**Lesson Plan**

Lesson 1.4.2 Online Criminal Money Flow Typologies

|  |  |  |
| --- | --- | --- |
| Lesson 1.4.2 Online Criminal Money Flow Typologies | | Duration:  180 Minutes |
| **Resources Required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Session Aim:**  The aim of this lesson is to illustrate some of the most frequently used methods and instruments for (a) holding proceeds of online crime and (b) laundering proceeds from online crime and to allow the participants to consider the presence (or absence) of the components of the crime of money laundering from their national legislation in the online typologies. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the criminal money flow typology of the use of money remittance providers. * Explain the criminal money flow typology of the use of wire transfers, takeover/opening of accounts. * Explain the criminal money flow typology of the use of cash withdrawals. * Explain the criminal money flow typology of the use of Internet payment services. * Explain the criminal money flow typology of the use of money mules. * Explain the criminal money flow typology of the use of international transfers. * Explain the criminal money flow typology of the use of virtual currencies. * Explain the criminal money flow typology of the use of purchasing through the Internet. * Explain the criminal money flow typology of the use of shell companies. * Explain the criminal money flow typology of the use of prepaid cards. * Explain the criminal money flow typology of the use of online gaming and online trading platforms. * In the case of each typology listed above, list possible sources of evidence. * In the case of each typology listed above, list procedural powers in national legislation applicable to the identification of the use of the typology. * In the case of each typology listed above, and if applicable, list the procedural powers applicable to the freezing, seizing and confiscation of funds held in an online form. * In the case of each typology listed above, consider whether the components of the crime of money laundering as defined in their national legislation are present. | | |
| **Trainer Guidance**  This session provides information about a selection of online criminal money flow technologies.  All information about this session is included in the PowerPoint presentations entitled “1.4.2 – Online Criminal Money Flow Typologies (hour 1)”, “1.4.2 – Online Criminal Money Flow Typologies (hour 2)” and “1.4.2 – Online Criminal Money Flow Typologies (hour 3)” in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made; however the objectives should be achieved.  The typologies lessons as envisioned in the PowerPoint presentations involve a significant amount of interactive discussion between the trainer and the students. In situations where there are students from different countries and/or speaking different languages, this approach may be impractical.  Therefore, an alternative approach that can be used that might work is to present all of the typologies that are included in the presentations during the first hour and then break the delegates up into groups. Each group is to be provided with one (or more) of the typologies and asked to spend the second hour preparing a five minute presentation on their national experience with their assigned typology, focussing in particular on (a) the possible source of evidence, (b) procedural powers available, (c) confiscation of funds held in an online form (if applicable) and (d) what, if any, elements of the crime of money laundering are present in the typology.  Trainers should be particularly aware of point (d) because in previous deliveries of this material it has been noted that delegates considered the typologies in the context of commission of a criminal offence. In other words they interpreted the typologies more like *modi operandi* of predicate offences. Therefore, the trainer should take particular attention to draw the student’s attention to the elements of the crime of money laundering. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| **HOUR 1** |  | |
| Slide 4 | The trainer should ask the students what is a money remittance provider and to give examples of any specific money remittance providers they might be aware of. Examples that will typically arise are Western Union and MoneyGram.  Through guided discussion the trainer should identify the following categories of remittance providers:   * Large “traditional” providers, such as Western Union and MoneyGram * Informal value transfer networks and underground banking systems, such as Hawala networks   The trainer should ask the attendees how money remittance providers work, in general terms, focusing on the following key points:   1. Person A presents at a location of the remittance provider 2. They provide funds to the remittance provider 3. Person B presents at a location of the remittance provider (possible in a foreign jurisdiction) 4. Person B receives funds from the remittance provider 5. A fee is charged by the remittance provider for this service   The trainer should explain that most, but not all, money remittance providers have an online presence.  The trainer should highlight the point that there are both formal and informal money remittance providers. Formal examples are western union and MoneyGram. Informal remittance providers are common, often used within particular ethnic groups, whereby one individual will accept funds and transfer them to a family member in their home country. The family member in the home country will they pay out funds to the recipient in the home country. | |
