Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

Bank of Lithuania
Law and Licensing Department
Director Arūnas Raišutis

By email prieziura@lb.lt, jgruodiene@lb.lt

13 October 2023

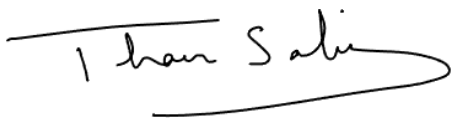
Dear Arūnas Raišutis,

Re: EMA response to the Fraud Prevention Guidelines of the Bank of Lithuania

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

The EMA welcomes the Bank of Lithuania's initiative in providing guidance to payment service providers (PSPs) on its expectations with regards to fraud prevention. We acknowledge the importance of tackling fraud, and believe that doing this successfully requires a balanced and considered approach, and cross-sector support from industry as well as customer engagement.

As a matter of principle, the EMA does not believe it is appropriate to hold PSPs responsible for losses caused by fraud where they were not at fault. In general, liability should be connected to fault, but in the case of impersonation or other scams, these cases, PSPs have limited or no means of identifying or preventing the fraud from occurring.

The EMA also supports a harmonised approach to fraud prevention and mitigation across the EU, to avoid a situation where consumers in Member States where there is automatic reimbursement/refund are targeted by fraudsters as they may be seen as "easier targets".

The EMA welcomes this opportunity to comment on the draft Fraud Prevention Guidelines ("Guidelines") prepared by the Bank of Lithuania and has the following comments to make.

- **Definition of Fraud - Paragraph 5.1**

Para 5.1 defines "Fraud" as follows:

"5.1 **Fraud**:
5.1.1. extortion or theft of payment instruments and/or data of a person(s) (payment service user(s), PSU) with the intention of unlawfully carrying out operations or concluding transactions in the name of the PSU;
5.1.2. initiation and execution of a payment transaction by deception, misleading the payer as to the purpose and consequences of the payment transaction or other circumstances, where the payment instrument or its personalised security data are used by a non-legitimate owner to gain fraudulent or unauthorised access to a payment account."

We note that this definition is not aligned with that in the EBA Guidelines on fraud reporting or with PSD2, where a clear distinction is made between unauthorised transactions and authorised transactions (manipulation of the payer). It also does not appear to be consistent with the remainder of the BoL Fraud Guidelines, which include a test to determine whether or not a payment is authorised. We would recommend instead aligning the definition of Fraud to those set out in current EU texts, to maintain a harmonised approach. This will allow firms operating in Member States other than Lithuania to maintain a consistent EU policy in relation to fraud, and provide customers of Lithuanian PSPs with a consistent experience regarding refunds and complaint-handling.

We propose that the Fraud Guidelines differentiate between unauthorised transactions and authorised fraudulent transactions in line with the EBA Guidelines on Fraud reporting under PSD2, paragraph 1.1:

English text	Lithuanian text
1.1. For the purposes of reporting statistical data on fraud in accordance with these Guidelines, the payment service provider should report for each reporting period: *a. unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transactions'); and* *b. payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer').*	*1.1 Norėdamas pateikti statistinius duomenis apie suk**čiavimą pagal šias gaires kiekvieną** ataskaitinį laikotarpį mokėjimo paslaugų teikėjas turėtų pranešti apie:* *a. atliktas neleistinas mokėjimo operacijas, įskaitant operacijas, atliktas praradus, pavogus arba neteisėtai pasisavinus neskelbtinus mokėjimo duomenis arba mokėjimo priemonę, nesvarbu, ar tai įmanoma susieti su mokėtoju prieš mokėjimą ar ne ir ar tai įvyko dėl didelio mokėtojo aplaidumo arba atlikta nesant mokėtojo sutikimo ar ne (toliau – neautorizuotos mokėjimo operacijos); ir* *b. mokėjimo operacijas, atliktas, kai suk**čius** manipuliuoja mokėtoju, kad šis išduotų mokėjimo nurodymą arba sąžiningai pavestų tai padaryti mokėjimo paslaugų teikėjui, kad mokėjimas būtų atliktas į mokėjimo sąskaitą, kuri, jo įsitikinimu, priklauso teisėtam mokėjimo gavėjui (toliau – manipuliavimas mokėtoju).*

- **Differences between an authorised fraudulent transaction and an unauthorised transaction - Paragraph 67, 67.1, 67.2, Paragraph 70, Annex 2**

Paragraph 67 proposes a new test for assessing whether the transaction is an authorised or an unauthorised transaction, consisting of a two-part criteria:

1. **objective element:** whether the transactions has been validated in the manner in which the parties have agreed to validate the submitted payment instructions in the concluded contract; and
2. **subjective element:** whether the transaction was made with the knowledge and consent of the PSU, i.e. whether there was a will on the part of the PSU to carry out the relevant payment transaction.

