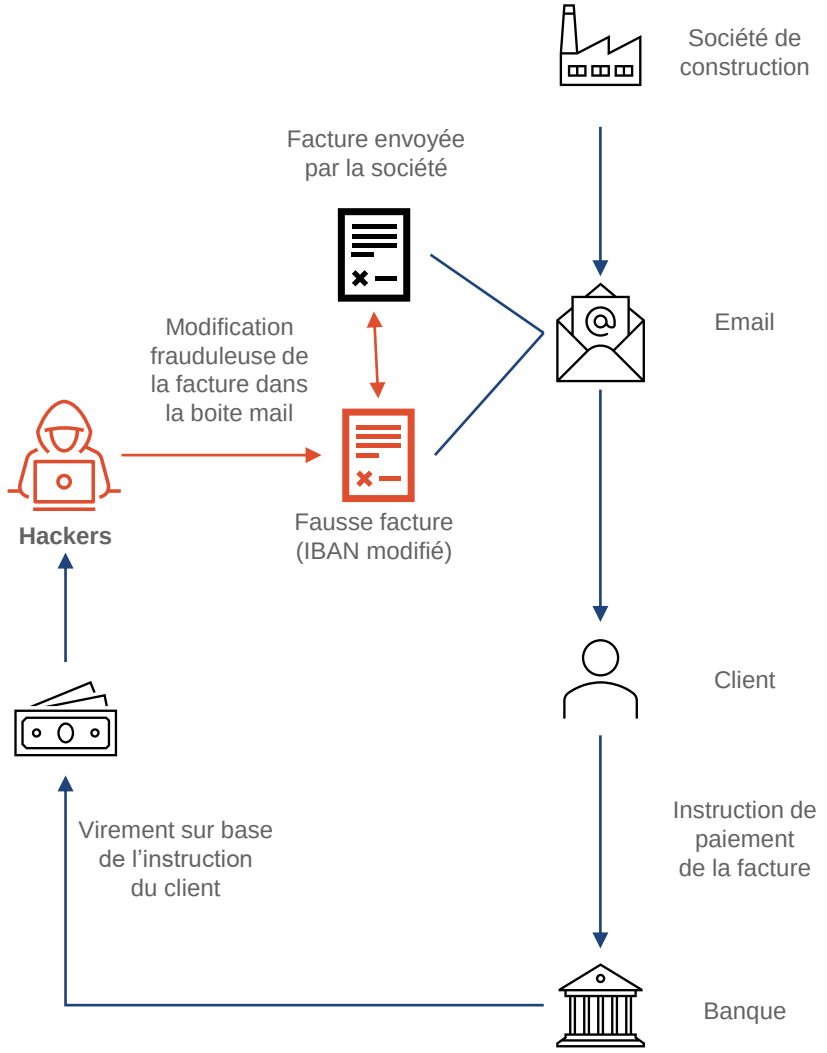
Exemple 1: Phishing et paiement frauduleux dans un fonds Luxembourgeois

- Lors d'un cas récent, des hackers se sont introduits dans les systèmes d'un fonds d'investissement au Luxembourg grâce à un e-mail frauduleux (phishing) envoyé au directeur général du conseiller en investissement (« investment advisor »).
- Cette intrusion a permis aux hackers d'accéder à des communications et aux informations permettant de faire valider des transferts.
- Ils ont analysé les communications (style de communication, interlocuteurs…) avec la banque, les documents utilisés, les procédures.
- Ceci leur a permis de demander avec succès à un employé de la banque dépositaire du fonds de remplacer la « call-back list ».
- Une fois la « call-back list » remplacée, ils ont effectué trois transactions frauduleuses : l'une d'entre elles a permis de transférer 1 million de dollars américains à une entité en Amérique du Sud.
- La banque a identifié que la transaction était inhabituelle mais a appelé les numéros figurant sur la nouvelle call-back list, frauduleusement modifiée.
- **Une modification de la liste de call-back suivie quelques jours plus tard seulement de plusieurs transactions inhabituelles auraient dû générer une alerte.**



Exemple 2: Fraude à l'IBAN suite au piratage d'une boite mail

- Après avoir effectué des travaux de rénovation importants pour un client, la société de construction envoie la facture au client par email.
- Des hackers avaient cependant piraté la boite mail du client et intercepté la facture avant que le client ne puisse la voir.
- Ils ont remplacé l'email et la facture, reprenant toutes les informations initiales mais en changeant le numéro de compte sur lequel le paiement devait être effectué.
- Le client a ensuite effectué un virement depuis le site de sa banque, en indiquant les informations trouvées sur la fausse facture, à son insu.
- La banque a effectué le paiement vers le compte des hackers, sur base de l'instruction du client.
- Ce type de fraude pourrait être évité au niveau de la banque en mettant en place une vérification de la correspondance entre l'IBAN et le nom associé au compte. **Ce contrôle devrait être mis en place à partir d'octobre 2025 (EU).**



Exemples de condamnation de banques à rembourser des clients

ARGENT & PLACEMENTS • VIE QUOTIDIENNE

La Cour de cassation condamne BNP Paribas à rembourser un client victime d'une escroquerie téléphonique

« Au regard des circonstances dans lesquelles l'escroquerie a eu lieu, il ne peut être reproché au client d'avoir commis une négligence grave », a confirmé la Cour de cassation dans un communiqué.

Le Monde avec AFP

Publié le 23 octobre 2024 à 20h48 · Lecture 2 min.

Source: https://www.lemonde.fr/argent/article/2024/10/23/la-cour-de-cassation-condamne-bnp-paribas-a-rembourser-un-client-victime-d-une-escroquerie-telephonique_6358823_1657007.html

Un client de la banque BNP Paribas a été victime de spoofing en 2019. Un faux conseiller de la banque l'a appelé en utilisant frauduleusement le numéro de téléphone de la banque. Le faux conseiller a demandé au client d'ajouter des personnes sur la liste des bénéficiaires de virements et de confirmer ses informations personnelles par téléphone.

L'ajout de ces bénéficiaires était un prétexte, et le faux conseiller en a profité pour effectuer plusieurs virements frauduleux pour un total de 54,500 euros.

La Cour de cassation a estimé que le client « *n'avait pas été gravement négligent* » et que BNP Paribas devait donc rembourser ce client lésé.

Suite à la vente de son appartement, un retraité niçois a reçu environ 115,000 euros sur son compte courant. En attendant que les nouveaux propriétaires s'y installent, le retraité a laissé un jeune homme s'y installer.

Ce jeune homme a profité de l'accès au courrier et aux documents présents dans l'appartement pour détourner 115,000 euros en trois mois.

Bien que la banque ait décliné toute responsabilité, elle a été condamnée par le tribunal correctionnel à rembourser le montant détourné, et à verser 10,000 euros de dommages et intérêts pour un manque de vigilance.