| Slide 5 | The trainer should ask the students what they consider to be the problems with money remittance providers from the perspective of investigation, search, seizure and confiscation of crime proceeds.  Through guided discussion the trainer should help the class to identify the following key issues:   1. If the remittance provider accepts or pays out in cash there is a possibility that an investigation could be impeded. 2. If the remittance provider does not adequately identify and retain identification of the customer, an investigation could be impeded. 3. If the remittance provider does not retain adequate transaction records, an investigation could be impeded. 4. If the remittance provider is not required by regulation to report suspicious activity, an investigation could be impeded. 5. If the remittance provider does not register their activities with the regulator, an investigation could be impeded.   The volume of legitimate cash transactions presents a challenge for identification of illegal cash transfers. | |
| Slide 6 | Trainer should describe the typical remittance provider laundering typology, as per this slide.  Trainer should not focus too heavily on the mule recruitment aspect of the typology, because this will be covered separately elsewhere. | |
| Slide 7 | Trainer should ask participants to discuss how they might approach an investigation where the money remittance provider itself, or some specific staff member, is complicit in the crime.  Trainer should also ask participants to discuss whether this is a higher risk in formal or informal money remittance providers. | |
| Slide 8 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of remittance providers.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Remittance slips/receipts for funds 2. Forensic analysis of suspect computers can reveal use of online remittance services 3. Interviews with remittance provider staff 4. Records of remittance provider 5. Interception of suspect communication. | |
| Slide 9 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of remittance providers.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 8). | |
| Slide 12 | The trainer should ask the participants to consider a hypothetical scenario whereby a criminal has gained control of a victim’s bank account. The criminal would now like to extract funds from the victim’s bank account. What techniques can the criminal use to transfer/obfuscate the source of funds?  Through guided discussion the trainer should help the participants to identify the following key items:   1. International transfers 2. Structured transactions, using many small transactions below a reporting threshold 3. The use of mule accounts 4. The use of shell companies, either to transition or to aggregate funds 5. Withdrawing funds in cash 6. The use of compromised bank accounts as mule accounts 7. The use of payment services to purchase goods online   Trainer should not focus too heavily on the mule recruitment aspect of the typology, because this will be covered separately elsewhere.  Trainer should not focus too heavily on the cash withdrawal aspect of the typology, because this will be covered separately elsewhere. | |
| Slide 13 | Trainer should describe the typical wire transfer laundering typology, as per this slide.  Trainer should not focus too heavily on the mule recruitment aspect of the typology, because this will be covered separately elsewhere. | |
| Slide 14 | Financial institutions are heavily dependent on online banking services but that the non-face-to-face nature of the online banking service presents additional risks. It is also reasonable for a financial institution to expect that a certain percentage of customers will fall victim to cybercrime attacks and lose control of their banking credentials. The trainer should ask the participants to consider what controls financial institutions put in place to prevent the misuse of the banking credentials of a victim who has lost control of their banking credentials.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Additional controls around creation of new beneficiaries and international transfers (e.g. a customer may be allowed to log in to view their balance but may need to call a call-centre in order to set up a new beneficiary). 2. The use of second authentication factors, such as two factor authentication devices, mobile SMS codes, etc.   Automated fraud detection techniques which will identify transactions that are out-of-character for a particular customer | |
| Slide 15 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of wire transfers.  Through guided discussion the trainer should help the participants to identify the following key items:   * Banking records of the victim’s financial institution * Additional/new beneficiaries added to victim’s bank account * Forensic analysis of suspect PCs can reveal the use of online banking services * Large numbers of transfers of funds with descriptions such as “gift”. | |
| Slide 16 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of wire transfers.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 15). | |
| Slide 18 | The trainer should ask the students to discuss what challenges they think cash might present to cybercriminals, as opposed to other types of crime.  Through guided discussion, the trainer should help the students to identify the following key points:   1. Due to the inherently trans-national nature of cybercrime, cash withdrawn in one country may not easily be transferrable into the possession of the organising criminals, who may be residing in a different country. Therefore, further transfers, at additional cost to the criminals, will be required. 2. Direct contact is required between criminals to hand over cash. 3. Direct contact is required, in many cases, to use cash value. 4. Cybercriminals frequently structure funds into many small transactions to avoid financial reporting requirements and therefore aggregating the cash can be logistically challenging. 5. Carrying large amounts of cash across border increases risk of seizure   Cybercriminals are not stealing cash directly and therefore the cash is predominantly of value as a technique for breaking the chain of value. | |
