

Commission des Finances

Procès-verbal de la réunion du 29 janvier 2026

Ordre du jour :

Échange de vues avec le ministre des Finances au sujet de la motion 4623 concernant les fraudes bancaires numériques (motion de M. Ben Polidori du 15 octobre 2025)

*

Présents : Mme Diane Adehm, M. Guy Arendt, M. Maurice Bauer, M. Sven Clement, M. Franz Fayot, M. Patrick Goldschmidt, M. Claude Haagen, M. Marc Hansen, M. Ben Polidori remplaçant Mme Taina Bofferding, M. Laurent Zeimet

M. Gilles Roth, Ministre des Finances

Mme Martine Hansen, Ministre de la Protection des consommateurs

M. Claude Marx, Directeur général de la Commission de surveillance du secteur financier (CSSF)

M. Jerry Grbic, CEO de l'Association des Banques et Banquiers Luxembourg (ABBL)

M. Pascal Steichen, CEO de la Luxembourg House of Cybersecurity (LHC)

M. Marc Fischer, du Ministère de l'Agriculture, de l'Alimentation et de la Viticulture - Protection des Consommateurs

Mme Catherine Phillips, du Ministère de la Protection des consommateurs

M. Jean-Claude Neu, M. Andy Pepin, M. Vincent Thurmes, du Ministère des Finances

Mme Caroline Guezennec, de l'Administration parlementaire

Excusés : M. André Bauler, Mme Taina Bofferding, M. Michel Wolter

*

Présidence : Mme Diane Adehm, Présidente de la Commission

*

M. Ben Polidori du parti politique LSAP fait allusion aux fraudes bancaires numériques qui ont eu lieu au milieu de l'année 2025 et présente le contenu de sa motion du 15 octobre 2025 reprise en annexe et par laquelle il demande au gouvernement d'agir sur les points suivants :

1. créer un guichet unique national, avec plateforme numérique et hotline téléphonique vingt-quatre heures sur vingt-quatre, permettant de signaler en temps réel les fraudes numériques, assurant la coordination immédiate entre banques, police, autorités judiciaires et opérateurs télécoms ;

2. imposer des obligations techniques aux opérateurs de télécommunication, y compris une liste noire centralisée des numéros frauduleux, des règles d'authentification stricte pour les communications sensibles, et des sanctions claires en cas de manquement ;
3. mettre en œuvre, dans les meilleurs délais, une adaptation du cadre législatif national, en s'inspirant des principes contenus dans les projets de directive PSD3 et de règlement PSR, notamment en ce qui concerne l'inversion de la charge de la preuve en cas de fraude numérique, ainsi que la mise en place d'une obligation claire de remboursement des victimes par les établissements financiers, sauf en cas de négligence grave et démontrée de leur part ;
4. instaurer un protocole d'intervention rapide entre banques et forces de l'ordre, permettant le blocage immédiat de transferts suspects et l'assistance rapide aux victimes ;
5. évaluer l'impact de la récente campagne nationale de sensibilisation sur les risques de fraude en ligne et les gestes de prévention, en ciblant en priorité l'effet escompté auprès des publics vulnérables, et présenter cette évaluation à la Chambre des Députés ;
6. réaliser une étude transversale du cadre actuel de protection des consommateurs dans l'espace numérique, incluant les services financiers, les communications électroniques et les plateformes numériques, afin d'identifier les lacunes juridiques et les pistes d'amélioration en matière de droits, de sécurité et de recours effectif pour les consommateurs.

Le ministre des Finances conçoit que le sujet est important pour les citoyens et signale qu'il est pris très au sérieux par le gouvernement, la CSSF et l'ABBL. Il est, en effet, primordial de préserver la confiance des citoyens dans le secteur financier luxembourgeois et donc d'agir ensemble (gouvernement, Chambre des Députés, CSSF et ABBL) dans cette direction.

