Cellule de Renseignement Financier

Trend alert #2

Business Email Compromise (BEC) targeting the investment sector

Business Email Compromise (BEC) targeting the investment sector

Context

Over recent months, FIU Luxembourg observed an increasing number of Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs) related to cyber-enabled fraud schemes targeting professionals of the investment sector. These scams aim to divert funds to accounts controlled by criminals and are becoming increasingly sophisticated and hence difficult to detect.

Fraudsters often possess detailed information about the targeted companies and the entities they impersonate. A wide range of scams using fake capital call or drawdown notices, falsified invoices or fraudulent loan repayment instructions has been detected. These documents often contain accurate and credible information about the targeted investments. Fraudsters also appear to have detailed knowledge of the layout, structure, and formatting of genuine documents issued by the impersonated entities.

Such scams typically involve high-value transactions and are generally perpetrated through Business Email Compromise (BEC) and impersonation techniques to issue fraudulent payment instructions. They target various professionals active in the investment fund industry, such as fund managers, fund administrators, investors and professionals providing Trust and Company Services.

The high degree of sophistication of these attacks highlights the need for rigorous verification procedures, including Confirming your client's designated contact person, along with the authorized individuals for payment validation and signature.

Should you encounter the described typology, please include the following hashtag #TA-2025-002 in your report, in the "reason for suspicion"-section.

Business Email Compromise (BEC) targeting the investment sector

Key characteristics*:

70%

of cases involved spoofed (lookalike) email addresses used to alter payment instructions.

60%

suspicions involve **fraudulent capital call notices**

45%

of cases were **identified before** any fraudulent transfers occurred

1,5 mio. €

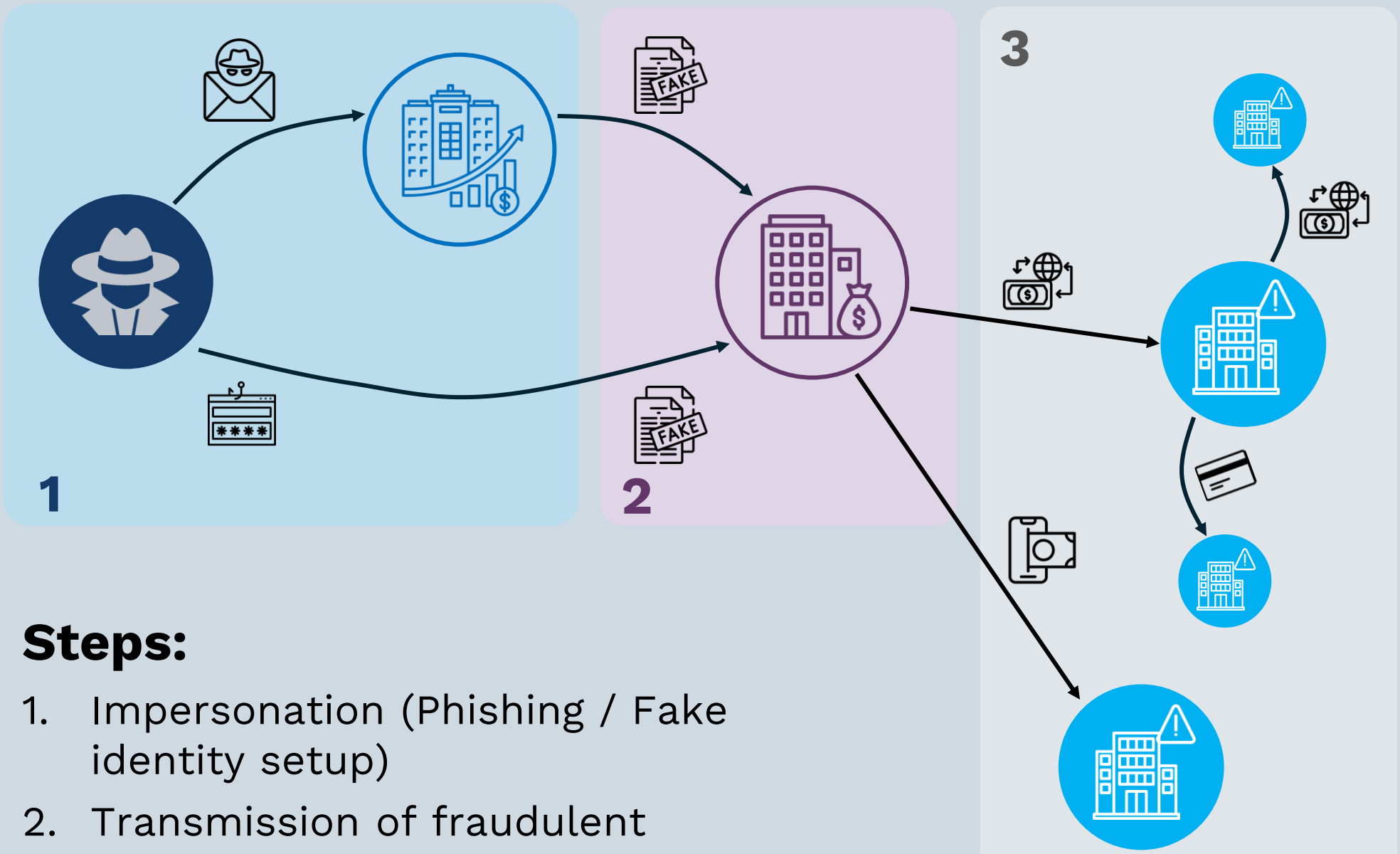
is the **average amount** per suspicious activity or transaction report (SAR/STR) involved in these fraud cases