| Slide 20 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of cash withdrawals.  Through guided discussion the trainer should help the participants to identify traditional indicators of cash usage, such as possession of large volumes of unexplained cash. Also, technological indicators such as possession of large numbers of prepaid value cards. | |
| Slide 21 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of cash withdrawals.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 20). | |
| Slide 23 | The trainer should ask the students what is a Internet payment service and to give examples of any specific Internet payment services they might be aware of. The example that will typically arise is Paypal.  Through guided discussion the trainer should identify the following categories of Internet payment services:   1. Banks offering money transfer services, where the Internet is only the channel through which the payment instruction is issued. 2. Non-banking services, operating only on the Internet, which are indirectly associated with a bank account.   The trainer should ask the attendees to consider what is the significance of banks offering money transfer services where the Internet is the channel through which the payment instruction is issued. Through guided discussion the trainer should help the attendees identify that the non-face-to-face nature of the transaction is the key differentiator. | |
| Slide 25 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of Internet Payment Services.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Banking records of the victim’s financial institution 2. Additional/new beneficiaries added to victim’s bank account 3. Forensic analysis of suspect PCs can reveal the use of online banking/Internet payment services 4. Records of Internet payment service provider. | |
| Slide 26 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of Internet payment services.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 25). | |
| Slide 27 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held by an Internet payment service provider.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| **HOUR 2** |  | |
| Slide 4 | Trainer should describe explain that mules are essential to many online laundering schemes.  Broadly speaking there are two categories of mules; those that know they are participating in illegal activity and those that think they are involved in a legitimate activity, e.g. a job offer.  Trainer should explain that unwilling mules are recruited through job offers listed on legitimate recruitment websites for jobs such as “financial manager” or “work at home” positions. Spamming services are also used to advertise and recruit potential money mules. | |
| Slide 5 | The trainer should ask the students to discuss the issue of willing vs. unwilling mules. The trainer should guide the discussion as follows:  The unwilling mule is often described as a credulous individual who is deceived by the professional nature of the engagement by their “employer” and believes that they are working for a legitimate company. However, this image is now being questioned more and more by police because there have been numerous instances where it has become apparent that the mule was fully aware of the illegal nature of their deeds.  The trainer should ask the opinion of the participants and consider how one might go about establishing whether or not an individual that is claiming to be an unwilling mule was, in fact, unaware of the illegal nature of their activities. | |
| Slide 6 | Trainer should describe the typical money mule laundering typology, as per this slide. | |
| Slide 7 | The trainer should ask the students to discuss the issue value of arresting/charging mules. The trainer should guide the discussion as follows:  The amount of funds handled by any particular mule is usually small, typically totalling less than 3,000 USD. However, when the amount of funds handled through the entire mule network is aggregated, the gains for the organisers of the cybercriminal activity are substantial, of the order of millions of dollars. The trainer should ask the students to bear in mind that the organisers of the cybercriminal activity may be located in more than one foreign jurisdiction, the organised crime activity can be complex and time consuming.  The trainer should also point out that a common technique involving money mules is for the mules to enter the country for the specific purpose of money mule activity. If they are arrested, it will presumably be their first offence in this jurisdiction and therefore they will, most commonly be charged and released, at which point the mule flees the country.  The trainer should ask the students to discuss the value of charging individual mules. The trainer should also ask the students to consider if and how the international organised criminal activity should be approached. | |
| Slide 8 | The trainer should ask the students what they consider to be the problems with money remittance providers from the perspective of investigation, search, seizure and confiscation of crime proceeds.  Through guided discussion the trainer should help the class to identify the following key issues:   1. If the remittance provider accepts or pays out in cash there is a possibility that an investigation could be impeded. 2. If the remittance provider does not adequately identify and retain identification of the customer, an investigation could be impeded. 3. If the remittance provider does not retain adequate transaction records, an investigation could be impeded. 4. If the remittance provider is not required by regulation to report suspicious activity, an investigation could be impeded. 5. If the remittance provider does not register their activities with the regulator, an investigation could be impeded.   The volume of legitimate cash transactions presents a challenge for identification of illegal cash transfers. | |
