

**Statement on Fraud Prevention Measures**

# General Provisions

Fraud management is a continuous and essential part of our operations. We actively identify, assess, and monitor risks related to fraud to ensure we can effectively prevent and address any issues that may impact our goals.

VIALET is dedicated to preventing fraud and has a strict zero-tolerance policy for any form of fraudulent activity, whether internal or external. We will thoroughly investigate any suspected or detected fraud.

We cooperate fully with law enforcement and regulatory authorities to handle and report fraud. We prioritize quick and transparent reporting to meet legal requirements and minimize any potential harm.

# Scope

The Statement applies to all aspects of the Company's operations and involves every member of the organisation in preventing and detecting fraud, promoting a culture of vigilance and responsibility. In addition, the Statement serves as an educating measure for Company’s customers, employees, and shareholders.

# Requested information/documentation from customers

When requesting information from a customer due to potential fraud, VIALET shall provide a detailed explanation of the specific documents and information required. This includes outlining the content, format, and issuing authorities of the documents.

Regular contact shall be maintained with the customer regarding the requested documentation. If the customer is unable to provide the exact documents in the specified format, alternatives that offer equivalent information can be arranged. Customers are welcome to seek further clarification or guidance as needed.

# Payment order cancellation

To ensure the security of VIALET’s customers' funds and payment services, the Company shall:

* Contact customers who report fraud outside business hours by the next business day.
* Ensure that reported fraud on payment cards and access to payment accounts is blocked within the same business day.
* Initiate the procedure to revoke the payment order or consent to initiate or execute a payment transaction (where consent has been given to a payment initiation service provider or payee) and undertake similar actions upon receipt of notification on the same business day.
* Provide information on fraud reporting and transaction dispute procedures on the Company’s website [www.vialet.eu](http://www.vialet.eu);
* Maintain timely access to Customer Service through support@vialet.eu;
* Promptly notify the payee's PSP and relevant financial institutions within one business day of receiving a customer's request;
* Cooperate with other financial institutions to stop or cancel transactions and make reasonable efforts to recover funds.

Company should respond promptly to customer enquiries and requests:

* Regarding any inconsistencies between the payee’s details in the payment order and the information the Company has on the payee;
* Regarding revocation of a payment order or consent, prioritizing such requests without additional time limits;
* Clarifying the purpose of the customer’s request to cancel a payment transaction and providing necessary information to assist the customer in deciding on further action.

# Customer awareness

To educate customers about fraud and how to protect themselves, the Company takes a proactive approach by:

* Keeping a fraud prevention page on the website [www.vialet.eu](http://www.vialet.eu) that highlights the importance of fraud prevention.
* Publishing articles with statistics and updates on effective fraud prevention practices and fraud types.
* Sharing Periodically sharing information about phishing, vishing, and other fraud types via email, private messages, or during live consultations.

Customer Service shall inform customers about changes in payment services through electronic means without including direct links to the customer’s internet banking platform to ensure security.

VIALET ensures that customers are clearly informed about when they might be asked to provide specific confidential personal information, such as their personal identification number or ID number, but not their personalized security features for payment devices. For example, if a customer wants to increase transaction limits via e-banking, VIALET may contact the customer to request confidential information to verify the authenticity of the request.

Customer Service shall assist customers with all matters and respond promptly to requests for help and notifications, especially in unusual or security-related issues with payment services. If a customer becomes a victim of fraud, Customer Service must proactively reach out and offer guidance on the next steps. Assistance and advice provided will be updated to address new threats and vulnerabilities.

Customers can report fraud by emailing support@vialet.eu or complaints@vialet.eu. To maintain proactive measures and ensure the integrity of the financial market, the Company will also review fraud reports from any relevant party through various communication channels, including live consultations, messages, and publications.

# Fraud types and their red flags

Fraud involves deceptive activities carried out by individuals or entities outside the Company. This includes schemes like phishing scams, identity theft, unauthorized access attempts, and more. Effectively understanding and addressing these risks is crucial for maintaining the integrity of operations and protecting customers' assets.

**Phishing and Vhishing**

Phishing is a social engineering technique used online to deceive individuals into revealing sensitive information like usernames, passwords, bank account numbers, and payment card details by pretending to be a trustworthy source. Vishing is a similar type of fraud but occurs over the phone, where scammers use calls to extract personal data.

|  |
| --- |
| **Red Flags** |
| * Any unsolicited requests for personal or financial information, especially via email, SMS, or phone calls;
* Urgent or threatening language;
* Unusual URLs or domain names;
* Unusual email domain;
* Requests for account verification;
* Suspicious links;
* Poor grammar and spelling;
* Unsolicited attachments or downloads.
 |

**Identity theft**

Fraudsters steal personal information to impersonate individuals, open fraudulent accounts, or conduct unauthorised transactions within electronic money platforms. Identity theft can occur after fraudsters gain access to personal information through methods such as phishing scams, data breaches, or social engineering tactics.

|  |
| --- |
| **Red Flags** |
| * Unexplained withdrawals or payments;
* Suspicious emails or messages;
* Problems with accessing personal accounts;
* Requests for verification;
* Unusual email communications.
 |

**Romance Fraud**

Romance fraud involves people being tricked into sending money to criminals who gain their trust and convince them that they are in a genuine relationship. They use language to manipulate, persuade and exploit so that requests for money do not raise alarm bells. These requests might be highly emotive, such as criminals claiming they need money for emergency medical care, or to pay for transport costs to visit the victim if they are overseas.

|  |
| --- |
| **Red Flags** |
| * Emotional manipulation;
* Requests for financial aid;
* Avoiding face-to-face meetings;
* Inconsistencies in stories;
* Isolation from friends and family;
* Communication in overly flattering language;
* Reluctance to provide personal details.
 |

**Stolen Card Fraud**

This fraud type involves fraudsters making unauthorised payments online, usually in massive pushes like card testing or BIN attacks.