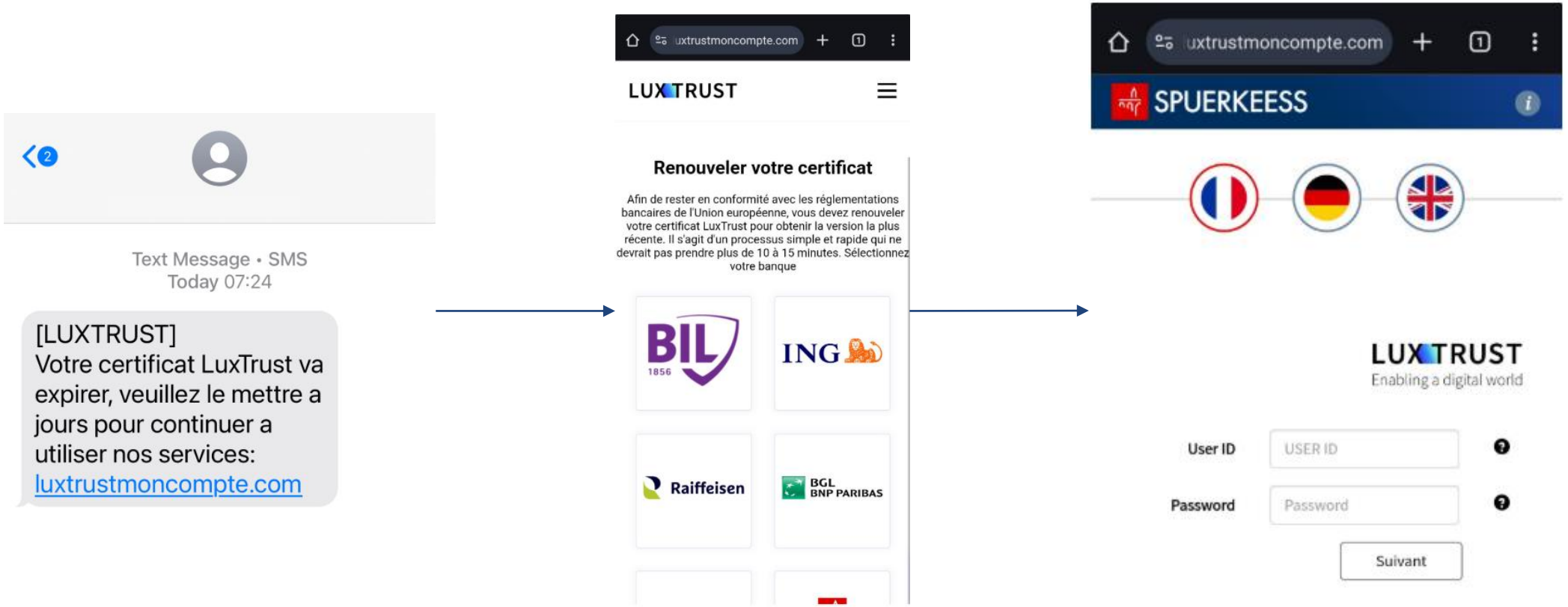
Nice : le Crédit agricole condamné à verser 125.000 euros à un retraité

Europe1 .fr

10h53 · le 6 juin 2017 - Mis à jour le 10/02/2025 à 16:21 · 1 min

Source: https://www.europe1.fr/societe/nice-le-credit-agricole-condamne-a-verser-125000-euros-a-un-retraite-3352565

Exemple récent au Luxembourg (LuxTrust)



Un SMS frauduleux est envoyé avec un lien, prétextant de l'expiration du certificat LuxTrust.

En cliquant sur ce lien, une page internet s'affiche, demandant de renouveler le certificat et de se connecter avec ses identifiants LuxTrust. Les identifiants sont ensuite récupérés par les fraudeurs.

Source: https://govcert.lu/de/articles/phishing-threats/20250212-1/

Exemples récents au Luxembourg

Tentatives de phishing sous le nom de LuxTrust

02.12.2024 COMMUNIQUÉS DE PRESSE

— Depuis plusieurs mois, la place luxembourgeoise est confrontée à des attaques de **phishing (hameçonnage) via email, sms et/ou téléphone** de plus en plus sophistiquées. Les fraudeurs se font passer pour un agent LuxTrust en prétextant une opération frauduleuse sur le compte bancaire de la personne concernée pour soutirer aux utilisateurs de LuxTrust des informations confidentielles. Les équipes de LuxTrust, ayant à cœur la sécurité de ses clients et utilisateurs, alertent sur ces actions frauduleuses et les bonnes pratiques à suivre.

Source: https://www.luxtrust.com/fr/news/tentatives-de-phishing-sous-le-nom-de-luxtrust

ALERTE FRAUDE

Tentatives de « phishing » *(hameçonnage)* suivies de « vishing » *(hameçonnage par téléphone)* avec « spoofing » *(usurpation d'identité)* !

Les fraudeurs n'hésitent pas à se faire passer pour des employés de la BIL ou d'institutions légitimes (tout en usurpant le numéro de téléphone de la banque ou de l'institution) dans le but de récolter vos données/identifiants et de les détourner à des fins frauduleuses.

Rappelez-vous que la BIL ne vous demandera jamais vos données/identifiants.

Un employé BIL ne demandera jamais à un coursier de venir chercher des cartes bancaires à votre domicile.

Source: https://www.bil.com/fr/particuliers/prevention-securite/Pages/Index.aspx#

VOTRE POLICE | RECRUTEMENT | APPELS PUBLICS | AIDE AUX VICTIMES | PRÉVENTION | LÉGISLATION

Prévention > Arnaques et dangers sur internet

ESCROQUERIES PAR DE FAUX EMPLOYÉS DE BANQUE

La police a récemment reçu plusieurs signalements de personnes ayant été contactées par des individus se présentant comme des employés d'une banque ou de la société Luxtrust et leur annonçant qu'elles avaient été victimes d'une cyberfraude ou que leur compte bancaire posait problème.

Pour résoudre le problème, les victimes devaient communiquer leurs identifiants de connexion à leur interlocuteur et effectuer certaines transactions via l'application Luxtrust.

En communiquant leurs identifiants de connexion aux fraudeurs et en autorisant les transactions via l'application Luxtrust, les victimes se sont vu prélever des sommes considérables.

Nous tenons donc à rappeler que de telles demandes ne correspondent pas aux pratiques des administrations, sociétés ou banques sérieuses. Celles-ci ne vous demanderont jamais de communiquer vos identifiants de connexion par téléphone ni d'autoriser des transactions.

Si vous n'êtes pas certain qu'il s'agisse d'une tentative de fraude, ne vous laissez pas mettre sous pression et contactez la société ou la banque concernée par les moyens habituels. **Nous tenons à souligner que cette technique frauduleuse utilise souvent le « Call ID Spoofing »**, qui permet d'afficher de faux numéros de téléphone. La victime croit ainsi recevoir un appel provenant d'un numéro de téléphone mobile luxembourgeois ou d'une autorité officielle, ce qui n'est toutefois pas le cas.

À cet égard, nous vous prions également d'informer et de sensibiliser les personnes âgées de votre entourage à cette technique frauduleuse.

Si vous avez subi un préjudice suite à un tel appel, veuillez vous adresser à un poste de police de votre choix.

Source: https://police.public.lu/fr/prevention/arnaques/arnaque-faux-employes-banque.html

LUXEMBOURG Publié 9. mai 2025, 12:37

Débités de «sommes considérables» par de faux employés de banque

La police grand-ducale met en garde contre les agissements de prétendus employés de banque ou de LuxTrust qui sévissent actuellement au Luxembourg.

