****

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Data Protection and Cybercrime Division Directorate General of Human Rights and Rule of Law Strasbourg, France  Version March 2018 |

**Advanced Cybercrime and Electronic Evidence Training Course for Judges and Prosecutors**

**2018**

*Introduction to the Investigation Exercise Case Study*

*And the Trainers Guide*



**Contents**

**1. Introduction ..………………………………………………………………………………………………………. 3**

**2. Investigation ………………………………………………………………………………………………….……. 4**

**2.1 Establishing of the initial facts**

**2.2 Establishing reasonable doubt about possible beginning of the crime**

**3. Financial setup .………………………………………………….………………………………………………… 5**

**4.** **Start of actual perpetration and investigation key point ………………………….……………….. 6**

**5.** **Ending of the perpetration and start of the case ………………………….…………………………… 8**

**6.** **Key investigation steps and key electronic evidence …………………..……………………..…… 10**

**7. Appendix .………………………………………………….….…………………………………………………… 11**

**1. Introduction**

This case study scenario belongs to recently well-known, so called “Business E-mail Compromise” schemes, or “BEC” cases, which is deriving from previously detected “CEO fraud” or “Man-in-the-middle” frauds. The scope and size of these frauds is astonishing.

Substantial damage inflicted to victims is constantly growing although government authorities and private sector in a large number of countries globally, have been constantly trying to raise awareness amongst public and private communities. Unfortunately, the latest information about the aggregated financial damage globally, does not support the opinion that progress has been made in this area.

*Trainers notice:* **The scenario begins with establishment of Federal Bank of Atlantis (FBA) as a well-known, long established and reputable international bank. A description like this should lead trainees to conclude that this kind of bank shouldn’t be involved in any kind of problems, let alone ones similar to those which are going to be described later in this document.**

On the other hand, exactly this kind of banks are now regular targets of schemes such this, possibly due to their reluctance to adjust business security procedures to meet new challenges or because of a false sense of security, importance and global presence.

**By the end of the training trainees should be aware that even banks or financial institutions like these can be targets and victims of frauds.** Also, in this case the developing investigation will reveal that BEC is committed with the additional influence of Advanced Persistent Threat (APT) and reverse cyber social-engineering, combine with the use of crypto currencies.

*Trainers notice*: **The idea behind this exercise is to have more of the investigative legal approach which should lead trainees to the step-by-step process of using legal tools at their disposal for conducting almost real-like investigation and building up of a criminal case.** This exercise is a combination of a Budapest Convention articles and domestic legal provisions that will allow them to successfully resolve the case from the investigation phase, through prosecution following the way to the main trial and final adjudication. This will include also some important steps which could and should be taken undertaken in the MLA process in accordance with the Convention.

For this training fictitious countries have been created. They are Atlantis, Norland, Ostland, Westland and others**. For the exercise setup all of them have ratified the Council of Europe Convention on Cybercrime (“Budapest Convention”).** This approach should allow transferability of the training among jurisdictions, without the need for major changes to the course materials over the time.

*Trainers notice:* **At the end of this session, delegates should be able to:**

* **Identify legal and natural persons involved in scenario;**
* **Explain case layout and state of the introductory facts;**
* **Follow and explain flow and development of the case investigation;**
* **Establish how and where criminal investigation should start and which procedural vectors should be followed.**

**2. Investigation**

**2.1 Establishing of the initial facts**

“*The Federal Bank of Atlantis (FBA) is a well-known, successful and trustworthy bank in Europe. It has many branches and businesses in several different countries not only in Europe, but also worldwide. Its banking and business activities are known to be reputable and trustworthy. It seems that due to its policies, the bank is attracting more customers, who are opening bank accounts and using other banking products, than its competitors.*

*The FBA Board of Directors decided to issue a special anniversary bond to mark its 100 years of existence and successful operations. The Board empowered the Department for Logistics and Operations (DLO) to make the necessary preparation for the printing of bonds, including finding a suitable partner to supply all necessary printing elements.*

*The DLO identified a partner, well known in the field for providing printing products and services. The selected partner, United Bank Printing (UBP) is headquartered in the Atlantis, with a European branch based in Norland. The DLO also engaged internally with the Finance Department of the FBA).”*

**The main facts are**:

* Federal Bank of Atlantis (FBA) is a well-known, successful and trustworthy bank;
* FBA wants to issue a special anniversary bond;
* Department for Logistics and Operations (DLO) is in charge of logistical arrangements with this regards;
* United Bank Printing (UBP) is a printing material supplier;
* Inclusion of FBA Finance Department by DLO into business logistics.