Le ministre des Finances revient au point 3 de la motion concernant la directive PSD3 (Directive sur les services de paiement 3) et le règlement PSR (Règlement sur les services de paiement). Le Luxembourg souhaite figurer parmi les premiers États membres à transposer et mettre en œuvre ces nouvelles règles arrêtées, dans le cadre d'un accord politique provisoire au niveau européen fin novembre 2025. Ces dispositifs renforcent la protection contre la fraude et notamment contre le *spoofing* et le *phishing*. Le *spoofing* (ou usurpation d'identité en français) est une cyberattaque au cours de laquelle un fraudeur falsifie des données (adresse e-mail, numéro de téléphone, IP) pour se faire passer pour une source de confiance afin de tromper la victime pour voler des données personnelles ou des informations bancaires. Parmi les nouveautés introduites par le règlement PSR figure la disposition selon laquelle, lorsqu'un utilisateur de services de paiement qui est un consommateur a été manipulé par un tiers se faisant passer pour la banque du client, en utilisant illégalement des canaux de communication attribués à celle-ci, et que cette manipulation donne lieu à des opérations frauduleuses autorisées par le client, les banques seront tenues de rembourser ces clients victimes de *spoofing*. Le client aura pour obligation de signaler la fraude à la police et à sa banque dès qu'il en a connaissance et la banque ne pourra refuser le remboursement que si elle prouve un acte frauduleux ou une « négligence grave » de la part du client (renversement de la charge de la preuve).

De plus, le règlement PSR prévoit que les grandes plateformes et réseaux sociaux pourront être tenus responsables si un utilisateur est victime d'une fraude via une publicité ou un contenu frauduleux qu'elles n'auraient pas retiré après signalement.

Le paquet PSR/PSD3 comporte un volet préventif qui vise à bloquer la fraude *avant* qu'elle ne se produise. Ainsi, le paquet législatif européen prévoit un monitoring renforcé des transactions par les banques, le blocage d'instruments financiers en cas de doute d'usage frauduleux, la non-exécution de transactions douteuses, l'introduction de l'IBAN-check obligatoire par les banques, l'introduction de limites de paiement par les clients pour limiter l'exposition en cas de vol de données.

Si une banque ne respecte pas les nouvelles règles du paquet PSR/PSD3, elle s'expose à des sanctions administratives et à une obligation d'indemnisation des clients.

Finalement, le règlement PSR introduit des obligations de partage de données entre prestataires de services de paiement (PSP) et d'autres secteurs (notamment celui des télécoms) pour identifier les schémas de fraude. Il appartient à la Commission européenne de mettre en place une plateforme d'échange de données européenne à cet effet.

Le ministre conclut en s'engageant à faire en sorte que le paquet PSR/PSD3 soit transposé/mis en œuvre le plus rapidement possible (à savoir que des travaux techniques et juridiques sont encore en cours de finalisation au niveau européen).

La ministre de la Protection des consommateurs revient au point 5 de la motion demandant une évaluation de l'impact de la récente campagne nationale de sensibilisation sur les risques de fraude en ligne et les gestes de prévention. Elle signale que la Luxembourg House of Cybersecurity (LHC) a orchestré cette campagne. Le CEO de la LHC présente la campagne en question en fin de réunion.

En ce qui concerne le cadre légal actuel, la ministre cite la multitude de règlements et directives européens qui ont pour but de protéger les consommateurs :

- Unfair commercial practices directive ;
- Consumer rights directive ;
- Digital services act depuis 2024 ;
- Digital markets act depuis 2024 ;
- AI act, applicable progressivement jusqu'à son application complète en 2027 ;
- Cyber resilience act, idem.

La ministre précise que le gouvernement s'efforce de transposer et de mettre en œuvre les directives et règlements le plus rapidement possible.

M. Claude Marx, Directeur général de la Commission de surveillance du secteur financier (CSSF) explique que le paquet PSR/PSD3 prévoit également des obligations en matière de sensibilisation et d'éducation financière des consommateurs. De plus, les banques devront mettre en place davantage de systèmes de monitoring et de prévention de la fraude.

L'EBA (European Banking Authority) a déjà publié des lignes directrices sur la sensibilisation et l'éducation financière dans le passé. Au Luxembourg, la sensibilisation financière du grand public est déjà avancée. La CSSF a participé à la campagne récente de la LHC menée au cours de l'été et en décembre 2025. D'autres initiatives dans ce sens sont régulièrement lancées par l'ABBL, la CSSF et d'autres organismes. La CSSF dispose d'ailleurs d'un site internet dédié à l'éducation financière (www.letzfin.lu). Il est, de plus, utile que les médias diffusent les avertissements émis par la CSSF et il est également important d'agir au niveau des réseaux sociaux qui sont souvent utilisés par les fraudeurs.