Source: https://www.lessentiel.lu/fr/story/luxembourg-debites-de-sommes-considerables-par-de-faux-employes-de-banque-103339410

Luxembourg

Comment les criminels volent votre carte bleue et votre code PIN

Pierre Weimerskirch – adapté pour RTL Infos | Actualisé: 19.04.2025 18:14

La plupart des gens retirent de l'argent liquide aux distributeurs automatiques sans trop y penser, mais ils peuvent néanmoins être victimes de fraude par le biais de techniques telles que le piégeage de cartes, l'écrémage ou l'utilisation de faux claviers.

La Spuerkeess et la police mettent en garde les utilisateurs de distributeurs automatiques contre de nouvelles arnaques qui ont cours au Luxembourg. Il existe différentes techniques pour voler ou copier une carte bancaire. Souvent, elles sont si habiles que les victimes ne s'en rendent même pas compte.

Les plus lus

1 Opération escargot des taxis
Des kilomètres de bouchons à prévoir sur l'A31 toute la journée

2 Que s'est-il passé dans l'avion ?
"Complicité" ou coup au visage:

Source: https://infos.rtl.lu/actu/luxembourg/a/2295509.html

Les banques vérifieront bientôt chaque virement que vous effectuez

Toute personne effectuant des virements en ligne doit s'assurer que le nom saisi correspond au numéro de compte. Dans le cas contraire, la banque émettra une notification. ©Shutterstock

ROBBE VAN LIER

25 avril 2025 08:36

Source: https://www.lecho.be/entreprises/banques/les-banques-verifieront-bientot-chaque-virement-que-vous-effectuez/10604258.html

Les qualifications pénales en matière de cybercriminalité

Qualifications pénales

- **Appropriation de l'argent**

Fraude technique (attaque informatique)	• Vol
Fraude humaine (ingénierie sociale)	• Escroquerie (ruse, tromperie) • Extorsion (violences, menaces)

- Peut-on voler de la monnaie scripturale / électronique ?
- Circonstances aggravantes
- Qui est la victime ?

Qualifications pénales

- **Moyens pour commettre l'infraction**
  - **Faux et usage de faux** (faux intellectuel, y compris numérique)
  - **Fraudes informatiques** : attaques aux « systèmes de traitement de données »
    - Accès et maintien frauduleux
    - Introduction de données
  - Infractions en matière d'**instruments de paiement**
    - Contrefaçon des instruments de paiement
    - Obtention des données (phishing ; skimming)
    - Utilisation de moyens de paiement contrefaits
  - La **clef électronique**
    - Notion & protection
    - Exemple du phishing

2020
28 affaires

2023
1310 affaires

0
condamnations

Les obligations du banquier

1. Enjeux
2. Les obligations contractuelles
3. Les obligations en matière de sécurité des paiements et des systèmes
4. Les obligations en matière de lutte contre le blanchiment

Enjeux


Risque administratif
Risque pénal
Risque civil
Risque réputationnel
Risque opérationnel

Les obligations contractuelles

Obligations contractuelles

Obligation d'exécution correcte et diligente de l'ordre

S'assurer de l'origine de l'ordre de virement

Vérifier la régularité et la sincérité du titre

- Forme
  Apparence
- Circonstances générales

Anomalie de nature à éveiller un doute sur l'authenticité

Le banquier surseoit à l'exécution et demande confirmation au client

Obligations contractuelles

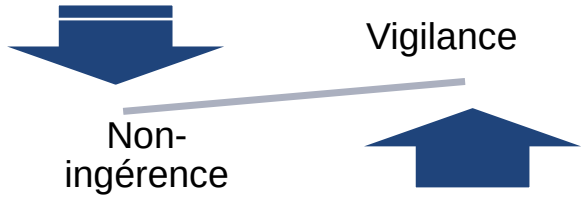
Devoir de vigilance

Déceler des anomalies intellectuelles ou matérielles

- Montant
- Bénéficiaire
- Juridiction
- Fréquence
- Historique des transactions
- Profil du client

1. Paramétrer le système de surveillance des transactions en veillant à ces critères
2. Importance d'une revue humaine
3. Contacter le client

Obligation de moyens



Obligations contractuelles

Obligation d’information et de conseil

Fournir des informations exactes et suffisantes, loyales et complètes

- Simplicité / Complexité
- Qualité du client
- Circonstances

Obligation de conseil et non de surveillance

Le client doit aussi s’informer et se renseigner -> prudence

Les obligations en matière de sécurité des paiements et des systèmes

Obligations en matière de sécurité des paiements et des systèmes

DSP II

Etablir un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés pour gérer les risques opérationnels et de sécurité

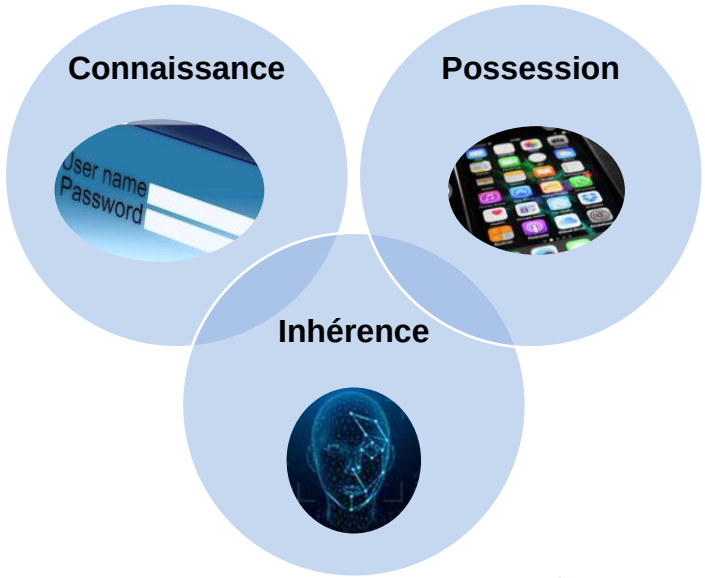
→Procédures efficaces de gestion des incidents

Moyens appropriés pour notifier la perte, le vol, le détournement, l'utilisation non autorisée de l'instrument de paiement

Empêcher l'utilisation d'instruments de paiement après une telle notification

Authentification forte

Assurer la confidentialité et l'intégrité des données de sécurité



Utilisation de deux éléments

Indépendance de ces éléments

Protection de la confidentialité des données d'authentification

Le payeur ne supporte aucune conséquence dès lors que l'opération de paiement non autorisée a été effectuée sans authentification forte

Obligations en matière de sécurité des paiements et des systèmes

DORA

Gestion des risques liés aux TIC

Gestion, classification et déclaration des incidents liés aux TIC

Test de résilience opérationnelle numérique

Gestion des risques liés aux prestataires tiers de services TIC

Echange d’informations et de renseignements sur les cybermenaces

Obligations en matière de sécurité des paiements et des systèmes

Orientations EBA/GL/2025/02

Circulaire CSSF 25/880

Relation avec les utilisateurs de services de paiement

Sensibiliser les utilisateurs aux risques et fournir une assistance

Mise à jour de l'assistance et des conseils (nouvelles menaces)

