OZGURKONAKCI.COM · LOGISTICS GUIDE · 47

Fraud in trade and logistics

From payment diversion to fake forwarders, forged bills of lading and cargo theft: the common types, their first warning signs, public verification routes in Türkiye and what to do in the first hours

Author: Özgür Konakcı · Level: Beginner–Intermediate · Version: 17 November 2026

Online interactive version: **https://ozgurkonakci.com/en/guide/fraud-in-trade-and-logistics/**

SHORT ANSWER

The most common fraud in international trade is an "our bank account has changed" message from a compromised or imitated mailbox (BEC). In 2025 the FBI's IC3 received 24,768 complaints of this type with about USD 3.05 billion in reported losses. The basic safeguard is to confirm changes of bank details and cargo release requests by voice, on a phone number you already know. In Türkiye you can check that a company exists through the Trade Registry Gazette, MERSİS and the confirmation code on its e-tax certificate, and a forwarder's authorisation through its TİO certificate. If you spot a fraudulent payment, call the bank first and ask for the transfer to be recalled, then preserve the evidence and file a complaint with the prosecutor.

A short note first

This page is for information only and is not legal or security advice. If you suspect fraud, call your bank first, then use the official reporting channels together with your legal adviser. Figures are given with their sources; recommendations are our own view and are marked as such.

Types of fraud at a glance

Fraud in international trade rarely starts with a sophisticated cyberattack. It usually starts with trust placed in the wrong thing: an email that looks familiar, a document that looks genuine, a phone call made in a hurry. This page brings together the common types of fraud along the sales, payment and transport chain, their first warning signs, the public verification routes available in Türkiye, and what to do when it happens.

Fake social media accounts, digital footprint and the fake-email warnings issued by industry bodies are covered in Security: digital footprint and fraud; we do not repeat them here.

Type	How it works	First warning sign	First check
Payment diversion (BEC)	A supplier's, forwarder's or customer's mailbox is compromised or imitated, and you are told "our bank account has changed".	New bank details, urgency, a small difference in the domain name	Voice confirmation on a number you already know
Fake forwarder or carrier	A "transport company" that does not exist, or uses another firm's name, takes an advance payment or collects the cargo and disappears.	A price far below the market, a free email address, no registry details	Tax certificate, Trade Registry Gazette, TİO authorisation certificate
Forged bill of lading or documents	A bill the carrier never authorised, a forged copy, or a document with the date or port altered goes into circulation.	Number, vessel or date that does not match the carrier's records	Verify the bill through the carrier's official channel
Fake buyer	A large first order, resistance to any payment security, and requests to release documents or cargo before payment.	Insistence on open account or release without payment	Company verification and payment method
Fake supplier	A seller copying a real manufacturer's website, or one that does not exist at all, asks for payment in advance.	Newly registered domain, advance payment only, bank account in a different name	Official registry record and independent confirmation
Cargo theft and impersonation	Using the identity of a real carrier or broker, someone collects the cargo and changes the destination.	Last-minute change of driver, plate or delivery address	Confirmation through a second channel before releasing the load
Fake load postings	Non-existent loads are posted on freight platforms; carriers who bid receive a malicious link or a fake contract.	The poster pulls you off the platform or asks you to click a link	Verify the poster from an independent source
Misdeclaration	The type, quantity or weight of the goods is misstated in the documents.	A description out of line with the price, contradictions between documents	Consistency of invoice, packing list, bill of lading and VGM

Payment diversion: the "our bank account has changed" email

The FBI's Internet Crime Complaint Center (IC3) describes business email compromise (BEC) as a scam targeting businesses that work with suppliers and regularly make wire transfers. According to IC3's 2025 annual report, there were 24,768 complaints of this type with reported losses of about USD 3.05 billion. These figures cover only reports made to IC3; we did not find a comparable official statistic for Türkiye.

In international trade the typical sequence is:

1. The supplier's, forwarder's or customer's mailbox is compromised, or a domain name very close to theirs is registered.
2. The correspondence is quietly monitored for a while to learn the order, shipping and payment schedule.
3. When payment is due, an invoice resembling the real one arrives, or a letter saying "our account has changed because of an audit".
4. Urgency is created: "if it is not paid today the cargo will be stuck at the port", "don't call, I'm in a meeting".

A 2026 FBI alert lists the typical forms of lookalike domains: accounts on free email services imitating the company's name, domains with extra punctuation, different top-level domains (for example .com or .us instead of .gov), added prefixes or suffixes, and misspellings. Fraudsters also use internet calling (VoIP) and short-lived phone numbers.