** Disclaimer: The analysis is based solely on the reports selected for this specific purpose and reflects the information available at the time of review. – Period under review (January – November 2025)*

Cellule de Renseignement Financier

Business Email Compromise (BEC) targeting the investment sector

Illustrative diagram



Steps:

1. Impersonation (Phishing / Fake identity setup)
2. Transmission of fraudulent payment instructions
3. Fund diversion & layering

Cellule de Renseignement Financier

Business Email Compromise (BEC) targeting the investment sector

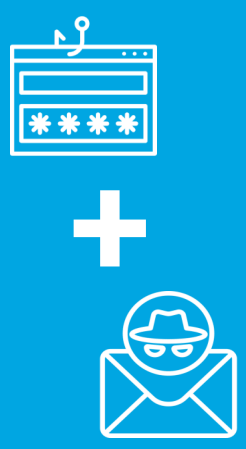
Step 1: Impersonation techniques

Use of spoofed or lookalike email addresses

- Fraudsters register and configure a domain similar to the real one, by adding, changing, or deleting one or more characters in the legitimate domain name (lookalike domain).
- Fraudsters use fraudulent or lookalike email accounts but falsify sender identity (e.g., email header) to appear as a trusted source.

Use of compromised email addresses

- Fraudsters aim to compromise email accounts of professionals of the investment sector and use these trusted identities to send fraudulent payment requests, bypassing checks to validate payment requests.
- Access to email accounts is obtained via social engineering or phishing.
- Once access is gained, attackers observe ongoing communications, collect sensitive information, and craft sophisticated messages.



Combined use of compromised and lookalike addresses

- In some cases, attackers combined compromised email accounts with lookalike domains.
- The compromised account was used initially to establish trust and legitimacy.
- Once confidence was built, fraudulent emails from lookalike domains took over to execute the scam.

Cellule de Renseignement Financier

Business Email Compromise (BEC) targeting the investment sector

Step 2: Vectors for fraudulent payment instructions

Fake **capital call notices** requesting transfer of committed funds sent to investors

Fake **invoices for service provision** sent to investment fund managers

Fake **drawdown notices** sent to investment fund administrators

Fake **loan repayment instructions** sent to investees

Cellule de Renseignement Financier

Business Email Compromise (BEC) targeting the investment sector

Step 3: Fund diversion & layering

Payments are redirected to alternative accounts, either by **changing both the beneficiary and bank** (often located in a different jurisdiction) or by **only replacing the bank account with a PSP or e-money account.**

Funds are rapidly routed through **shell companies** across different jurisdictions. These companies are often registered in office rental spaces or at suspicious locations.

Illicit funds transit through mule accounts, which are used to move money across different jurisdictions. Payment cards linked to these accounts are also employed to layer funds.

Cellule de Renseignement Financier

Business Email Compromise (BEC) targeting the investment sector

Risk indicators

Sender or CC email contains spelling changes, added or missing characters, or uses an alternate domain.	Sudden change in communication pattern (e.g. sudden change in sender email or CC emails, unusual phrasing, or sudden urgency regarding payment)	Payment instructions are modified without clear justification or document contains bank details that differ from those previously verified.
Request for cross-border transfers to jurisdictions unrelated to the investor's / client's profile.	Document layout differs from previous documents received by the same company, is of low resolution, company logo is of poor quality.	Document contains information or amounts that differ from previous documents or from contracts.

Cellule de Renseignement Financier

Cellule de Renseignement Financier

Contact

Cellule de Renseignement Financier (CRF)
Email address: crf@justice.etat.lu
Website: www.crf.lu

Follow us:

Ref. TA-2025-002

November 2025