College of Informatics and Virtual Education (CIVE)

IA 418: Cyber Criminology and Techniques

Fraud and Financial Crimes:

Fraud and Money Laundering

1

Credit/Debit Card Fraud

- A **credit card** is a payment card, usually issued by a bank, allowing its users to purchase goods or services or withdraw cash on **credit**.
  - ✓ Many people use credit cards and pay off their balances each month in full, incurring no fees or interest.
  - ✓ Others carry balances from month to month, meaning they are paying interest on money they have already spent, and could be charged a fee for missing a payment.



Credit/Debit Card Fraud

- Credit cards provide automatic, predictable fraud protection that limits your liability in case your card is stolen or used without your permission.
- A **debit card** is a card issued by a bank or credit union to checking account holders that is used to **access funds in the account**.
  - ✓ You can use a debit card to access cash from an ATM or to buy goods or services.
  - ✓ Spending with a debit card means you're spending your money – it comes directly from your account.

Credit/Debit Card Fraud

- Credit/Debit card fraud is a type of cybercrime where a fraudster gains access to sensitive information regarding your credit/debit card.
  - ✓ Such sensitive information include:
    - Credit card number
    - Personal Identification Number (PIN)
    - Credit Verification Value (CVV)-a three digit number provided by companies that make bank cards.
    - Other similar details needed to use the card to make a purchase.



Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Lost or stolen cards**:
    - Fraudsters can obtain credit cards by either finding them after they have become **lost** or **stealing** them from someone's possession.
    - The fraudster may not be able to use the lost or stolen card at a point of sale (PoS) device, which requires a PIN.
    - However, the fraudster can use the card details to make purchases **online**.



Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Card-not-present fraud**:
    - In this case, the fraudster does not require the criminal to have a physical credit card.
    - Fraudsters obtain **basic details**, such as the **account holder's name**, the **credit card number**, and the **expiration date**.
    - With this information, they can commit fraudulent activity by mail, via the phone, or online.

Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Card-not-present fraud**:
    - Basic details can be obtained from the victim using **phishing**.
    - Fake emails looking authentic prompts a victim to share sensitive information or click a link to make a seemingly urgent payment.

Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Counterfeit, doctored, or faked cards**:
    - Devices known as **skimmers** can illegally obtain credit card details.
    - Skimmers capture information from the credit card's magnetic strip.
    - Captured information are used by the fraudster to create fake cards by encoding details.
    - It might be hard to detect the difference between a regular card reader or ATM and one with a skimmer attached to it.



Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Application fraud**:
    - A fraudster applies for new credit in someone else's name.
    - It is achieved by using the victim's personal information, such as their full name, date of birth, address, and Social Security Number/NIDA Number.
    - They may even steal supporting documentation to substantiate their application.

Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Account takeover**:
    - After gaining personal information, a fraudster can then contact their credit card company and pretend to be the account holder.
    - The fraudster presents information like previous purchases, passwords, and card details.
    - Works by registering a change of address and then report the card as lost or stolen to get a new card sent out through the mail.



Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Mail Interception**:
    - Credit cards can be intercepted when sent by posts.
    - The fraudster intercepts or steals a new credit card from the victim's mailbox.
    - This is why most card issuers will use unmarked letters and packaging when sending cards.



Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Pagejacking**:
    - Fraudsters create web pages and websites that look authentic.
    - Victims are tricked into making a purchase or executing a financial transaction on such fraudulent pages.
    - Fraudsters get free access to sensitive information the credit/debit card.



Credit/Debit Card Fraud

- How does Credit/Debit Card fraud happen?
  - ✓ **Keystroke Logging**:
    - The fraudster uses keylogging software to record the keystrokes made on a computer.
    - The software is typically downloaded on your computer when you click a suspicious link.
    - The software helps fraudsters identify the PIN, passwords, credit card numbers, and other such crucial details to execute a well mastered credit card fraud.



Credit/Debit Card Fraud

- Signs of Credit/Debit card fraud:
  - ✓ Unauthorized charges appearing on your statement
  - ✓ Reporting a lost or stolen card, or receiving unfamiliar receipts from unknown merchants.
  - ✓ Frequent transaction declines, especially for legitimate purchases.

Credit/Debit Card Fraud

- Signs of Credit/Debit card fraud:
  - ✓ Unsolicited calls or emails requesting your card information, alterations in your monthly statements or the unexpected arrival of new cards you didn't request.
  - ✓ Unusual activity, and multiple failed login attempts on your card account.
- **Class activity:**
  - ✓ Experimenting with e-commerce services, explain credit/debit card details requested when making online payments.