Désactiver / ajuster des fonctionnalités / des limites de dépenses

Alertes sur les tentatives initiées / échouées d'opérations

Assistance et informations sur cette assistance

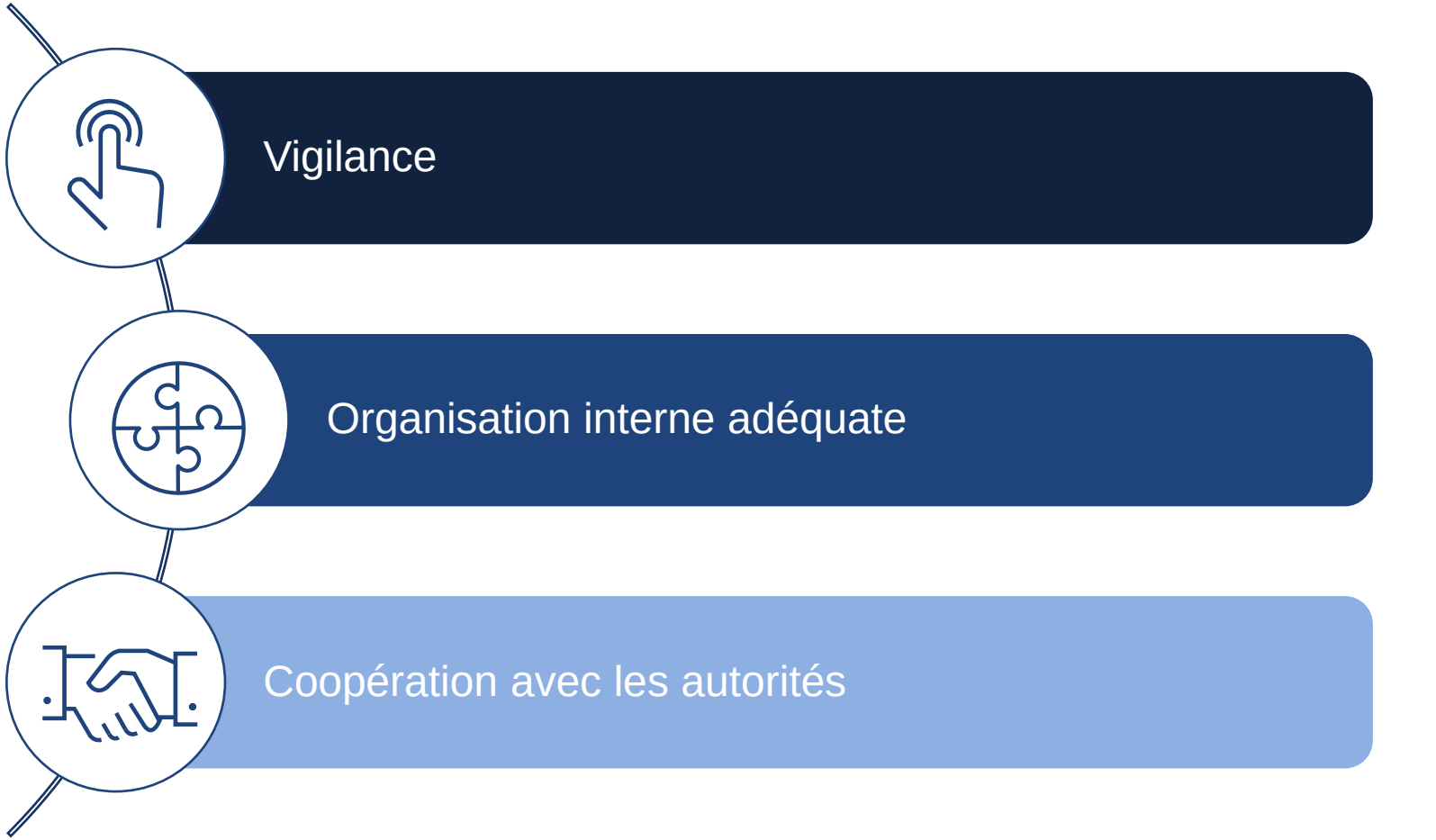
Relation avec le régulateur

Fournir une évaluation actualisée et complète des risques

Les obligations liées à la prévention du blanchiment

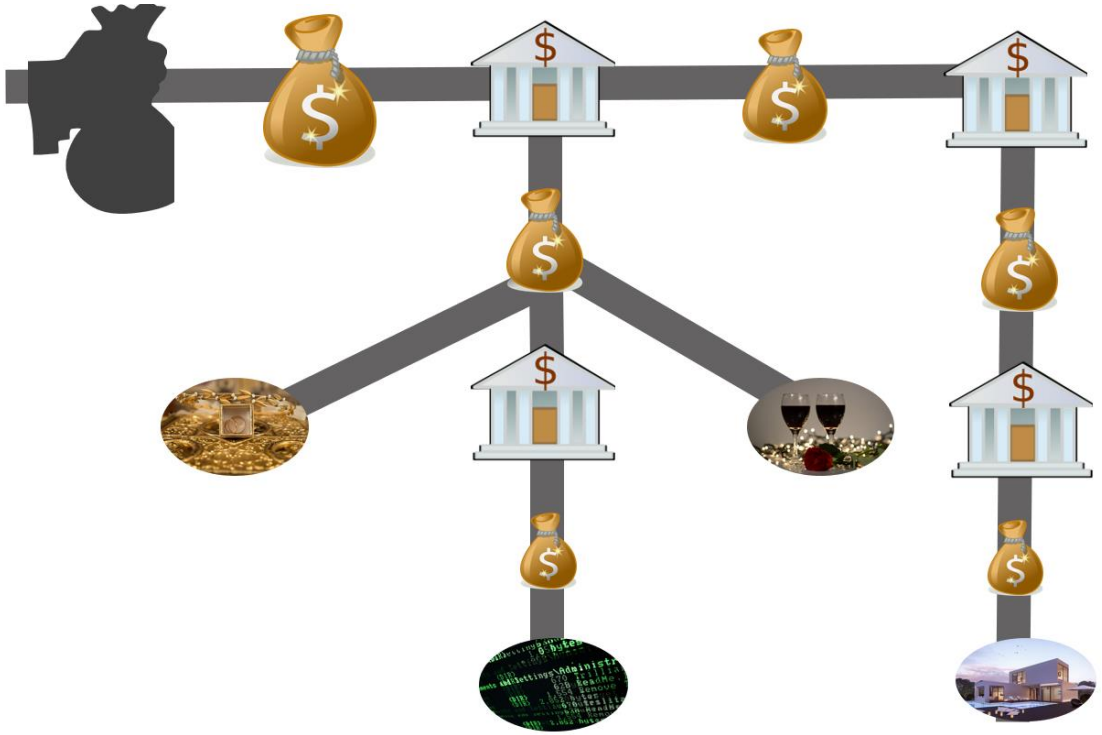
1. Obligations professionnelles : la lutte contre le blanchiment
2. Point d’attention : la participation active au blanchiment

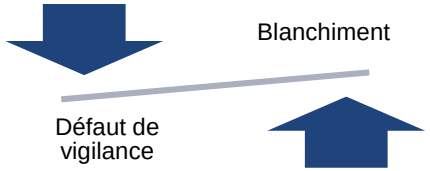
Obligations professionnelles en matière de lutte contre le blanchiment



Augmentation de la liste des infractions primaires au fil des années

Point d’attention : la participation active au blanchiment (1)





En acceptant des fonds ayant une origine illicite, une banque peut participer à une opération de blanchiment

