EUROPEAN DISTRIBUTION FRAUD (EDF): PREVENTION CHECKLIST

What is EDF and how can this document help prevent it.

European Distribution Fraud (EDF) is where an individual or group, imitates the details of a legitimate company, to pass credit checks and purchase goods. Once they have received the goods, they become uncontactable leaving the supplier to face a financial loss. EDF can be committed in many ways depending on the individuals, while some attempts are more blatant others are more strategically planned.

This document is designed to help protect businesses from becoming a victim of EDF by sharing best practice. Shared below are checks you may wish to add into your current procedures, to protect your business and enable you to recognise the signs of EDF attempts.

POTENTIAL SIGNS OF EDF

- A new address has been given from an existing customer for an order to be delivered to. It is important to double check the address change is legitimate before accepting.
- Poor grammar and spelling across all business documentation such as emails, invoices and the business website.
- The business does not match the product they are ordering. For example, a business places an order for meat but are listed as an alcohol supplier.
- Unexpected orders placed by well-established/known businesses without prior contact, business connection or audit. Offenders can utilise the perceived trust people have in established brands.
- Orders from completely new customers requiring a quick turnaround. Offenders may refer to ‘supply chain issues’ as a reason for a tight deadline, in order to remove any suspicion aroused by sudden contact being made. This can often be accompanied by a promise of future substantial orders.

Lack of due diligence by the customer when requesting a product. Offenders will focus on the commodity they require, as well as the volume, and may not ask for relevant technical details those working in the industry would seek to know; Food Chain Information, provenance etc.

HOW TO PROTECT YOUR BUSINESS AGAINST EDF

When engaging with new customers be sure to follow key points on this check list to minimise the risk of becoming a victim to EDF.

- Check when a website was created compared to the business. Are you engaging with a well-known business who has only created a site within the past year?
- Conduct in person audits. COVID-19 has meant a move to virtual audits, do not be afraid to move back to in person audits now restrictions have lifted.
- Check there is a lock on the business's website? If not this this shows the site is unsecure, and though not a direct sign of fraudulent activity the vast majority of legitimate businesses operate from a secure site. An unsecure site should alert you to be extra vigilant during due diligence checks.
- If a different staff member of an existing customer places a new order be sure to check any staff changes within the business. You can do this by asking to speak to the previous contact to confirm the change, ask to speak to a manager or someone else in the business or challenge the person making the order; their answers may show you they know nothing about the business.
- Understand the specifics of how your existing customers place orders with you, so that you are alerted to any changes in how those orders are placed. A change in how the order is made may indicate it is not a legitimate business behind the order, as offenders may seek to imitate those you have existing relationships with.
- Use internet searches to ensure the address given by the business is not only valid and matches the address given but is also an address fitting of the business; e.g., industrial estate or residential street.
- Ensure your bank verifies the details given by the business, cross checking the name and the account number match
- Check the business on Companies House to ensure they match the information you have been given.
- Check the business and employee(s) on social media platforms. Its important to check that the information shown on the employee(s) social media matches the information given on the business platform. Does the employee have the business as a current place of work? Does the business platform list the employee(s) job title/role? Do not be afraid to message them on these platforms to double check.
- Implement a mandatory policy whereby if a driver receives a change of address while in transit, they stop immediately to check with head office.
- Request a deposit be paid in advance if you are unsure about the buyers' intentions.
- Double check all new customer details such as email and contact numbers provided. Good practice to implement is to find out who the business personnel is via internet search and if you can find contact details for them in order to verify.

While this list is not exhaustive it is designed to help food businesses protect themselves against EDF. It is important to remember to report all incidents to **Action Fraud** and to speak to your local Police Force. Please contact us if you wish to receive further engagement on EDF and what you can do to reduce the risk to your business.

Freight Auction Sites

The NFCU have become aware of offenders impersonating courier companies and biding for work through Freight Auction websites. This Modus Operandi (MO) has similarities with EDF, and we strongly encourage businesses to carry out stringent due diligence, as laid out above, when dealing with new customers in this area as well. Furthermore, be sure to check with any courier companies you have contracts with that they are not sub-contracting via these platforms.

Contact information

Action Fraud number – 0300 123 2040

NFCU Prevention Team - NFCU.Prevention@food.gov.uk

Food crime confidential number - 020 7276 8787

Online confidential reporting tool - Report a food crime