| Slide 9 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the activity of money mules.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Suspicious transaction reports from financial institutions where mules have accounts/presented themselves 2. Records from financial institution where stolen funds where held 3. Mule’s financial records. | |
| Slide 10 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/activity of money mules.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 9). | |
| Slide 11 | Note: During the discussion of international transfers, the trainer should endeavour to keep the conversation away from the area of international cooperation mechanisms, because this is covered in a separate lesson later in the day. | |
| Slide 13 | The trainer should ask the participants to consider challenges arise to the search, seizure and confiscation of criminal funds when the funds have been transferred internationally.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Increased difficulty gaining access to evidence 2. Mutual legal assistance delays 3. Jurisdictional issues 4. Inconsistent regulation of financial entities (e.g. virtual currency exchanges)   *Broken audit trails. How can you follow the criminal money trail if the funds are removed in cash?* | |
| Slide 14 | Trainer should describe the typical international transfer typology, as per this slide. | |
| Slide 15 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of international transfers.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Suspicious transaction reports made by financial entities to FIU 2. Banking records of the victim’s financial institution 3. Additional/new beneficiaries added to victim’s bank account 4. Forensic analysis of suspect PCs can reveal the use of online banking services. 5. Admissions 6. Special Investigative techniques 7. Surveillance. | |
| Slide 16 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of international transfers.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 15). | |
| Slide 18 | The trainer should ask the students to identify any virtual currencies they are aware of.  Through guided discussion, the trainer should help the students to identify at least the following:   * One example of a decentralised virtual currency, such as bitcoin * One example of a centralised virtual currency such as linden dollars * One example of e-money such as google checkout, paypal, payment cards, etc.   Any ideas identified by the students should be written on a flipchart, whiteboard etc. | |
| Slide 19 | Trainer should explain that this course uses FATF definitions for virtual currency, e-money and digital currency. See for further information:  [http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf%20)  Trainer might like to reference the ECJ judgement C-264/14 of October 22nd 2015, where the following definition is used:  “49. Transactions involving non-traditional currencies, that is to say, currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to the transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions.  52. In the case in the main proceedings, it is common ground that the ‘bitcoin’ virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators.  55. It is common ground that the ‘bitcoin’ virtual currency is neither a security conferring a property right nor a security of a comparable nature.”  The trainer should guide the students through a whiteboard exercise where the digital currencies identified during the previous discussion should now be categorised using the terminology here. | |
| Slide 20 | The trainer should, referring to the previous slide, point out that all three definitions refer to a “digital representation”. The trainer asks the participants what they think the significance of this expression in the definitions. The trainer should explain that this is an important point with significant practical and legal implications for cases involving digital currency.  Through guided discussion, the trainer should help the students to identify the following key points:   1. A digital representation is a representation of something in the form of digital data. 2. A physical object such as a computer, flash drive, CD ROM etc. may contain a digital representation of currency but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the relevant virtual currency system. 3. The critical point is that the digital data itself is the virtual currency, not the medium on which the digital data is stored. 4. The digital data can be copied or transferred to another storage medium, but the value remains inherent in the digital representation. | |
| Slide 21 | Trainer should explain that this course uses FATF definitions for virtual currency, e-money and digital currency. See for further information:  <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.  The trainer should guide the students through a whiteboard exercise where the digital currencies identified during the previous discussion should now be categorised using the terminology here. | |
| Slide 22 | Trainer should briefly introduce Bitcoin, being one of the most popular virtual currencies, particularly with cybercriminals. | |
| Slide 23 | Trainer should highlight some of the key properties of Bitcoin. | |
| Slide 24 | Trainer should explain using the example of ransomware, how criminals use virtual currencies. | |