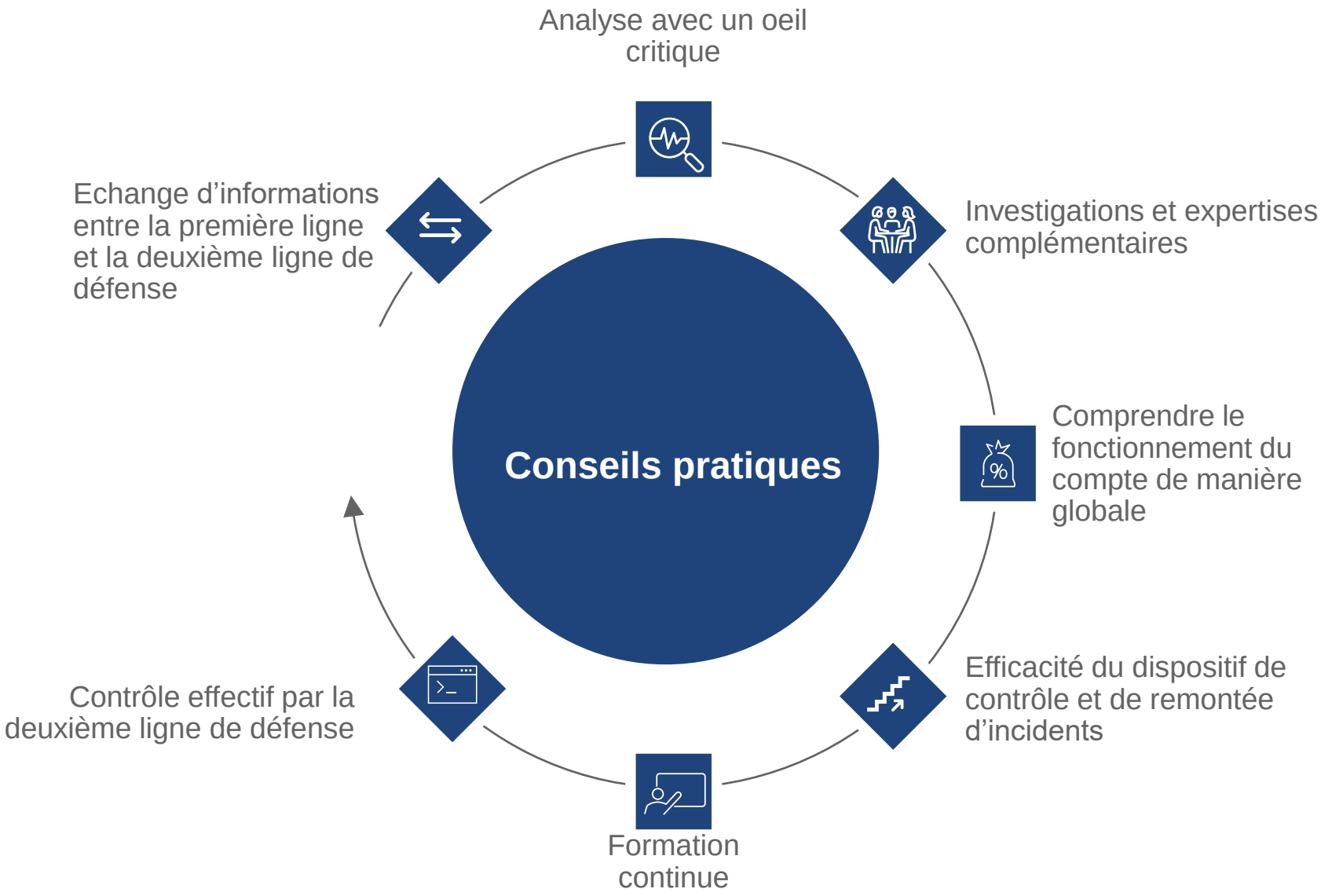
Ensemble de circonstances de fait qui doivent nécessairement éveiller la méfiance

Présomptions graves, précises et concordantes

Conscience de l’origine frauduleuse des fonds

il suffit de savoir ou de se douter, sur la base des données de fait, que toute provenance légale des fonds peut être exclue.

Point d’attention : la participation active au blanchiment (2)



L’engagement de la responsabilité civile du banquier

1. Quelles bases légales ?
2. Deux régimes de responsabilité
3. La responsabilité civile engagée sur base de la LSP
4. La responsabilité civile engagée sur base du droit commun

Quelles bases légales ?

- Responsabilité contractuelle - articles 1134, 1147 C. civ.
  Théorie du mandataire substitué - article 1994 du Code civil
- Responsabilité délictuelle - art. 1382, 1383 C. civ.
- Loi du 12 novembre 2004 relative à la lutte contre le blanchiment et le financement du terrorisme – Obligation de vigilance
- Loi modifiée du 10 novembre 2009 relative aux services de paiement (« **LSP** »)
  Directive 2007/64/CE du 13 novembre 2007 (« **DSP I** »), abrogée par Directive (UE) 2015/2366 du 23 novembre 2015 (« **DSP II** »)

Deux régimes de responsabilité

Régime spécial

- Responsabilité de plein droit
- Loi modifiée du 10 novembre 2009 relative aux services de paiement (« LSP »), ayant transposé DSP I puis DSP II

Régime de droit commun

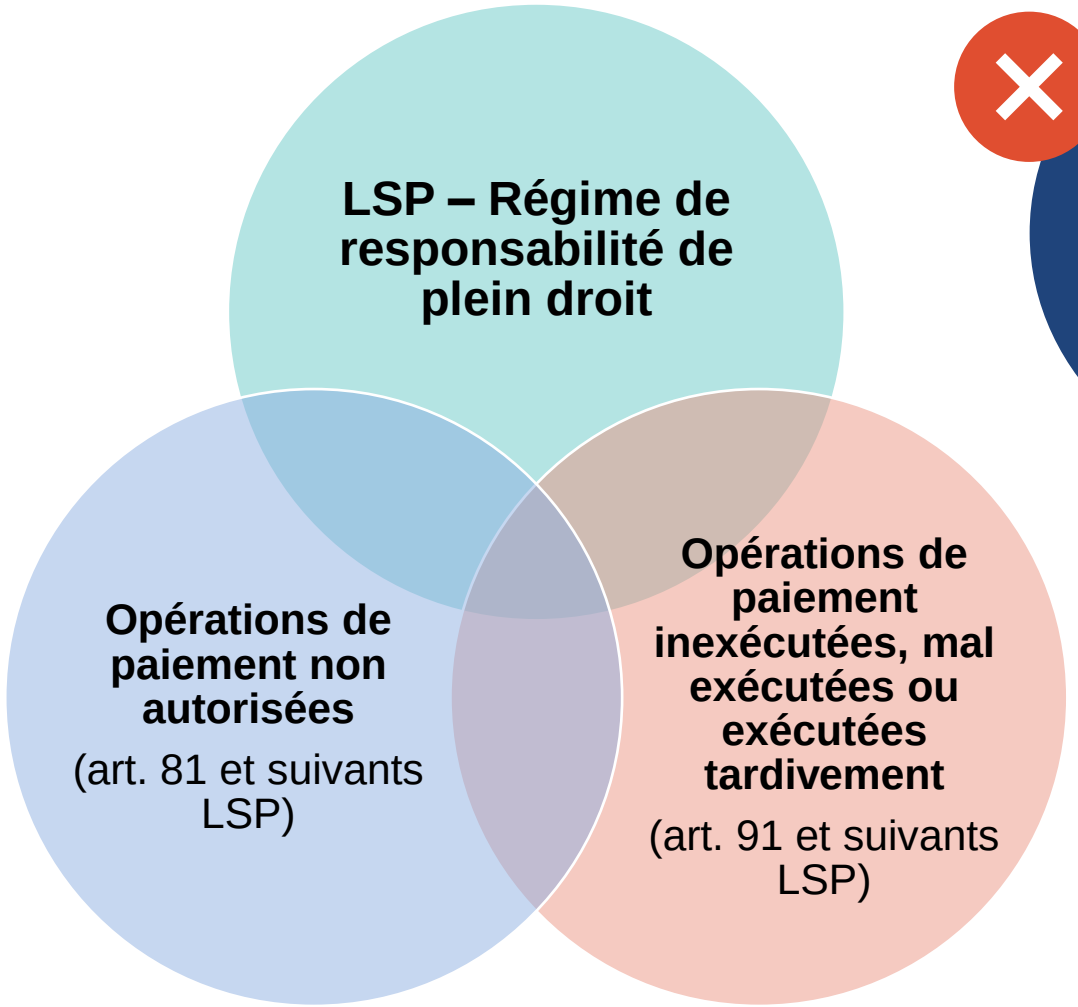
- Responsabilité pour faute
- Responsabilité contractuelle / Théorie du mandataire substitué
- Responsabilité délictuelle
- Manquements aux obligations visées par la Loi de 2004 / obligation de vigilance