*Card testing* is an automated process where fraudsters validate stolen credit card information by making small transactions, typically on e-commerce websites. These transactions serve to test the validity of the card details and identify which cards are still active and usable for fraudulent purposes.

*BIN attacks* involve targeting specific ranges of credit or debit card numbers issued by a particular bank or financial institution. Each bank identification number (BIN) identifies the institution that issued the card, as well as other details such as card type and brand.

These two fraud types apply to VIALET’s acquiring product only.

|  |
| --- |
| **Red Flags** |
| * Unusual time of the transactions;
* Transactions that are incoming in unusually fast pace;
* Repeated use of BINs (Bank Identification Numbers);
* Slight variations in card details (one or two numbers off);
* High amount of failed authorizations;
* Low and round value purchases (10 EUR, 20 EUR).
 |

**Money mules**

Money Mules areindividuals who are recruited, often unknowingly, by criminals to transfer illegally obtained money between different accounts or jurisdictions. These individuals are used as intermediaries to launder money and conceal the true origins of illicit funds.

|  |
| --- |
| **Red Flags** |
| * Unexpected job offers;
* Vague/unusual job descriptions;
* Lack of employment documentation;
* High payments for minimal work;
* Lack of clear communication;
* No clear employment contracts.
 |

**Investment fraud**

Investment fraudinvolves deceptive practices where investors are misled about the nature of an investment opportunity. This can include misrepresenting the potential returns, the underlying assets, or the risks involved. Instead of legitimate investment activities generating returns, the scheme uses investors' funds for unauthorised purposes or personal gain. Investment fraud can take various forms beyond Ponzi schemes, such as advance fee scams, pyramid schemes, or unauthorised trading schemes.

|  |
| --- |
| **Red Flags** |
| * Unsustainable returns - Ponzi schemes typically promise unusually high or consistent returns on investment with minimal or no risk;
* Operating from high-risk jurisdiction;
* Complex investment structures;
* Promises of guaranteed returns;
* Unknown financial institutions;
* Lack of proper documentation.
 |

# Reimbursement of Losses

VIALET must ensure that handling customer complaints and requests about disputed payments complies with legal requirements and standard practices, ensuring thorough and careful assessments of each case.

Upon receiving a complaint about a disputed payment transaction, VIALET shall start the examination immediately and no later than by the end of the next working day. The examination must be completed within the maximum time limits set by legislation for handling customer complaints.

When a customer disputes a payment transaction as being executed by fraudsters or due to fraudulent activity, it must first be determined if the transaction should be considered authorized.

If the customer challenges the authorization of the payment transaction, the Company is responsible for proving that the transaction was properly authorized according to the agreed terms and procedures.

A payment transaction, although formally authorized according to agreed procedures, may still be considered unauthorized if there is evidence that the customer did not genuinely intend to execute it. This could include cases where the customer did not express intent, was influenced by a third party, or was misled about the transaction.

If there is strong evidence that the transaction was initiated through unlawful actions, such as misuse of the customer's payment instrument or security features, or significant misleading about the transaction's details, the transaction may be deemed unauthorized due to these factors.

VIALET shall thoroughly investigate the circumstances of a disputed payment transaction to assess both its authorization and the customer's conduct. This is especially crucial if the transaction is considered unauthorized due to potential customer intent (bad faith) or gross negligence.

If a disputed payment transaction is deemed authorized, compensation for damages can be pursued according to general civil liability principles.

Upon discovering or declaring a payment transaction as unauthorized, reimbursement to the customer should follow the procedure and time limits specified in Article 38 of the Payments Law.

VIALET’s liability for unauthorized payment transactions is limited to cases specified by law. The Company can be fully exempt from reimbursing the customer only if it provides evidence of the customer’s dishonesty, intent, or gross negligence.

Gross negligence, intent, or dishonesty are evaluative factors. When determining if the customer's conduct was grossly negligent (or dishonest, which is treated as intent) and led to an unauthorized transaction or loss of a payment device, VIALET evaluates the specific circumstances based on evidence that is supported and not contested by the parties involved.

A breach of the duty to protect the confidentiality of payment method security features does not automatically imply gross negligence. Customers are only liable for losses from unauthorized payment transactions if both of the following conditions are met:

* The customer fails to meet obligations under the Law on Payments regarding the use and security of payment devices.
* The customer's actions are either intentionally dishonest or involve gross negligence

The customer must cooperate with VIALET by providing all relevant information and requested data to aid in the investigation of disputed payment transactions and ensure an accurate decision on authorization and reimbursement. If the customer fails to cooperate, such as by withholding information or providing false data, VIALET will make its decision based on the available information.

VIALET’s decisions to deny compensation for losses due to fraud must be evidence-based, well-reasoned, and take into account all circumstances of the case, including the authorization of the transaction and the customer’s behaviour.

When VIALET refuses to reimburse a disputed payment, Customer Support must inform the customer in writing with reasons and supporting evidence, including details on challenging the decision.

# Final Provisions

The Statement is reviewed at least once a year or immediately after changes in relevant laws or significant circumstances. Necessary updates are made accordingly.

To help VIALET uphold top standards in fraud prevention, customers are encouraged to report any suspicious activities. Reports are investigated promptly and confidentially.

VIALET continuously monitors and improves its fraud prevention measures. If customers have questions or concerns about this Statement, they should contact VIALET’s Customer Support team at support@vialet.eu.