*Trainers notice:* **Trainees should identify main facts and key business divisions and decision makers in order to understand the scope and the setup of the business circle in which further case facts are going to be laid-down.**

**Case Study material to be used**:

* *Folder “Day 2/2.2.2 Investigation Exercise Introduction/Pre-read Material”*:
* Case study synopsis;
* Introduction to the Case Study Presentation and Trainers Guide for Case Study Investigation;
* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/ Profiles”*:
* Company profile of Federal Bank of Atlantis;
* Company profile of United Bank Printing;
* Company profile of Docklands Security Bank of Norland.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/Documents and reports”*:
* FBA Announcement of the Anniversary Bond;
* FBA Bond.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/E-mails”*:
* 1st e-mail;
* 2nd e-mail.

**Possible questions for the trainees**:

*- Which authorities and what kind of legal tools will be used on the local level for establishing aforementioned main facts?*

*- How will these facts influence further investigation development?*

**2.2 Establishing reasonable doubt about possible beginning of the crime**

“*Due to the summer vacation period, the DLO was short staffed, and the Deputy Head used junior and recently employed staff to work on this activity, making calls and engaging with colleagues from the Finance Department.”*

*Trainers notice*: **Introduction of the fact that due to the summer vacation period junior and recently employed staff was included in such important operation should promptly raise suspicion amongst trainees.** Key element is that one of the junior staff is actually member of the organized crime group who applied for the lower level position of the DLO in order to gain any kind of direct access to the FBA computers. The aim was to introduce specific e-mail spyware able to send copies of e-mail correspondence between FBA DLO, Financial Department and outsourced businesses to designated computer and user, in this case to the junior staff/main suspect. With this kind of access close insight and detection of possible BEC target is set in motion.

**Case Study material to be used**:

* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/E-mails”*:
* 1st e-mail;
* 2nd e-mail;
* 5th e-mail;
* 7th e-mail.

**Possible questions for the trainees**:

*- What should be undertaken and by which authorities in order to establish identity of the possible perpetrator?*

*- How to establish the type of malware that was used?*

*- How to establish consequences of that malware, traces of the malware communication with outsides contact points and what are other important facts investigation should follow at this stage?*

**3. Financial setup**

*“An order was placed by FBA for the purchase of 20,000 specialized paper materials from UBP for the price of €300,000. The relevant departments in FBA and UBP began logistical and financial arrangements.*

*FBA and UBP exchanged details about invoicing and payment including SWIFT and IBAN accounts and codes. UBP required an advance payment of €100,000 to be paid into their account at Docklands Securities Bank of Norland. This was completed within 24 hours of the order being accepted.”*

Besides the introduction of financial facts, there is couple of additions to the main facts:

*- The inclusion of Docklands Securities Bank of Norland in the business circle as designated bank of UBP for money transfer;*

*- Successful payment of the initial transfer of €100,000 between FBA and UBP with DSBL accounts;*

*- Introduction of the facts that SWIFT and IBAN accounts are included into the transaction.*

*Trainers notice*: **This setup should indicate that initial bank money transfer was done without problems and that mentioning of SWIFT and IBAN codes and accounts means that money transfer is of the international, not domestic nature.** That being said, trainees should start considering use of the international legal assistance articles of the Budapest Convention.

**Case Study material to be used**:

* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/Documents and reports”*:
* FBA-UBP Contract.
* *Folder ““Day 2/ 2.2.3 Investigation Exercise/ Evidence/Bank Statements”*:
* UBP pro-forma invoice;
* FBA Bank Statement;
* UBP Bank Statement.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/E-mails”*:
* 3rd e-mail;
* 4th e-mail;
* 6th e-mail;
* 7th e-mail;
* 8th e-mail

**Possible questions for the trainees**:

* *What are the main substantive articles of the Contract?*
* *How and when advance payment was transferred?*
* *Was the transfer done without problems and why?*
* *Was there a possibility that transfer was monitored by uninvited party?*
* *If so, how?*

**4.** **Start of actual perpetration and investigation key point**

“*The contract required the printing of the 20,000 paper materials to be completed within seven days. UBP fulfilled this obligation one day before the deadline. The Business and Commercial Division informed the UBP Finance Department that the goods are ready to ship upon receipt of the final payment.*

