

I Have Fallen Victim to Online Fraud. What Should I Do?

A practical legal guide outlining immediate protective steps and the basic legal framework

July 2026

Time is critical. Contact your bank or payment service provider immediately, request the blocking of the relevant payment instruments and dispute the transaction, while preserving all available evidence.

Online fraud now takes many forms: deceptive e-mails and text messages, fraudulent websites imitating banks or public authorities, telephone calls from persons posing as officials, online sales advertisements, purported investment opportunities, account breaches and the alteration of bank details on invoices. The first twenty-four hours may prove decisive, both in limiting the loss and in preserving evidence.

1. The Most Common Forms of Online Fraud

- **Phishing / smishing:** A deceptive e-mail or text message directs the recipient to a fraudulent website and requests passwords, card details or confirmation through an application.
- **Vishing and caller ID spoofing:** A telephone call from a person posing as a bank employee, accountant, police officer or representative of a public authority. The displayed number may appear genuine.
- **Remote-access fraud:** The offender persuades the victim to install remote-control software and gains access to the device or online banking services.
- **Fraud involving online advertisements and purchases:** A fraudulent buyer or seller requests payment, card details or the use of a false link purporting to belong to a courier company or bank.
- **Altered IBAN / business e-mail compromise:** A business e-mail account is breached and a falsified invoice or message is sent containing different bank account details.
- **Investment fraud:** Promises of high and guaranteed returns on shares, crypto-assets or other investments, often through unauthorised platforms.

Regardless of the form of online fraud involved, a prompt response by the victim is usually the most important factor both in limiting the loss and in preserving critical evidence. Although every case has its own particular features, the following steps should generally be taken without delay.

2. The First Steps Following the Incident

Step 1: Contact Your Bank or Payment Service Provider Immediately

Calling the bank through its official customer-service number is generally the first step required. Request the blocking of cards, accounts, online banking access and any payment instrument that may have been compromised. State expressly that you dispute the transaction as unauthorised, provided that you did not in fact authorise it.

Step 2: Request the Recall, Freezing or Tracing of the Transfer

Where a bank transfer is involved, immediately request a recall procedure and ask your bank to contact the beneficiary bank with a view to potentially freezing the funds. A bank will not normally guarantee recovery, and even the possibility of recovering the funds diminishes as time passes.

Step 3: Submit a Written Dispute of the Transaction

Telephone notification is important, but it will not normally be sufficient on its own. Send an e-mail or submit a request through the bank's secure online environment. Ask for a reference number or written confirmation that your request has been received.

Step 4: Preserve All Evidence

Retain screenshots, e-mails with full headers where possible, text messages, telephone numbers, links, transfer receipts, IBANs, beneficiary names, conversations, advertisements, dates and times. Do not delete the application through which the communication took place, or the conversation itself, before making copies.

Step 5: Secure Your Accounts and Devices

Change your passwords using a clean and secure device, beginning with your e-mail account. Enable two-factor authentication, sign unknown devices out of your accounts and contact your mobile network provider if a SIM-swap attack is suspected.

Step 6: Report the Incident

The incident may be reported to the Hellenic Police Cyber Crime Division through telephone line 11188, through the relevant online reporting service on gov.gr, or by filing a criminal complaint with the competent police or prosecutorial authority.

Step 7: Check Whether Other Data Has Been Compromised

If you disclosed a copy of your identity document, Taxisnet credentials, card details or other personal data, notify the relevant institutions and monitor your accounts and credit activity for further attempts at fraud.

Step 8: Do Not Pay Again for Purported Recovery Services

A second fraud frequently follows the first: individuals falsely present themselves as lawyers, accountants, technicians or "recovery companies" and demand an advance payment. Avoid engaging in any such communication.

3. What the Law Provides for Banking Transactions

Law 4537/2018, which transposed the European legislation on payment services into Greek law, regulates the rights and obligations of payment service users and providers. The application of its provisions depends on the facts of each case and, in particular, on whether the transaction was genuinely unauthorised or whether the user was deceived into authorising it personally.

Article 69: The user must use the payment instrument in accordance with the applicable security terms, safeguard personalised security credentials and notify the provider without undue delay upon becoming aware of loss, theft, misappropriation or unauthorised use.

Article 71: A disputed transaction must be notified without undue delay and, as a general rule, no later than thirteen months after the debit date. The existence of this maximum period does not justify waiting: the report should be made immediately in order to secure the victim's legal position as effectively as possible.

Article 72: Where the user denies having authorised a transaction, the provider bears the burden of proving authentication, accurate recording and proper operation. The mere fact that use of the payment instrument was recorded is not, by itself, sufficient to establish authorisation, fraud or gross negligence.