Le hasard veut qu'aujourd'hui-même sera publiée une vidéo sur la cyberfraude développée par la CSSF et une banque de détail luxembourgeoise. La CSSF prévoit également de publier aujourd'hui de nouveaux factsheets sur les escroqueries crypto et la fraude financière et escroquerie en ligne réalisées à l'aide de l'IA.

L'ensemble de ces initiatives montre que le sujet est pris très au sérieux – il est important de sensibiliser les citoyens dès leur plus jeune âge et donc aussi au sein des lycées.

Le ministre des Finances ajoute que des travaux de modification de la loi organique de la CSSF sont en cours afin de souligner le rôle de la CSSF en matière d'éducation financière à celle-ci. (cf projet de loi 8705)

M. Jerry Grbic, CEO de l'Association des Banques et Banquiers Luxembourg (ABBL) confirme que la sensibilisation et l'éducation financière doivent avoir lieu à tous les niveaux de la population. L'ABBL prend le sujet très au sérieux ; elle a d'ailleurs été le plus grand contributeur financier à la dernière campagne de sensibilisation. Il est prévu de réitérer des campagnes de ce type, mais davantage de moyens financiers sont nécessaires pour agrandir leur périmètre afin de toucher un public encore plus large et diversifié. La dernière campagne a coûté environ 220.000 euros.

La sensibilisation de la population est d'autant plus essentielle que les banques font d'importants efforts au niveau technologique pour protéger et sécuriser leurs systèmes et que le point faible de ces systèmes réside malheureusement dans l'humain qui les utilise. Aux Pays-Bas, les victimes de fraudes bancaires suivent des traitements similaires à ceux utilisés dans la lutte contre les addictions (Suchtbekämpfung).

Les banques améliorent leur technologie en permanence et il n'est donc pas considéré comme normal qu'elles soient contraintes de rembourser les victimes dans tous les cas de fraude réussie. Une telle façon de procéder risquerait d'entraîner une baisse de la vigilance des clients ou même de tenter certaines personnes à commettre de fausses fraudes pour obtenir un remboursement. (Il a été constaté qu'il existe beaucoup de cas de « money muling » au Luxembourg et que ces actes sont surtout commis par de jeunes personnes inconscientes de l'aspect criminel de ce « service » rendu.) Il est donc important que les banques puissent invoquer la négligence des clients dans certains cas de fraude.

Le CEO de l'ABBL salue qu'à l'avenir les opérateurs de télécommunication et de plateformes de réseaux sociaux soient associés au partage de données dans le cas de fraudes bancaires numériques.

Faisant allusion au point 1 de la motion demandant la création d'un guichet unique national, avec hotline téléphonique 24/24, le CEO de l'ABBL explique qu'un tel service existe déjà, son numéro d'appel étant le 49 10 10. Ce numéro doit être appelé pour bloquer les cartes de paiement, mais, depuis le 24 novembre 2023, également pour bloquer l'accès Luxtrust. Les futures campagnes de sensibilisation de la population (pour lesquelles des fonds sont nécessaires) devront également faire de la publicité pour ce numéro d'appel.

M. Pascal Steichen, CEO de la Luxembourg House of Cybersecurity (LHC) fournit les informations suivantes :

Une campagne nationale de lutte contre la cyberfraude a été menée en 2025. La LHC, l'ABBL et BeeSecure ont coordonné cette campagne et 12 acteurs additionnels y ont été impliqués (pour la liste complète, il est renvoyé au site www.cyberfraud.lu). Le ministre de l'Économie a lancé la campagne le 5 juin 2025 dans le cadre d'une conférence.

La campagne comportait 2 vagues de 2 semaines (en raison du budget limité et du peu de temps de préparation), essentiellement via les médias digitaux : plateformes de facebook, instagram, snapchat, youtube et sites de médias nationaux (dont RTL) et étrangers (150 plateformes/sites au total).