| Slide 25 | Trainer should explain the virtual currency ecosystem concepts on this slide:  Virtual Currency Exchange: A person or entity engaged in the business of exchanging virtual currency for real currency, funds, other virtual currencies, precious metals, etc. for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wire transfers, credit cards and other virtual currencies. The currency exchange(s) may or may not be associated with the virtual currency administrator.  Virtual Currency Administrator: A person or entity engaged as a business in issuing (putting into circulation) or redeeming (withdrawing from circulation) a virtual currency. A virtual currency administrator will only exist for centralised virtual currencies. By definition, a decentralised virtual currency does not have an administrator.  A user/owner is a person who obtains virtual currency and uses it to purchase goods or services or transfers it to another person.  A miner is a person who participates in the operation of decentralised virtual currency by running software on their computer(s) to solve complex mathematical problems. The operation of mining is essential to the functioning of decentralised virtual currencies, such as Bitcoin, because the solution to the complex mathematical problem solved by the miners serves as the basis for validation of transactions in the virtual currency system. Miners typically receive a reward in virtual currency for performing mining activity.  A virtual currency wallet is a software, or other mechanism, for holding, storing and transferring virtual currency.  A wallet provider is an entity that provides a virtual currency wallet service to hold, store and transfer virtual currency. The wallet provider holds a user’s private keys, possession of which allows the user to conduct transactions involving specific currency units. Wallet providers provide services such as backups (hot or cold backups), mixing (obfuscation of virtual currency transactions), etc.  Merchants receive funds in the form of virtual currency from users/owners in exchange for goods and services.  Other entities such as software developers, site administrators and so on may also be involved in the operation of a virtual currency. | |
| Slide 26 | The trainer should ask the participants to consider how the virtual currency ecosystem interfaces with the traditional financial system.  Through guided discussion the trainer should help the participants to identify the following interfaces:   1. Virtual currency exchanges 2. Financial institutions 3. Cash/ATMs 4. Payment Cards 5. Money remittance providers 6. Merchants accepting virtual currency. | |
| Slide 27 | Trainer might want to point out that the 4th EU money laundering directive will require customer due diligence to be carried out by virtual currency exchanges. | |
| Slide 28 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of Virtual Currencies.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Banking records of the victim’s financial institution 2. Forensic analysis of suspect PCs can reveal the use of virtual currency software and/or virtual currency exchange 3. Examination of blockchain/transaction records of virtual currency provider 4. Records of virtual currency exchange 5. Records of virtual currency administrator (if exists).   Trainer should ask participants to consider what types of information might be available from a virtual currency business. Virtual currency businesses that are subject to know-your-customer (KYC) obligations would be able to provide:   * Identity documentation (which could include user’s picture) * Location verification documentation * IP address * Phone number * Transaction history * Deposit and withdrawal addresses * Bank name, bank account number and transaction information. | |
| Slide 29 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of cash withdrawals.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 25). | |
| Slide 30 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held in the form of virtual currency.  Through guided discussion the trainer should help the participants to identify the relevant national provisions.  Depending on the student group, the trainer may consider highlighting some of the challenges with freezing, seizing and confiscation of virtual currency value, such as volatility of the exchange rate, the fact that the criminal may have wallet backups stored elsewhere, etc.  These topics are further elaborated in the advanced course. | |
| **HOUR 3** |  | |
| Slide 4 | The trainer should ask the students to discuss the issue of purchases through the internet. The trainer should guide the discussion as follows:   * Suppose you had a stolen credit card, how could you use it on the Internet for your personal gain? * The trainer should highlight the following key points: * Purchasing goods and services through the Internet, which are then shipped to the criminal or to a mule, is a good way of converting stolen data into real-world value. * Goods and services which can be easily resold are particularly attractive. One particular example (other than obvious things like jewellery and other high-value goods) is airline tickets. * The use of stolen data is prevalent in high-risk markets such as counterfeit pharmaceuticals, firearms, child pornography, etc. * Online gambling sites are another high-risk area for money laundering/use of stolen credentials * The use of online auction sites is another risk area. | |
| Slide 5 | Trainer should describe the typical internet purchase typology as per this slide. Trainer should point out that the financial advantage to the criminal comes from the payment from the winner of the auction, not directly from the compromised credentials. With this in mind, the trainer should ask the students what difference it makes if the payment comes via the action site (e.g. ebay), via an Internet payment service (e.g. paypal) or directly from the winner (e.g. by bank transfer or money remittance provider). | |