*The UBP Finance Department e-mailed their FBA counterparts informing them that the order is ready for delivery and that the final payment in the sum of €200,000 will be due within 48 hours. That evening FBA received an email from UBP, informing them that the company bank account in the Norland would not be accessible for the following 3 days, due to a national holiday in the country. The email requested that the balance should be paid to UBP account in Docklands Securities Bank of Norland branch in Ostland.*”

*Trainers notice*: **This should be recognized as a triggering moment for the perpetration of the whole scheme.** Previously mentioned member of the organized criminal group by use of the spyware was able to detect and follow development of the business exchange between FBA and UBP. The only action left was to identify and react promptly at the time of the final payment, which should occur as soon as UBP informs FBA that the printing of requested paper material has been completed.

Once UBP Finance Department notified their FBA counterparts that the payment was due the “mole” was able to intercept that e-mail and notify the rest of the criminal group. Together with co-perpetrators, he was ready to send previously prepared false invoices with e-mail headings almost the same as the UBP Financial Department ones by the use of the open SMTP server services which were leased prior to the introduction of the perpetration of the crime.

**Variant of the scenario** including facts that e-mail has been changed by with some small changes in the actual name of the e-mail account of the UBP financial employee instead of using of free SMTP server, should be used in situations when trainers observe lesser technical knowledge of the trainees which could lead to the problems in the successful ending of the investigation exercise.

A bank account under criminal control was opened purposely with criminal intent in the other country (Ostland in this exercise), in behalf of a “dummy” company with similar name to the original one (UBP in this case), which was previously registered with the branch of the main bank, meaning that fraudulent banking account was opened with Docklands Securities Bank of Norland branch in Ostland. The bank account was not used before with FBA and was created with data known to the principal and support perpetrators. Data which was used during registering process was forged and almost identical to the original one with details from FBA financial employees.

A sense of urgency was added to the whole scheme due to the upcoming national holiday in Norland. This was used by the criminals as an additional justification for the bank account change. From this point on, stage was set.

**Main facts:**

* *Actual printing of paper material was done and UBP notified about that fact FBA requesting due payment;*
* *Infiltrated member of organized crime group by use of spyware detected final moments of the business closure;*
* *Group registered “dummy” company in Ostland and opened company bank account in that country with branch of the bank used in regular operations of UBP in Norland;*
* *False documentation, including main pieces of it – false invoice, e-mail server and e-mails, was prepared;*
* *Open SMTP server was leased and tested for sending false e-mail (or example of a webmail account with slight change in the name of the e-mail account can be used, depending on the trainer skills);*
* *Open SMTP mail server services were paid by Bitcoins (or in a webmail case example, without it);*
* *False e-mail was prepared, including names of the actual financial people, details about contract and language which was previously used;*

**Case Study material to be used**:

* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/E-mails”*:
* 9th e-mail;
* 10th e-mail.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/Evidence/Bank Statements”*:
* UBP false invoice
* *Folder “Day 2/ 2.2.3 Investigation Exercise/Evidence/Documents and reports”*:
* UBP dummy company registration in Ostland;
* DSBN UBPO dummy company bank account registration in Ostland;
* Anti-spyware software scan results report;
* SMTP server network tracing report;
* SMTP Server Company Bitcoin payment report.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/Evidence/ Witness Statements”*:
* FBA IT Statement.

**Possible questions for the trainees**:

* *How the information about finalization of the business was acquired and how to retrieve it, if possible?*
* *How to get information about “dummy” company and bank account details from Ostland?*
* *What kind of information should be requested from Ostland and in what way?*
* *Is some of the information urgently needed and will it be justified for that reason to activate 24/7 Contact Point of CoE Network?*
* *How to obtain evidence about false/forged documentation and how to analyze it?*
* *How to get information about open SMTP server (or information from web based E-mail Company) and what can be revealed from that?*
* *What is Bitcoin, how it was used and in which way it can be used as electronic evidence?*
* *What’s the summary of the electronic evidence which can be acquired?*

**5.** **Ending of the perpetration and start of the case**

“*On the following working day FBA Finance Department was ready to transfer the money. Chief Financial Officer authorized the transfer of the remaining €200,000, which was transferred to the communicated bank account of the UBP in Ostland.*

*On the morning of expiration of the 48 hours deadline, UBP Finance Department contacted their FBA counterparts requesting immediate payment of the outstanding balance. FBA informed UBP that the payment had already been made and that they were expecting delivery of the goods. As an aside, FBA offered their congratulations to UBP on the National Holiday.*

*The UBP Finance Department checked their bank account and responded to FBA that no payment had been received from them. They also asked why UBP is congratulating them on a public holiday, when the next one is not due for another two months*.”