Intérêt : sur base de la LSP, responsabilité engagée sans avoir à prouver de faute ≠ droit commun

Contrebalancé par le délai court de contestation ?

Deux régimes de responsabilité

Champ d'application de la LSP ?

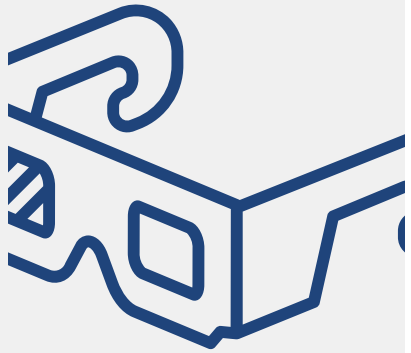


Opérations de paiement autorisées = droit commun

CSJ, 7 mars 2023, n°39/23
CJUE, 02.09.2021, C-337/20
CJUE, 16.03.2023, C-351/21

Les deux régimes ne se cumulent pas

Deux régimes de responsabilité



Distinction ?

Opération de paiement autorisées

- Le payeur a techniquement consenti
- Notion de consentement ? Consentement obtenu par ruse, abus ou tromperie ?
- Ex. : fraude au président, phishing, arnaque téléphonique, etc.

Article 81. – Le consentement et le retrait du consentement.

(1) Une opération de paiement n'est réputée autorisée que si le payeur a donné son consentement à l'exécution de l'opération de paiement. Une opération de paiement peut être autorisée par le payeur avant ou, si le payeur et « le »[245] prestataire de services de paiement en ont convenu ainsi, après son exécution.

(2) Le consentement à l'exécution d'une opération de paiement ou d'une série d'opérations de paiement est donné sous la forme convenue entre le payeur et « le »[246] prestataire de services de paiement. « Le consentement à l'exécution d'une opération de paiement peut aussi être donné par l'intermédiaire du bénéficiaire ou du prestataire de services d'initiation de paiement. »[247]

En l'absence « de »[248] consentement, l'opération de paiement est réputée non autorisée.

(3) Le consentement peut être retiré par le payeur à tout moment, mais pas après le moment d'irrévocabilité prévue à l'article 93. Le consentement à l'exécution d'une série d'opérations de paiement peut aussi être retiré« , auquel cas »[249] toute opération de paiement postérieure « est »[250] réputée non autorisée.

Opérations de paiement non autorisées

- Violation d'une règle de sécurité technique / fraude technique
- Ø d'authentification forte,
- Utilisation après notification (perte, vol, détournement)
- Ø possibilité de notification à tout moment
- Ex.: Utilisation d'un moyen de paiement volé (carte volée, données de carte volées, moyen de paiement se trouvant sur le téléphone qui a été volé, substitution frauduleuse d'un RIB), etc.

Responsabilité civile sur base de la LSP

Exemples jurisprudentiels

JP Lux., 8 mars 2013, n° 1017/13 confirmé en appel TA Lux., 25 mars 2014, n° 87/2014

- Victime d'un vol de carte bancaire
- Carte laissée avec le code secret (?), opposition tardive (6 jours)
- Négligence grave sur base des articles 83 et 88 LSP + conditions contractuelles
- "*L'utilisateur supporte les risques liés à une gestion insouciante de ses moyens de paiement*"

JP Lux., 6 mai 2022, n° 320/22

- Victime d'un vol de carte bancaire, retraits malgré blocage immédiat des cartes
- "*L'utilisation d'un instrument de paiement ne suffit pas, à elle seule, à établir une négligence grave*" (Ccass. Fr. 2 oct. 2007, 28 mars 2008, 3 avril 2019, 14 nov. 2019)

CSJ, 7 mars 2023, CAL-2022-00563

- LSP s'applique lorsque PSP du payeur et du bénéficiaire sont situés dans un Etat membre (virements)
- LSP applicable pour apprécier responsabilité de la banque ≠ droit commun invoqué par la victime
- Rejet de la demande de la victime : PSP responsable à l'égard de son seul client

Responsabilité civile sur base de la LSP

Changements attendus en matière de responsabilité ?

Calendrier ?

Proposition de Directive

concernant les services de paiement et les services de monnaie électronique dans le marché intérieur modifiant la directive 98/26/CE et abrogeant les directives (UE) 2015/2366 et 2009/110/CE

Proposition de Règlement

concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) n°1093/2010

Nouveautés attendues en matière de responsabilité du PSP sur base de ces textes :

1. Système de vérification de la concordance entre le nom du bénéficiaire et l'IBAN avant d'exécuter un virement dans le but de réduire les erreurs et les fraudes dans les transactions électroniques
2. Cas des de responsabilités étendus : application incorrecte de l'obligation de vérification de la concordance entre le nom du bénéficiaire et l'IBAN, cas d'usurpation d'identité,
3. Possibilité pour les PSP d'échanger des données à caractère personnel dans le but d'améliorer la détection des opérations de paiement frauduleuses

Responsabilité civile sur base du droit commun

A quel titre la responsabilité civile peut-elle être engagée ?

- **Responsabilité contractuelle - art. 1134, 1147 Code civil**
  - Relation contractuelle nécessaire : action d'un utilisateur de service de paiement à l'égard du PSP dont il est client
  - Théorie du mandataire substitué - art. 1194 Code civil : selon cette théorie, le banquier du bénéficiaire du virement agirait en qualité de mandataire du bénéficiaire (pour la réception et l'encaissement du paiement) mais aussi en qualité de mandataire substitué du donneur d'ordre en tant que celui-ci e charge d'inscrire la somme virée au crédit du bénéficiaire

- **Responsabilité délictuelle - art. 1382 et 1383 Code civil**
  - Absence contractuelle nécessaire
  - Actions d'un utilisateur de service de paiement à l'égard du PSP du bénéficiaire

Pour quels types de fautes ?