How to protect yourself

- **Never accept a change of bank details by email.** The FBI recommends verifying requests through an independent second channel. In our view that channel is not the number in the email but a phone number you already know and hold on file.
- **Put a written procedure in place.** In our experience the most effective safeguard is that no change of bank details goes into the system without approval by two people and a voice confirmation. A clause in the proforma or contract saying "our bank details change only by signed letter confirmed by telephone" also puts the other side on notice.
- **Compare the account holder with the company name.** If the holder of the new account does not match the name on the invoice, or the account is in a completely different country, stop.
- **Protect your mailboxes.** Turn on multi-factor authentication. The FBI points out that new or unexplained mailbox rules you did not create (for example rules that automatically forward or delete certain emails) are a sign of compromise.
- **Warn your own customers too.** In our view a note on your invoices and email signature saying "our bank details do not change; if you receive a message saying they have, call us on a known number" also makes an attack in your name harder.

Fake forwarders, fake carriers and fake tracking pages

In our experience the first sign of a fake forwarder or carrier is the price: a quote well below the market, combined with a request for advance payment. A free email address, no fixed address or landline, a bank account in a different name from the company quoting, and vagueness about whose name the documents will be issued in are also signs to watch for. General questions to ask when choosing a forwarder are in How to choose a forwarder; here we focus only on verifying identity.

Public verification routes in Türkiye

Check	What you see	Basis
Mandatory details on documents	A Turkish merchant must show its registry number, trade name, registered office and, where it is required to have one, its registered website on its business letters and documents. These details are also published on the company's website. A missing detail is not proof of fraud on its own, but it is reason enough to ask.	Turkish Commercial Code (TTK) art. 39

Check	What you see	Basis
Tax certificate	You can check the electronic tax certificate (vergi levhası) sent by the other side with the tax number and confirmation code printed on it, using the Revenue Administration's verification service. It also shows if the certificate is out of date or the taxpayer has ceased business.	General Communiqué on the Tax Procedure Law No. 408
Trade Registry Gazette	Using the trade name, MERSİS number or registry number, you can find announcements of incorporation, change of address, change of authorised signatories and capital. Searches can be made in the official Turkish Trade Registry Gazette system, on TOBB's gazette and trade name search page, or through e-Devlet.	Trade Registry Gazette
MERSİS number	The 16-digit number given to every business in the Ministry of Trade's Central Registry System (MERSİS). Check that the number on the documents and the registry entry point to the same company.	MERSİS
TİO authorisation certificate	Anyone acting as a freight forwarder (taşıma işleri organizatörü) in Türkiye must hold a TİO authorisation certificate. Ask for a copy; the name and tax number on it must match the other records, and it must be within its validity period.	Regulation on Freight Forwarding (Taşıma İşleri Organizatörlüğü Yönetmeliği) art. 5
International membership	FIATA publishes a Members Directory on its website. Membership is not an operating licence; it only shows which professional rules the firm is bound by.	FIATA

These checks answer "does the company exist?", not "is the person I am dealing with really that company?". Fraudsters can use the name of a real, registered company. In our view the last step should therefore always be to call the company on the contact details in the registry or on its official website and confirm the quote and the bank account.

Fake tracking pages

A "track your shipment" link arriving by email or message can lead to a page set up to collect login or payment details. In our view the safe course is not to click the link but to go to the carrier's official website by typing the address yourself. You can look up a suspicious domain in the public list of malicious links kept by Türkiye's National Cyber Incident Response Center (USOM) and report it to USOM if it is not listed.

Forged bills of lading, document fraud and misdeclaration

Because a bill of lading represents the goods, it is one of the most valuable targets for forgery. A 2015 alert from a P&I club reported an increase in fraudulent and unauthorised bills and described two cases:

- An unauthorised agent issuing a "clean" bill "for and on behalf of the master", without the master's knowledge, with every other detail identical to the genuine one;
- A bank receiving a set of bills completely different from the set the owner had authorised.

The alert also flags the risk where an intermediate seller in a chain has not paid for the cargo and therefore does not hold the original bill.

The same alert notes that FIATA has also warned its members about bill of lading "cloning". The club's recommendations: insist on presentation of an original bill at discharge, do not commit in the charterparty to accepting LOIs, carry out enhanced due diligence on new or unfamiliar charterers, and contact the P&I club at once if anything looks irregular.

For cargo interests, the most practical check in our view is this: verify the bill number, vessel, voyage and dates through the carrier's official channel, finding the contact details yourself on the carrier's official website rather than taking them from the document or the email.