Identity Theft and Identity Fraud

- **Identity fraud :** an array of illegal activities based on fraudulent use of identifying information of a real or fictitious person.
  - ✓ Identity fraud encompasses **identity theft**.
- Although usually undertaken for financial gains, it can also be used for the following purposes:
  - ✓ Gain access to secure or privileged areas.
  - ✓ Minors may attempt to purchase alcohol or gain access to night clubs or gambling establishments.
  - ✓ Foreigners may seek border entry or terrorists desiring concealment.

Identity Theft and Identity Fraud

- Identity fraud is committed when a **credible identity** is created by accessing others':
  - ✓ Credit cards
  - ✓ Financial or employment records
  - ✓ Secure facilities
  - ✓ Computer systems, etc.
- Upon development of the credible identity, the criminals can engage in:
  - ✓ Credit card fraud
  - ✓ Create additional lines of credit and separate bank accounts

Identity Theft and Identity Fraud

- Upon development of the credible identity, the criminals can engage in:
  - ✓ Terrorism and exploit the information to conceal their true identities.
- Identity theft/fraud may be perpetrated by individuals, loose social or business networks, terrorist groups, and criminal organizations.
- It may be used for personal gain or corporate interests, or to facilitate the globalization of crime by terrorists and organized crime groups.

Identity Theft and Identity Fraud

- Identity theft happens when someone uses your personally identifying information, like **name**, **NIDA number**, or **credit card number**, without your permission.
  - ✓ The information is commonly used to commit **fraud** or other **crimes**.
- Identity theft and Identity fraud utilize personal information, such as **name**, **address**, **date of birth**, **taxpayer identification number**, alien registration or passport number, historical information, and/or biometric information.

Identity Theft

- What can cybercriminals do with the stolen identity?
  - ✓ **Credit Card Fraud**: a credit card is opened using the victim's identity and or change the billing address of the card.
  - ✓ **Phone and utilities**: open new accounts on the victims' identities and run up charges on their existing accounts.
  - ✓ **Bank/Financial**: create fake cheques on the victim's name or account number, write bad checks, take loans, create fake ATM cards, etc.
  - ✓ **Government:** use the identity to get a driving license, pension benefits, file fraudulent tax returns, etc.

How Identity Theft Occurs

- Phishing, Vishing and Smishing:
  - ✓ A fraudulent process of acquiring sensitive information (usernames, passwords, credit cards #, etc) by masquerading as a trustworthy entity.
  - ✓ **Phishing** is carried out by **email** and directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
  - ✓ **Vishing** works with a **phone** by asking a victim to call a phone number to verify some information.
    - ❑ When a call is made, the fraudster will ask for personal information.

How Identity Theft Occurs

- Phishing, Vishing and Smishing:
  - ✓ With **smishing**, cybercriminals send deceptive text messages (SMS) to lure victims into sharing personal or financial information.
  - ✓ These deceptive messages often appear to be from trusted sources.
  - ✓ They use social engineering tactics to create a sense of **urgency**, **curiosity**, or **fear** to manipulate the recipient into taking an undesired action.

How Identity Theft Occurs

-----Original Message-----
From: Well Fargo Online [mailto:onilinebanking@wellsfargo.toxement.com.co]
Sent: Tuesday, August 07, 2012 9:58 PM
To: O'Brien, Aimee
Subject: Alert: You Have (1) New Security Message

Wells Fargo is constantly working to ensure security by regularly screening the accounts is our system. We recently reviewed your account (error code : 00562), and we need more information to help.

How can I restore my account access ?

Click Here, <http://www.isrjapan.jp/wp-content/themes/wells/www.wellsfargo/online.htm> login and complete the next step to "Your Security Questions."

Completing all of the informations required will automaticlly restore your account access.

You will be redirected to a secure, private Wells Fargo server on a random port due security issues.

Wells Fargo, N.A. Member FDIC.
© Wells Fargo Corporation. All rights reserved.