*Trainers notice*: **Finale of the scheme is unfolding on the following day when Chief Financial Officer of FBA authorized bank transfer on the basis of previously presented documents: false UBP mail with false invoice containing false bank account in the country not known both to the FBA and UBP.**

In that very moment fraud was completed. 200.000 EUR has been transferred to the fraudulent account. Depending on the case scenario development, trainers can develop further transactions between Ostland bank account and bank accounts in other countries belonging to Budapest Convention statutory parties or not, as an exercise both on following online money trails and transactions through effective financial investigation and testing knowledge for mutual legal assistance procedure.

Depending on the trainers choice, ending of the banking transfers can be in the country which is reachable by Budapest Convention or not. In the second case most probably final traces and evidence are going to be lost or not retrievable forever. However, both examples can be useful to the trainees.

**Main facts:**

* *Chief Financial Officer of FBA authorizes transfer on the basis of previously presented documents;*
* *Document are false UBP mail with false invoice containing false bank account;*
* *200.000 EUR has been transferred. Depending on local training needs, bank transfers can be continued to other countries or stopped. Also, end transfer can be pointed to Budapest Convention country or other;*

**Case Study material to be used**:

* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/E-mails”*:
* 9th e-mail;
* 10th e-mail;
* 11th e-mail.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/Witness Statements”*:
* FBA DLO Statement;
* FBA FD Statement;
* FBA IT Statement;
* DSBN Ostland AD Statement.
* *Folder “Day 2/ 2.2.3 Investigation Exercise/ Evidence/Bank Statements”*:
* DSBN Ostland Bank Statement;

**Possible questions for the trainees**:

* *Why Chief Financial Officer did authorized transaction?*
* *To which account transaction was transferred?*
* *Since Ostland ratified Budapest Convention, what steps are going to be undertaken by LEA?*
* *Which documents and in what form should be obtained from FBA?*
* *Which documents and in what form should be obtained from UBP?*
* *Which bank should be contacted and in what way with what kind of request during the investigation?*
* *How money can be retrieved, if possible?*
* *What kind of applications and/or orders can be issued to all business entities and banks?*
* *What are the grounds for this kind of actions?*
* *Which articles of the Budapest Convention will be used?*

**6.** **Key investigation steps and key electronic evidence**

The trainees will presume that first moment of contact between FBA and LEA was on the day of the transfer when UBP e-mail arrived with question about the lack of money transfer and holiday. From that moment on, depending on the local legal framework, investigation starts. Model is versatile and can include both police, prosecutors, investigative judges and other entities, if needed. All institutions can have a role and their actions have common goal with different approaches.

However, **key investigation steps should be**:

* *Taking depositions from the possible suspects;*
* *Taking depositions from the representatives of the FBA;*
* *Obtaining electronic and other evidence from FBA;*
* *Taking depositions from the representatives of the UBP;*
* *Obtaining electronic and other evidence from UBP;*
* *Taking depositions from representatives of DSBN in Norland and Ostland;*
* *Obtaining electronic and other evidence from both banks;*
* *Obtaining evidence from competent Company Registration Authority in Ostland;*
* *Cooperation between police, prosecution and, if relevant, investigative judges;*
* *Inclusion of international legal assistance within Budapest Convention provisions;*
* *Other important investigative actions recognized and defined by the trainees with support by trainers.*

**Key electronic evidence:**

* *FBA computer records;*
* *Spyware used in FBA;*
* *SMTP server and record for sending false e-mails;*
* *Crypto-currency (Bitcoin), blockchain, blockchain ledger;*
* *Regular e-mails;*
* *False e-mail with full header;*
* *False invoice;*
* *UBP computer records;*
* *DSBN banking and account records;*
* *Company registry records;*
* *Surveillance records;*
* *Other electronic evidence*.

Both lists are not exhausted with this count and can be amended or updated with other investigation steps and electronic evidence as needed.

**Additional** **Case Study material to be used**:

* *Folder “Day 2/ 2.2.3 Investigation Exercise/Glossary”*:
* Advanced Persistent Threat;
* Cryptocurrencies;
* Cyber Social Engineering;
* Spyware;
* Open SMTP server and E-mail spoofing.

**7. Appendix**