Fraud does not always mean a forged piece of paper; a genuine document can also contain false information. Knowingly backdating a bill, issuing a clean bill for damaged cargo against an LOI, and changing the port of loading on a switch bill to hide origin all fall into this category. See The bill of lading in practice for details. With an electronic bill of lading, control of the document is tied to a platform record; in our view this reduces the risk of copies and of two sets circulating at once. For the framework, see Digital logistics and the electronic bill of lading (eBL).

Misdeclaration

Misstating the type, quantity or weight of the goods is done sometimes to reduce freight or duty, sometimes to hide a dangerous cargo. Under TTK art. 1145 the charterer and the shipper must give complete and accurate information about the goods and are liable to the carrier for loss caused by inaccurate statements. The Hague-Visby Rules also deem the shipper to have guaranteed the accuracy of the marks, number, quantity and weight it declares (art. III(5)). For the consequences of misdeclaring dangerous goods, see Consequences of undeclared or misdeclared cargo.

Fake buyers and fake suppliers: checks before payment and shipment

In our experience a fake buyer typically places a large first order, does not argue about the price, but resists any payment security. They ask for open account terms or for documents to be sent before payment, and push for the cargo to be released by telex release or sea waybill, that is, without waiting for the original bill of lading. With a fake supplier it is the other way round: advance payment only, a new domain imitating a real manufacturer's website, and a bank account in a name different from the one on the invoice.

Step	Company in Türkiye	Company abroad
Registration	Trade Registry Gazette and MERSİS record	The official company register of the country where it is registered; in many countries it can be searched online
Tax	Verification of the e-tax certificate with its confirmation code	The country's tax number verification service, where one exists
Contact	Call using the address and phone number in the registry, independently of the details in the email	Same principle: find contact details in the official register or on the official website
Bank	Is the account holder the same as the name on the invoice?	Is the account in the country where the company is registered, and in its name?

Step	Company in Türkiye	Company abroad
Payment security	Until trust is established, use a security such as a letter of credit or documents against payment instead of open account. The methods are ranked in The risk ladder.	
Release method	Do not choose a method that releases the cargo without the original bill before payment is secured. Use the decision table on the bill of lading page.	

For assessing supplier risk more broadly, avoiding dependence on a single source and scoring suppliers, see Supplier risk and multiple sourcing.

Cargo theft, impersonation and fake load postings

An FBI alert dated 30 April 2026 describes cyber-enabled cargo theft targeting brokerage processes in road freight in the US and Canada. The loss figures are given in the security section of the social media page. Here we look at how it works, because the same methods travel easily to other markets:

- **Account takeover:** clicking links that look like carrier agreements or negative-review notices installs remote management software, giving the attacker undetected access to the broker's or carrier's systems.
- **Fake load postings:** using compromised carrier accounts, tens of thousands of fake loads are posted on load boards. Carriers who bid are sent malicious agreement files.
- **Double brokering:** a real load is accepted under the compromised carrier's authority and passed on to drivers who are not fully aware of the situation. The bill of lading and the destination are altered, and the cargo is transloaded and resold.
- **Carrier identity theft:** the carrier's contact and insurance details in official records are changed. Carriers often find out only when brokers ask about loads they never accepted.

The FBI recommends verifying the request and the collecting vehicle through an independent second channel before releasing a load; not trusting a familiar name or email address on its own; recording the driver's licence, photos of the vehicle and plate, and contact details; and treating unexpected load enquiries and suspicious download links as warning signs.

In our view the same principle applies in ocean freight. The information needed to collect a container (delivery order, release number or PIN), a delivery address changed by a last-minute email, or a new haulier all call for a voice confirmation before the cargo is released. Instructing the warehouse and the terminal that "changes to delivery details are not applied until confirmed on a known number" reduces this risk.

What to do when it happens: the first hours

In payment diversion, the most critical variable is time. IC3 advises contacting your bank as soon as you discover a fraudulent transfer and asking for the funds to be recalled. US data show that in 2025 IC3's rapid-response process with banks froze USD 679 million, about 58%, of roughly USD 1.16 billion in transfers across 3,900 reported incidents. That is a US process, but it shows why acting early matters.

1. **Call your bank immediately.** Ask for the transfer to be recalled and for the receiving bank to be notified. Do not lose hours; prepare the written documents your bank asks for.