As to the subjective element, Paragraph 70 of the Guidelines suggests that where the payer is manipulated by a fraudster to authorise a transaction, such transaction could be considered unauthorised:

"70. It should be noted that a payment transaction, although formally authorised in the manner agreed between the parties, cannot be considered to have been duly authorised by the PSU itself, if there is evidence of deficiencies in the payer's intention to carry out the transaction (i.e. failure to express this intention himself, due to the influence of third parties, due to the misleading failure to understand the true meaning and consequences of his actions, etc.). If there is sufficient objective evidence that the disputed payment transaction may have been initiated and authorised by the will and unlawful actions of third parties, i.e. the unlawful misappropriation of the PSU payment instrument and/or its personalised security data, as well as the fundamental misleading of the

applicant as to the circumstances of the transaction or the consequences of the actions required to authorise the transaction, the payment transaction would have to be considered as unauthorised (the subjective element of the authorisation of a payment transaction)."

The position suggested in the draft Guidelines is different from the position established under PSD2. The meaning of "authorised" vs "unauthorised" transactions is derived from Art 64 PSD: a transaction is *authorised* "*if the payer has given consent to execute the payment transaction*", where the consent has to be given *"in the form agreed between the payer and the payment service provider."* Conversely, a transaction would be considered *unauthorised* if the payer has not provided their consent to the execution of a transaction to their PSP, in the form agreed with the PSP for giving such consent.

The PSD2 text provides for consideration of the objective element of authorisation only: either the payer did give their consent by validating the transaction in the form agreed with their PSP (authorised transaction), or did not (unauthorised transaction). There is no further requirement for PSPs to enquire into, or take account of, the payer's state of mind when authorising a transaction. In other words, the possible manipulation of the payer to authenticate the payment would lead to the transaction being authorised and fraudulent, but not an "unauthorised transaction" under the rules established under PSD2. This is also supported by the EBA Guidelines on Fraud reporting under PSD2, which clearly distinguish between unauthorised transactions, and manipulation of the payer transactions.

This has a significant impact on the reimbursement of such fraudulent transactions: while unauthorised transactions must be reimbursed under PSD2 by the PSP in most cases, this obligation does not extend to *authorised* fraudulent transactions as understood under PSD2.

Extending the definition of unauthorised transactions to certain authorised fraudulent transactions where the payer has been manipulated is not in line with current industry practice, is a significant divergence from PSD2 and the EBA Guidelines on Fraud reporting under PSD2, and would place a disproportionate financial burden put on Lithuanian PSPs. Most importantly, it goes against the general legal principles of liability, i.e. that liability should attach where there is a fault. In other words, PSPs should be held liable to refund the customer where they are at fault. However, if a customer is manipulated into making a payment to a recipient they did not intend, but has authorised the payment, the PSP is under an obligation to execute the payment under the customer's instruction. They are not in a position to know whether the customer has been manipulated, particularly when the payment is made remotely, and they are not in a position to prevent the fraud, unlike in the case of unauthorised transactions.

The EMA therefore disagrees with the addition of a subjective element in qualifying transactions as authorised, and with the suggestion that manipulation of the payer by a fraudster to authorise a payment is to be considered an unauthorised transaction, as is currently proposed in the draft Guidelines. We believe this would constitute a significant

departure from the PSD2 meaning of "unauthorised transactions" and the PSP's liability for unauthorised transactions under PSD2. We query whether such a significant departure complies with the PSD2 maximum harmonisation requirements. Considering also the potential financial consequences to the PSPs from changes in the unauthorised transaction refund liability would be significant, we query whether Bank of Lithuania's Guidelines is the appropriate instrument to affect this change.

We therefore support a harmonised approach to unauthorised transactions that aligns with PSD2 and suggest deleting paragraph 67.2 and modifying the Paragraph 70 to align with the PSD2 meaning of authorised and unauthorised transactions.

- **Reimbursement of Fraud by PSPs - Paragraph 70-73, 77**

As set out above, the guidelines on reimbursement appear to go beyond the requirements in PSD2.

While the reimbursement by PSPs of unauthorised transactions as defined under PSD2 is mandatory, PSPs should not be held responsible for reimbursing fraudulent authorised transactions, where the payer has been manipulated into authorising a payment. These cases could include the following typologies for example, social engineering attacks whereby the fraudster "convinces" the legitimate user to transfer funds to an account controlled by the fraudster (romance, impersonation, investment scams).

It is essential to maintain and assure consistency of treatment of such fraud typologies at EU level, to allow for the PSU as well as the PSP a clear and understandable legal framework in regards to fraud and reimbursement.

- **Possibility to reimburse victims and repatriate funds**

Under Article 16 of the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, it appears that unless they receive a written instruction from the FCIS following notification of a suspicious transaction, Lithuanian PSPs may only freeze funds for a maximum of 10 days. After this time, they must "resume" the transaction and release the funds to the recipient PSU.

For PSPs operating cross-border, the FCIS will often not be in a position to issue a written instruction within the required 10 days, even in cases where the fraud is proven by the sending PSP. In these cases, the recipient PSP has no legal option to freeze the funds beyond the 10 days, and must release them to the recipient PSU. However, in cases of identified fraud, the PSU will often be the fraudster.