| Slide 6 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of Internet purchases.  Through guided discussion the trainer should help the participants to identify the following key items:   * Records of the Internet site where the purchase transaction was performed (e.g. auction site) * Records of the payment mechanisms used to pay for the purchased goods (e.g. paypal) * Possession of goods * Records of service provider if service paid for using stolen credentials * Electronic evidence on suspect PC indicating use of internet payment services and/or internet purchase sites. | |
| Slide 7 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/activity of Internet purchases.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| Slide 8 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held in the form of virtual currency.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slides 7 and 8). | |
| Slide 12 | The trainer should ask the participants to consider challenges arise from the use of shell companies, particularly in the case where online crime proceeds are involved.  Through guided discussion the trainer should help the participants to identify the following key items:   * Increased difficulty gaining access to evidence * Mutual legal assistance delays * Jurisdictional issues * Increased complexity of financial/money laundering scheme may present challenges for online service providers. | |
| Slide 13 | Trainer should describe the typical shell company typology, as per this slide. | |
| Slide 14 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of shell companies.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Suspicious transaction reports made by financial entities to FIU 2. Banking records of the victim’s financial institution 3. Additional/new beneficiaries added to victim’s bank account 4. Forensic analysis of suspect PCs can reveal the use of online banking services 5. Business activities, assets and liabilities (or lack thereof) of shell company 6. Owners/controllers of shell company 7. Legal structure of shell company. | |
| Slide 15 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of shell companies.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 14). | |
| Slide 16 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held by a shell company.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| Slide 20 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of prepaid cards.  Through guided discussion the trainer should help the participants to identify the following key items:   * The possession of prepaid cards (or mobile phone topups, or other forms of anonymous credit) * Forensic analysis of suspect PCs can reveal the activity of purchasing prepaid cards and/or selling prepaid cards * Evidence from the physical location where the prepaid cards were purchased. | |
| Slide 21 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of prepaid cards.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| Slide 22 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of prepaid cards.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 21). | |
| Slide 23 | Note that the focus of this presentation is on the risks presented by online gaming platforms[[1]](#footnote-1).  Trainer should explain that the risks presented by online gaming platforms are understood, they have not been well studied at the time of writing of this course. Therefore, the information in this section is based on anecdotal experience and an understanding of the risks presented by these platforms at the time of writing. | |
| Slide 24 | Trainer should explain that online betting platforms allow for gambling of various types, from poker to scratch cards, horse racing, sports betting, etc.  Trainer should explain that funds are typically lodged to an account held by the online betting platform, from which bets are placed and to which winnings are lodged. Funds can be lodged using a variety of techniques although typically bank transfers and payment cards are used. Trainer should reference the prepaid cards discussion from immediately before this section.  Players can typically have their winnings credited to a bank account or to a payment card.  Trainer should point out that there are challenges with regulation of online gambling, due to the fact that in some countries online gambling platforms are illegal, whereas in others they are not. Additionally, due to the trans-national nature of the Internet, online gambling companies are often not in the jurisdiction where the players are located. | |
| Slide 26 | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of online gambling platforms.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Records of online gambling company 2. Suspicious activity reports by online gambling company, if online gambling company is regulated in your jurisdiction and required to produce suspicious activity reports. 3. Forensic analysis of suspect PCs can reveal the use of online gambling platforms (web activity and/or installed software). | |
| Slide 27 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of online gambling platforms.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 26). | |
| Slide 28 | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds from online gambling platforms.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. The trainer should also use the case studies to gauge whether the objectives of the session were met. | | |

1. FATF (2009) Report on Vulnerabilities of Casinos and Gaming Sector, see

   <http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf> [↑](#footnote-ref-1)