2. **Preserve the evidence.** Do not delete the emails. Keep the full header information, invoices, payment receipts and screenshots of the correspondence. In Türkiye, online content can also be recorded by an e-notary.
3. **File a criminal complaint.** In Türkiye a complaint can be filed with the public prosecutor's office in writing or in person, and also with the cybercrime units of the police and the gendarmerie. A complaint filed with the prosecutor where you are is forwarded to the competent office. State the date and details of the incident and the evidence.
4. **Report the malicious domain.** Report the fake site or link to USOM using its reporting form.
5. **Secure your accounts.** Change passwords, turn on multi-factor authentication, and check mailbox forwarding and deletion rules and open sessions. In our view, do this with your IT team or service provider.
6. **Inform those involved through known channels.** Tell the other party, the company whose name was used, the carrier and forwarder if the cargo is still in transit (so that it is not released), and your insurer. If an organisation's name was imitated, the organisation itself will want to hear, as FIATA asks, with the full header of the fake email.
7. **If the payment went to an account in the US,** IC3 recommends filing a complaint at www.ic3.gov with the transaction details, whatever the amount lost.

Internal controls: a short checklist

The list below combines recommendations from the sources with our own experience; every company should adapt it to its size.

Control	What it prevents	Whose job?
Written procedure for changes of bank details: two-person approval and voice confirmation on a known number	Payment diversion	Finance
Onboarding checks for new suppliers, customers and forwarders: tax certificate, Trade Registry Gazette, TİO certificate where relevant, independent phone confirmation	Fake companies	Purchasing, sales, operations
Email security: multi-factor authentication, limited admin rights, regular review of mailbox rules	Account takeover	IT
Verification of bills of lading and documents through the carrier's official channel	Forged documents	Operations, trade
Cargo release procedure: record driver, vehicle and plate details; voice confirmation for last-minute changes	Cargo theft	Operations, warehouse
Short training: a simple rule such as FIATA's "Stop, Assess, Flag, Escalate" (S.A.F.E.)	All of the above	HR, managers
Incident plan: who calls whom, and in what order (bank, legal, IT, insurer), written down in advance	Lost time	Management

Where to go next in the guide

- Fake social media accounts and digital footprint: Social media in logistics: security
- What to ask when choosing a forwarder: What is a freight forwarder?
- Rules on dates, clausing and switch bills: The bill of lading in practice
- Payment security and letters of credit: Payment methods and letters of credit
- Delivery without the original bill and LOIs: Delivery without the original bill of lading: LOIs and bank guarantees
- Supplier risk: Purchasing and supplier selection
- Electronic documents: Digital logistics and the electronic bill of lading (eBL)

Which courses cover this topic?

Our course map has no separate heading for fraud in trade and logistics. The closest cards are safety and security (ISPS, supply chain security) and international trade operations; we cannot say that every one of these courses deals with fraud specifically. A few examples:

- Irish International Freight Association (FIATA-accredited) — FIATA Diploma in Freight Forwarding (certificate) — Safety & Security
- University of Piraeus — M.Sc. in Shipping (master's) — Safety and Security in Shipping Operations
- KTO Karatay University — International Trade and Logistics (bachelor's) — Supply Chain Management in International Trade (01140003), as part of the course
- Anadolu University, Open Education Faculty — Foreign Trade (associate degree) — Import and Export Operations (TİC208U)
- ICC Academy — ICC Global Trade Certificate (certificate) — Introduction to Cross Border Trade

Test yourself

1. A supplier you have worked with for years emails from their usual address: "our bank account has changed because of the year-end audit". Since it came from the real address, can you pay? *(Answer: No. The mailbox may be compromised. Do not apply the change without a voice confirmation on the known number in your records.)*
2. A forwarder has a Trade Registry Gazette record and a valid tax certificate. Does that prove the quote really came from that firm? *(Answer: No. These records show the firm exists; a fraudster may be using a real firm's name. Call the firm on the contact details in the registry to confirm.)*
3. On a first order, the buyer says they will pay "when the goods arrive" and wants the cargo released immediately by telex release. What is the risk? *(Answer: You lose your security over cargo released without the original bill. Until trust is established, use a security such as a letter of credit or documents against payment, and an original bill.)*

4. You realise you have paid to a fraudulent account. What is the first thing to do? *(Answer: Call your bank immediately and ask for the transfer to be recalled. Preserving evidence and filing a criminal complaint come next.)*

Frequently asked questions

What is BEC (business email compromise)?

It is the diversion of a payment to a fraudster's account by compromising or imitating a real company's email. The FBI's Internet Crime Complaint Center (IC3) describes it as a scam targeting businesses that work with suppliers and regularly make wire transfers.

How can I check that a company really exists in Türkiye?

Look up its records in the Trade Registry Gazette by trade name, MERSİS number or registry number, and check its e-tax certificate with the confirmation code on the Revenue Administration's verification service. Ask a freight forwarder for a copy of its TİO authorisation certificate. Then call the company on the contact details in the registry to confirm the quote came from them.