Lithuanian PSPs operating cross-border would like to be able to return fraudulently acquired funds back to the sending PSP in order to allow them to reimburse their customer. However, under Paragraph 1 of Article 29 of the Law of the Republic of Lithuania on Payments returning

such funds without the consent of the PSU (the fraudster) would mean that the payment would be unauthorised.

Therefore, the EMA suggests additional guidelines that clarify the rules around freezing of funds.

The guidelines should clarify that in cases where the payer's PSP informs the payee's PSP of a fraudulent transaction, and after a proper investigation, Lithuanian PSPs may return the funds back to the victim when possible, by sending the frozen funds back to the payer's PSP.

In other Member States, this is good industry practice, and PSPs in this situation regularly notify each other of a transaction that has been flagged by the payer (and potential victim) as fraudulent. Following an investigation, the payee's PSP may then decide to cancel the transaction, and send the money back to the payer's PSP, in practice permitting the reimbursement of the victim. This cooperation mitigates the impact on fraud victims, while also encouraging the communication and sharing of fraud typologies between European PSPs and reducing overall losses to fraud.

Lithuanian PSPs are excluded from this business practice, as the current legal framework does not appear to permit the returning of these funds without the consent of the PSU. This gives the impression to other PSPs in the EU that Lithuanian PSPs are not willing to collaborate to combat fraud.

A clarification on this topic in the Guidelines would allow Lithuanian PSPs to provide a safer environment for their PSUs, as well as a higher level of harmonisation between EU Member States.

- **Status of the Guidelines and promotion of the cooperation as a way to prevent and mitigate fraud**

The EMA supports the Bank of Lithuania's efforts to combat fraud, but recommends that guidelines on dealing with fraud should be prepared and drafted with the participation of industry. From our experience in combating fraud in other jurisdictions, the most effective platforms and guidelines result from cooperation between industry and the different public bodies involved in the fight against fraud (e.g. regulators, law enforcement, government departments).

While guidelines are very useful, it is essential that they remain sufficiently flexible to adapt to the ever-changing nature of fraud and new typologies, and to allow financial institutions to adapt them to their own business models. While we understand that these guidelines are not meant to be mandatory *per se*, as they are published by the Bank of Lithuania, we expect they will be treated by the courts, dispute resolution bodies, and payment service users as the legal

expectation for financial institutions in Lithuania. Therefore, we strongly recommend engagement with industry before finalising these guidelines.

In regards to the cooperation between the public and the private sector, one aspect of fraud combating that we would recommend is cross-border cooperation between financial firms and the public sector, including law enforcement. Sharing emerging typologies, mitigating factors and red flags on a regular basis, and better cooperation and data sharing between the different national law enforcement bodies would allow for a more swift and effective resolution of cross-border fraud cases.

List of Members

- AAVE LIMITED
- Airbnb Inc
- Airwallex (UK) Limited
- Allegro Group
- Amazon
- American Express
- ArcaPay UAB
- Banked
- Bitstamp
- BlaBla Connect UK Ltd
- Blackhawk Network EMEA Limited
- Boku Inc
- Booking Holdings Financial Services International Limited
- BVNK
- CashFlows
- Checkout Ltd
- Circle
- Citadel Commerce UK Ltd
- Contis
- Corner Banca SA
- Crypto.com
- eBay Sarl
- ECOMMPAY Limited
- Em@ney Plc
- emerchantpay Group Ltd
- Etsy Ireland UC
- Euronet Worldwide Inc
- Facebook Payments International Ltd
- Financial House Limited
- First Rate Exchange Services
- FIS
- Flex-e-card
- Flywire
- Gemini
- Globepay Limited
- GoCardless Ltd
- Google Payment Ltd
- HUBUC
- IDT Financial Services Limited
- Imagor SA
- Ixaris Systems Ltd
- J. P. Morgan Mobility Payments Solutions S. A.
- Modulr Finance Limited
- MONAVATE
- MONETLEY LTD
- Moneyhub Financial Technology Ltd
- Moorwand
- MuchBetter
- myPOS Payments Ltd
- Nuvei Financial Services Ltd
- OFX
- OKG Payment Services Ltd
- OKTO
- One Money Mail Ltd
- OpenPayd
- Own.Solutions
- Park Card Services Limited
- Paymentsense Limited
- Paynt

- Payoneer Europe Limited
- PayPal Europe Ltd
- Paysafe Group
- Paysend EU DAC
- Plaid
- PPRO Financial Ltd
- PPS
- Ramp Swaps Ltd
- Remitly
- Revolut
- Ripple
- Securiclick Limited
- Segpay
- Skrill Limited
- Soldo Financial Services Ireland DAC
- Square
- Stripe
- SumUp Limited
- Swile Payment
- Syspay Ltd
- Transact Payments Limited
- TransferMate Global Payments
- TrueLayer Limited
- Trustly Group AB
- Uber BV
- VallettaPay
- Vitesse PSP Ltd
- Viva Payments SA
- Weavr Limited
- WEX Europe UK Limited
- Wise
- WorldFirst
- Worldpay
- Yapily Ltd