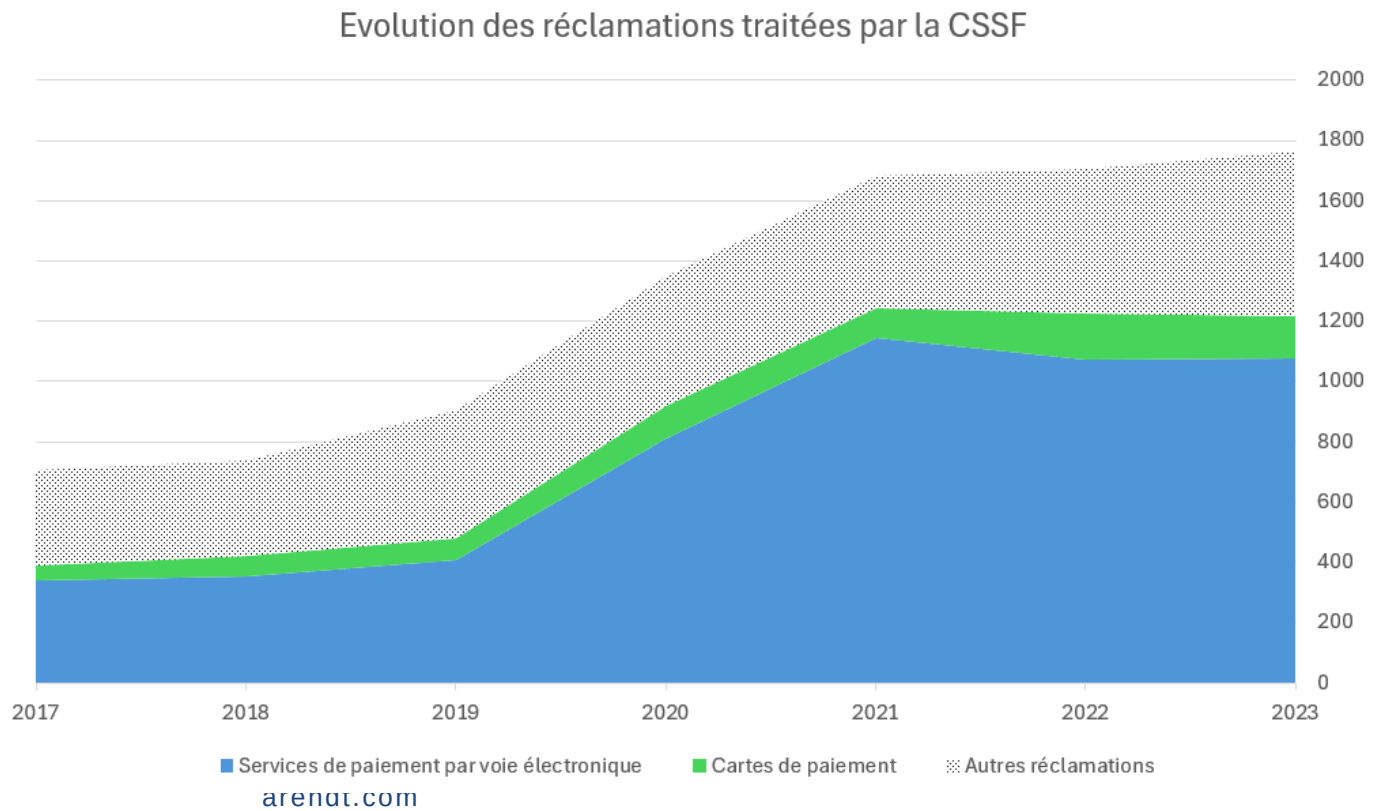
- **Violation du devoir de vigilance ?**
- **Violation des obligations AML?**
  - Obligation d'identification du client KYC, obligation d'identifier le bénéficiaire économique, évaluation du risque, vigilance continue sur la relation d'affaire, obligation de déclaration à la CRF, etc.
- **Infraction de blanchiment ?**

Aspects procéduraux

Aspects procéduraux

Extra-judiciaire

- **Négociations pré-contentieuses**
  - Obligations réglementaires (15 jours)
  - Avantages et désavantages d'un arrangement
  - Transiger en bonne et due forme
- **Procédure de règlement extra-judiciaire des litiges devant la CSSF**



Judiciaire

- **Procédures envisageables**
  - Procédure administrative (CSSF)
  - Procédure civile ou commerciale
  - Procédure pénale

- **Preuve**
  - ***Charge de la preuve***
    - Preuve du caractère autorisé ou non de l'opération
      - Opération non autorisée : responsabilité de plein droit, banquier devant établir la négligence grave
      - Opération autorisée : obligations du banquier = obligations de moyens > charge de la preuve reposant sur l'utilisateur
  - ***Accès à la preuve***
    - Droits de l'utilisateur/client/tiers pour accéder à la preuve ?
    - Valeur probante d'une décision administrative ?
    - Valeur probante d'une condamnation pénale

Les moyens de défense

1. Virements non autorisés

2. Virements autorisés

Virements non autorisés

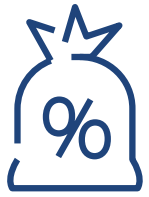
Perte | **Vol** | **Détournement**

Opérations postérieures à la notification

Le PSP ne permet pas de procéder à tout moment et gratuitement à la notification

Faute du PSP

Pas d'authentification forte



Fraude

Violation intentionnelle ou par négligence grave de ses obligations

Autres cas

Les moyens de défense

Virements non autorisés

La fraude ou la violation intentionnelle ou par négligence grave des obligations

Négligence grave inopérante :

- **en cas d'absence d'authentification forte**
- **de déficience technique**

Charge de la preuve

Obligations de l'utilisateur

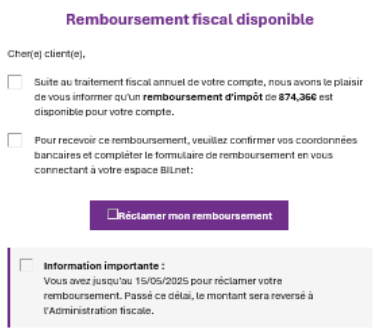
Utilisation conforme de l'instrument de paiement et préserver la sécurité des données

Informer sans tarder le PSP de la perte, du vol, du détournement ou de toute utilisation non autorisée de l'instrument de paiement

Illustrations jurisprudentielles

Oublier l'existence d'une carte bancaire
Laisser ses identifiants avec la carte

Déclaration tardive
Oublier de faire opposition



Apparence
Adresse mail de la banque
Signature du conseiller
Logo

Manque de prudence, de précaution ou de vigilance caractérisé

Virements autorisés

Contester la faute (1)

Documentation contractuelle

- **Conditions générales**
  - **Acceptation des virements après une certaine durée**
  - **Clauses limitatives de responsabilité**
  - **Obligations du client**
- **Profil du client**

Faute lourde

Virements autorisés

Contester la faute (2)

Obligations de moyens

Principe de non-ingérence

La banque n'est pas tenue d'intervenir dans les choix financiers du client

Absence d'anomalie apparente

Procédure de callback adéquate

Contenu

- Montant, destinataire, juridiction, libellé de la transaction
- Particularité du transfert au regard des transferts antérieurs