En juin 2025, la campagne a atteint 6 millions d'impressions et 26.000 clics ; la « click through rate » s'est élevée à 0,55% (taux relativement correct).

En novembre 2025, la campagne a atteint 3 millions d'impressions, mais plus de clics qu'au cours de la première vague. Elle a, cette fois-ci, également pu être diffusée sur la plateforme spotify.

Il est prévu de poursuivre les efforts dans ce sens. En 2026, le contenu existant sera développé et pourra être réutilisé par les acteurs participant à la campagne via leurs propres canaux. Il a été très bénéfique que ces acteurs aient pu se mettre d'accord sur un message commun et agir de manière solidaire.

Les cyberattaques sont très fréquentes et menées par des criminels professionnels. Il s'agit d'être extrêmement réactif face à ces attaques. La 5^e stratégie nationale de cybersécurité, mise en œuvre en collaboration avec les acteurs du secteur financier, poursuit cet objectif.

Évoquant les fraudes qui ont eu lieu via des faux sites de la BIL, M. Jerry Grbic, CEO de l'ABBL indique que les banques suivent ces phénomènes de très près et essaient de faire fermer ces sites. Or, il arrive souvent que ces sites soient hébergés dans des pays peu coopératifs, d'où des délais plus longs pour leur suppression.

M. Pascal Steichen, CEO de la LHC confirme ces difficultés. Les criminels choisissent ces pays en connaissance de cause. La coopération internationale des polices fonctionne bien, mais prend du temps. Il arrive aussi que des membres d'un CERT (Cyber emergency response team) luxembourgeois interviennent et demandent directement aux hébergeurs de fermer les sites frauduleux.

De l'échange de vues subséquent, il y a lieu de retenir les éléments suivants :

- En réponse à une question de M. Ben Polidori, le ministre des Finances indique que le règlement PSR a été adopté sur base d'un accord politique provisoire en novembre 2025 et est en cours de finalisation technique.

Un représentant du ministère des Finances ajoute que le paquet est volumineux et devrait être finalisé au premier trimestre 2026 pour entrer en vigueur à partir de ce moment-là. L'entrée en application de ses dispositions aura lieu au cours des 18 à 24 mois suivant l'entrée en vigueur, conformément au texte européen arrêté, afin de laisser le temps aux acteurs concernés de s'y préparer.

Le ministre des Finances souhaite que les banques de la place financière luxembourgeoise soient prêtes le plus rapidement possible.

Le CEO de l'ABBL est d'accord, mais attire l'attention sur le fait que certains points restent encore à être clarifiés ; il cite pour exemple la coopération entre les banques et les opérateurs de télécoms et son impact éventuel sur les dispositions du GDPR.

- M. Polidori évoque la coopération prévue par le règlement PSR entre les établissements de paiement et les opérateurs de télécoms et souhaite savoir si ces derniers pourront dorénavant également être considérés comme responsables en cas de fraude.

Le ministre des Finances renvoie à l'article 59a de la PSR relatif aux futures obligations des opérateurs de télécom.

Un représentant du ministère des Finances précise que le règlement PSR s'applique aux établissements de paiement et non directement aux opérateurs de télécom. Il prévoit une disposition générale de coopération entre banques et opérateurs de télécoms, mais ne va pas davantage dans le détail.

- M. Polidori comprend que la fermeture d'un site frauduleux situé à l'étranger prenne du temps. Il demande s'il ne serait pas possible d'envisager des moyens plus efficaces en légiférant.
- M. Sven Clement de la sensibilité politique Piraten indique qu'à l'heure actuelle, en cas d'usurpation d'identité d'un employé bancaire, la banque est contrainte de rembourser la victime de la fraude, mais que le cas d'une usurpation d'identité d'une banque ne semble pas encore tout à fait réglé. Il souhaite connaître la position du Luxembourg à ce sujet.

Le ministre des Finances fait référence à l'article 59 de la PSR selon lequel la victime est également protégée dans le 2^e cas mentionné par M. Clement (renversement de la charge de la preuve).

Annexe :

Motion de M. Ben Polidori du 25 octobre 2025

Procès-verbal approuvé et certifié exact