Does FIATA membership show that a firm is trustworthy?

Not on its own. The FIATA Members Directory shows that a firm belongs to a professional body, but membership is not an operating licence. In Türkiye the legal requirement for freight forwarding is the TİO authorisation certificate.

I sent money to a fraudulent account. Can I get it back?

There is no guarantee, but the best chance is in the first hours. Call your bank at once and ask for the transfer to be recalled. In the US, IC3's process with banks froze about 58% of the reported transfers in 2025. Then preserve the evidence and file a complaint with the public prosecutor.

Where do I report a fake tracking site or email?

Malicious domains can be reported to Türkiye's National Cyber Incident Response Center (USOM) using its reporting form. Also tell the company or organisation whose name was imitated, with the full header of the email. If you have suffered a financial loss, a criminal complaint to the prosecutor is needed as well.

SOURCES

FBI IC3 — 2025 IC3 Annual Report (BEC complaints and losses; recall advice and FFKC results) — https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
Adams and Reese — summary of the FBI 2025 report (cross-check of BEC figures) — https://www.adamsandreese.com/the-ledger/fbi-releases-2025-internet-crime-report-key-takeaways-for-the-payments-industry
FBI IC3 — Cyber-Enabled Strategic Cargo Theft Surging (PSA, 30 April 2026) — https://www.ic3.gov/PSA/2026/PSA260430
FIATA — Scam alert: beware of fraudulent emails (25 July 2025; S.A.F.E., Members Directory) — https://fiata.org/n/scam-alert-beware-of-fraudulent-emails/
Standard Club — Fraudulent bills of lading (27 January 2015) — https://standard-club.com/knowledge-news/web-alert-fraudulent-bills-of-lading-264
Ministry of Trade (Türkiye), Aydın Provincial Directorate — 6102 sayılı Türk Ticaret Kanunu, full text (arts. 39, 1145)(in Turkish) — https://aydin.ticaret.gov.tr/data/5d91fe5b13b876a92027f370/6102%20Say%C4%B1l%C4%B1%20T%C3%BCrk%20Ticaret%20Kanunu.pdf
legislation.gov.uk — Carriage of Goods by Sea Act 1971, Schedule: Hague-Visby Rules art. III — https://www.legislation.gov.uk/ukpga/1971/19/schedule/crossheading/3/enacted/data.pdf
Revenue Administration (Türkiye) — 408 sıra no.lu Vergi Usul Kanunu Genel Tebliği (tax certificate, confirmation code and verification)(in Turkish) — https://www.gib.gov.tr/node/88655/pdf
Alomaliye — Vergi levhası sorgulama (e-Devlet and Digital Tax Office; verification by confirmation code)(in Turkish) — https://www.alomaliye.com/2022/08/08/vergi-levhasi-sorgulama/?noamp=mobile
FFK Partner Hukuk — Ticaret Sicili Gazetesi nasıl sorgulanır? (2026)(in Turkish) — https://www.ffkpartnerhukuk.com.tr/ticaret-sicili-gazetesi-nasil-sorgulanir-2026-guncel-rehber-sirket-bilgileri-ilanlar-ve-ticaret-sicili-gazetesi-sorgulama/
Halkbank — MERSİS no nedir, nasıl sorgulanır? (in Turkish) — https://www.halkbank.com.tr/tr/blog/mersis-no-nedir
Ministry of Transport and Infrastructure (Türkiye) — Taşıma İşleri Organizatörlüğü Yönetmeliği (Official Gazette 27.08.2022, art. 5)(in Turkish) — https://uhdgm.uab.gov.tr/uploads/undefined/tio-yonetmelik.pdf
Kadim Hukuk — Bilişim suçları nereye şikâyet edilir? (2026; prosecutor, police, e-notary)(in Turkish) — https://kadimhukuk.com.tr/makale/bilisim-suclari-nereye-sikayet-edilir/
Webtekno — Bir sitenin dolandırıcı olup olmadığını anlama (USOM malicious links list and reporting form, 28 June 2025)(in Turkish) — https://www.webtekno.com/bir-sitenin-dolandirici-olup-olmadigini-anlama-h159404.html

This guide is for educational purposes and reflects the author's personal views, not those of any current or former employer. For contract, customs and finance decisions, consult current official sources and specialists. Incoterms® is a registered trademark of the International Chamber of Commerce (ICC).

© 2026 Özgür Konakcı · ozgurkonakci.com. This document may be shared and reproduced for educational purposes with credit to the source (ozgurkonakci.com); it may not be used for commercial purposes.