Destinataire

- Personne contractuellement habilitée

Preuve

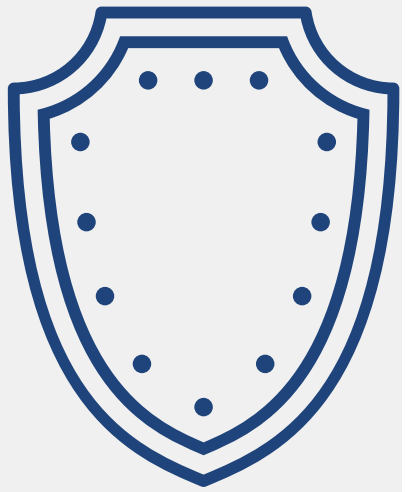
- Enregistrement du rappel téléphonique
- Confirmation électronique par écrit

Virements autorisés

Contester le lien de causalité

Virements autorisés

Contester le préjudice



- **Faute / négligence de la victime**
  - **Faute civile / négligence grave de la victime** : retard dans la notification, comportement négligent, absence de dépôt de plainte, etc.
  - **Obligation de vigilance du client eu égard à la sophistication technologique des arnaques**
  - **Faute pénale** - plainte du PSP contre le client ? Fraude commise par le client ; rôle actif du client dans la réalisation de l'opération : mise à disposition non autorisée du token ; remise du mot de passe ; communication de ses identifiants, etc.
  - **Partage de responsabilité : CSJ, 12 juin 2014, n°37554** : virement comportant une contradiction manifeste (titulaire ≠ bénéficiaire) ; anomalie apparente ; mandataire substitué ; négligence grave du client ; partage de responsabilité
  - **Remise en cause du lien de causalité en raison de la faute de la victime**

    CSJ, 7 mars 2024, n°CAL-2022-00867 : rupture du lien de causalité par la faute du donneur d'ordre ayant décidé de faire confiance « *(…) le préjudice allégué (…) est dû exclusivement à la circonstance (…) que les appelants ont, au mépris de toute prudence, procédé au virement litigieux au profit de PERSONNE8.) qu'ils qualifient eux-mêmes d'ami de longue date (…)* »

- **Preuve du préjudice ?**
  - Preuves des montants réclamés ?
  - Préjudice certain, direct, personnel ?

- **Licéité du préjudice ?**

- **Faute d'un tiers ? Force majeure ?**
  - Faute d'un tiers : doit en principe revêtir le caractère de la force majeure : une fraude peut-elle être considérée comme imprévisible ?

L'importance du "fact finding" pour préparer sa défense (ou l'offensive)

■ Si une transaction illicite et/ ou frauduleuse est effectuée / validée par la banque, cela implique souvent qu'un contrôle au sein de la banque n'a pas fonctionné ou que le paramétrage du contrôle ou du système était perfectible. Une autre possibilité, que l'on retrouve souvent dans les fraudes internes notamment est l'outrepassement du contrôle (« override »), qui peut être dû à un accès privilégié légitime ou non ou rendu possible par des décisions prises sous pression et dans l'urgence (technique classique dans les fraudes au président par exemple).

■ La personne (ou entité morale) victime d'une sortie de fonds frauduleuse aura pour premier réflexe de vouloir récupérer son argent et donc de chercher la responsabilité de la banque. C'est souvent la négligence de celle-ci que la victime cherche à démontrer (manquement à ses obligations de vigilance), arguant que la banque aurait dû détecter et bloquer une transaction suspicieuse (ex: compte bancaire vidé suite à un phishing, via un virement vers un pays hors Europe, avec une connexion au portail bancaire depuis la Russie ou transfert vers une société au Portugal dont le compte bancaire est en Bulgarie).

■ Avant toute argumentation contraire, il est critique que la banque investigue ce qui s'est passé (techniquement et humainement) afin d'avoir en main suffisamment d'informations factuelles et documentées: individus et parties impliqués, chaine temporelle, faiblesses, manquements... et de comprendre pourquoi la transaction frauduleuse n'a pas été détectée, ni bloquée par les contrôles internes (transaction monitoring), etc.

■ Non seulement l'investigation permet d'analyser la suite des événements ayant mené à la fraude, de comprendre comment elle a pu se produire, sur quelle période, qui était impliqué, etc. Mais elle est aussi importante pour mettre en évidence des éléments clés démontrant (au moins) une part de responsabilité du client ou d'autres parties prenantes, ou démontrant suffisamment que la banque a rempli ses devoirs prudentiels. **L'investigation permet donc de bien documenter et étayer ses arguments de défense mais aussi de préparer ses arguments d'offensives envers d'autres parties également responsables (en tout ou partie).**

■ Bien évidemment si cette investigation est menée de manière indépendante par des experts externes, cela limite le risque qu'elle soit contestée par les parties adverses. Nous avons quelques exemples récents.

Cas pratique: Lors d'un cas récent, un criminel s'est **introduit dans les systèmes** d'un fonds d'investissement au Luxembourg. Il a **analysé les communications avec la banque, les documents** utilisés, les processus. Ce criminel a ensuite envoyé un email à la banque afin de remplacer la « **call-back list** ». Quelques jours plus tard, le criminel a demandé à la banque d'effectuer un **virement d'un million de dollars** vers une contrepartie en Amérique du Sud. La banque a effectué **un call-back** pour s'assurer que la demande était authentique, sauf que la call-back list avait été remplacée, le virement a été effectué.

L'investigation a permis de démontrer que la banque avait mis en place un environnement de contrôle suffisant, et que les procédures avaient été respectées à la lettre, démontrant également que les emails venaient réellement du fonds d'investissement et que la banque n'aurait pas pu savoir qu'il s'agissait d'une fraude.

Les principales étapes d'une investigation objective et indépendante

1. **Sécuriser et collecter des preuves** y compris numériques, logs, emails et échanges avec le client, communications internes mentionnant le client ou les transactions frauduleuses, transactions, documents) de manière **Forensic** garantissant l'intégrité des données et leur **admissibilité légale**.

2. **Analyser les flux financiers** suspects via des outils comme Relativity, capables de traiter des millions de transactions en croisant données SWIFT, virements SEPA, historiques de comptes, emails.

3. **Reconstituer les chaînes de compromission** : examen des emails, analyse des journaux d'accès aux systèmes critiques, etc.

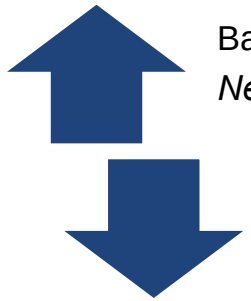
■ La revue de ces éléments permet de mieux comprendre la nature des échanges, de déceler un potentiel changement, et de reconstituer les chaînes de compromission.

■ La revue de l'environnement de contrôle est aussi extrêmement importante, y compris les contrôles automatisés par des systèmes informatiques. Ceci permet d'identifier de potentielles faiblesses et défaillances et d'y remédier.

Recours entre co-responsables

- **Recours contre l'auteur de l'infraction primaire**
  - Difficultés pratiques
  - Recours à concurrence de 100 %

- **Recours contre d'autres intermédiaires**
  - Intermédiaires bancaires, techniques, etc.
  - Opportunité d'introduire des recours ?
  - Base légale du recours ?
  - Partage de responsabilité
  - Illustration : TA Lux., com., 2e, 4 mai 2012, n° 706/2012



Banque luxembourgeoise
Négligence au niveau du changement d'adresse

75 %

Banque allemande
Négligence lors de l'ouverture du compte

25 %

Merci pour votre attention !


arendt