Article 73: In the event of an unauthorised payment transaction, the amount must in principle be refunded immediately and no later than the end of the following business day, unless there are reasonable grounds for suspecting fraud that are duly reported to the competent authority.

Article 74: The payer's liability varies according to the circumstances. The legislation provides specific limits for consumers, while in cases of fraud or gross negligence a larger part, or the entirety, of the loss may be allocated to the payer. A finding of gross negligence is not automatic and must be supported by specific evidence.

Critical distinction: An unauthorised transaction (for example, where the offender made the transfer without consent) is different from a transaction that the user personally authorised after being deceived. In the latter case, a claim against the bank is often more difficult and requires an individual legal assessment and, potentially, recourse to the courts.

4. Criminal-Law Provisions That May Apply

Depending on the facts and the method by which the fraud was committed, several criminal-law provisions may be relevant:

- **Article 386 of the Greek Criminal Code - Fraud:** This provision covers the causing of financial loss by knowingly presenting false facts as true, unlawfully concealing or suppressing true facts, with the intention of obtaining an unlawful financial benefit.
- **Article 386A of the Greek Criminal Code - Computer Fraud:** This provision concerns financial loss caused by improperly influencing the outcome of data processing, by unauthorised interference with an information system or data, or by the other means specified in the provision.
- **Article 370B of the Greek Criminal Code - Unlawful Access:** This provision may be considered where the offender circumvents a security measure and obtains unauthorised access to an information system or electronic data.
- **Related offences:** Depending on the case, offences involving forgery, unlawful processing of personal data, breach of the confidentiality of communications, participation in a criminal organisation or money laundering may also arise.

5. What the Victim's File Should Contain

- ☐ A detailed account of the incident, including dates and times.
- ☐ Bank statements and evidence of the disputed transactions.
- ☐ The written dispute submitted to the bank and its reference number.
- ☐ The bank's responses and the applicable online-banking or card terms.
- ☐ Screenshots, messages, e-mails, links and profile details relating to the offender.
- ☐ IBANs, beneficiary details and any card or account numbers used.

- ☐ Evidence of the report submitted to the police or the Cyber Crime Division.
- ☐ A technical report or examination of the device where a breach is suspected.
- ☐ Any communication with a platform, service provider or other involved body.

6. Frequently Asked Questions

Will the Bank Definitely Refund My Money?

Not automatically in every case. The answer depends on whether the transaction was unauthorised, the authentication method used, the user's conduct, compliance with security obligations and the available evidence.

If I Disclosed the One-Time Password Myself, Do I Lose Every Right?

Not necessarily. The method of deception, the warnings issued by the bank, strong customer authentication, the sequence of events and whether gross negligence is established must all be examined.

Is a Telephone Report to the Bank Sufficient?

Telephone contact is necessary for the immediate blocking of payment instruments, but it is not sufficient. It should always be followed by a written report and transaction dispute, and evidence of submission should be retained.

Can a Bank Transfer That Has Already Been Credited Be Recovered?

Possibly, particularly where the response is immediate and the funds remain in the beneficiary's account. However, a recall is not always possible and should never be taken for granted.

Should I Contact a Lawyer Immediately?

Where there has only been a minor attempted fraud without financial loss, immediate security measures may be sufficient. Where an actual debit, a significant amount, an account breach, business fraud or a negative response from the bank is involved, prompt legal assessment by a lawyer is advisable in order to address the matter effectively.

7. Conclusion

Online fraud is a complex matter requiring a combination of technical, banking and legal measures. The first priority is to terminate the offender's access and limit the financial loss. This should be followed by a written dispute of the transaction, preservation of evidence, reporting of the incident and, where required, the out-of-court or judicial protection of the victim's rights.

Important Note

Every incident of online fraud has different factual and legal characteristics. An assessment of the victim's rights cannot be based solely on general information, but requires examination of the particular circumstances of each case. Where financial loss has occurred or a dispute arises with the bank or another involved body, promptly contacting your lawyer may prove decisive in protecting your rights effectively.

Disclaimer: This article is provided for general informational purposes only and does not constitute legal advice. The applicable provisions and the steps required depend on the specific circumstances of each case.

Sources and Key Legal Framework

- Law 4537/2018, in particular Articles 69, 71, 72, 73 and 74, as currently in force.
- Law 5019/2023, amendments concerning the payer's liability for unauthorised payment transactions.
- Greek Criminal Code (Law 4619/2019), in particular Articles 386, 386A and 370B, as currently in force.
- Hellenic Police Cyber Crime Division, cyberalert.gr and telephone line 11188.
- Gov.gr, online service for filing an identified report concerning cybercrime.