How Identity Theft Occurs

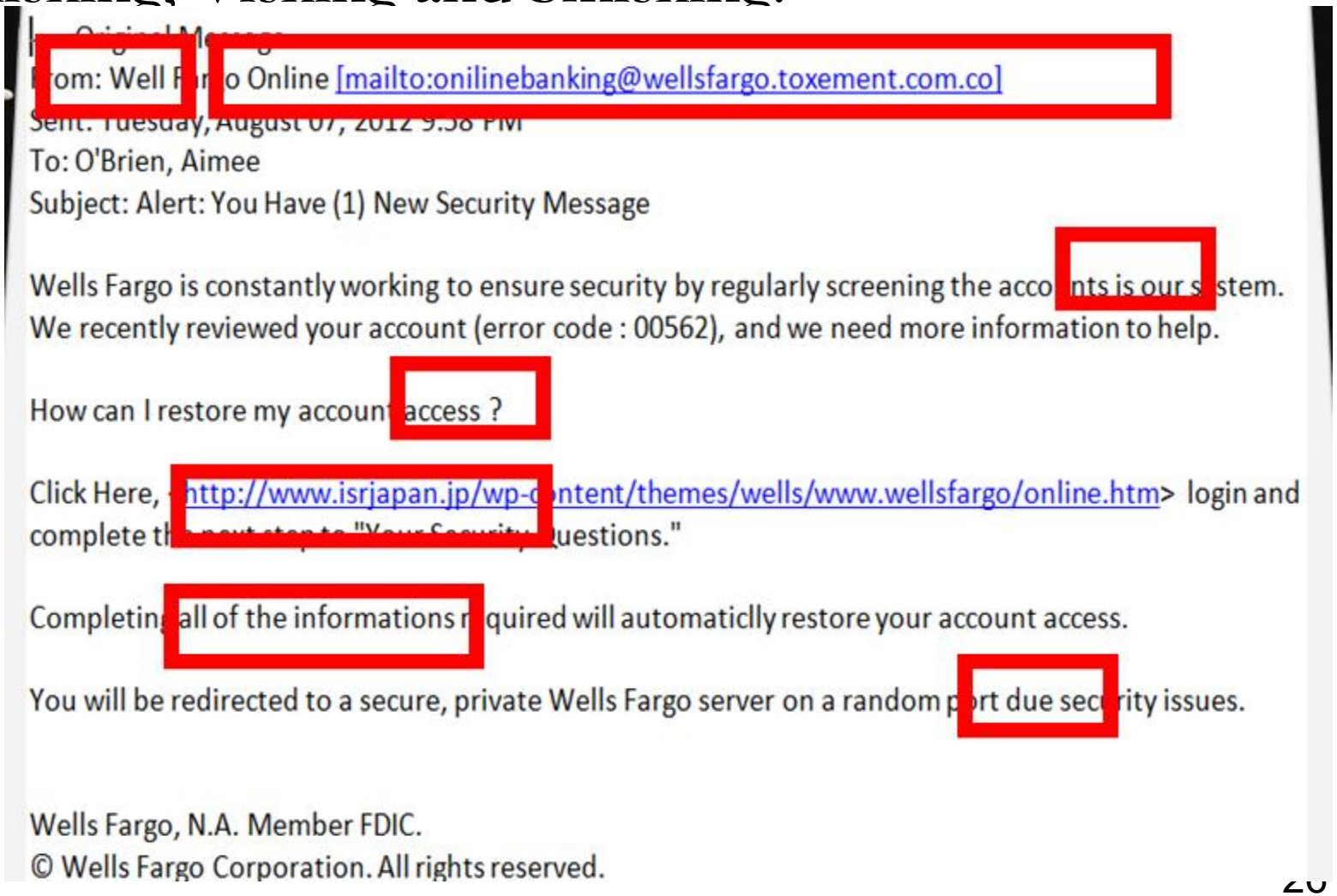
- Phishing, Vishing and Smishing:
  - ✓ Who can spot what's wrong with the email on the previous slide?
  - ✓ What are the red flags you'd notice that would identify to you this email is not from a trustworthy source?
  - ✓ What items should you look out for when you receive emails like this?

How Identity Theft Occurs

- Phishing, Vishing and Smishing:
  - ✓ Consider the following:
    - ❑ Misspellings, typos, random web links, strange 'from' email address, a sense of urgency, a generic greeting.
  - ✓ These would not appear in this way in a professional banking email from a large corporation.

How Identity Theft Occurs

- Phishing, Vishing and Smishing:



From: Well Fargo Online [mailto:onilinebanking@wellsfargo.toxement.com.co]
Sent: Tuesday, August 07, 2012 9:58 PM
To: O'Brien, Aimee
Subject: Alert: You Have (1) New Security Message

Wells Fargo is constantly working to ensure security by regularly screening the accounts is our system.
We recently reviewed your account (error code : 00562), and we need more information to help.

How can I restore my account access ?

Click Here, http://www.isrjapan.jp/wp-content/themes/wells/www.wellsfargo/online.htm> login and complete the next step to "Your Security Questions."

Completing all of the informations required will automaticlly restore your account access.

You will be redirected to a secure, private Wells Fargo server on a random port due security issues.

Wells Fargo, N.A. Member FDIC.
© Wells Fargo Corporation. All rights reserved.

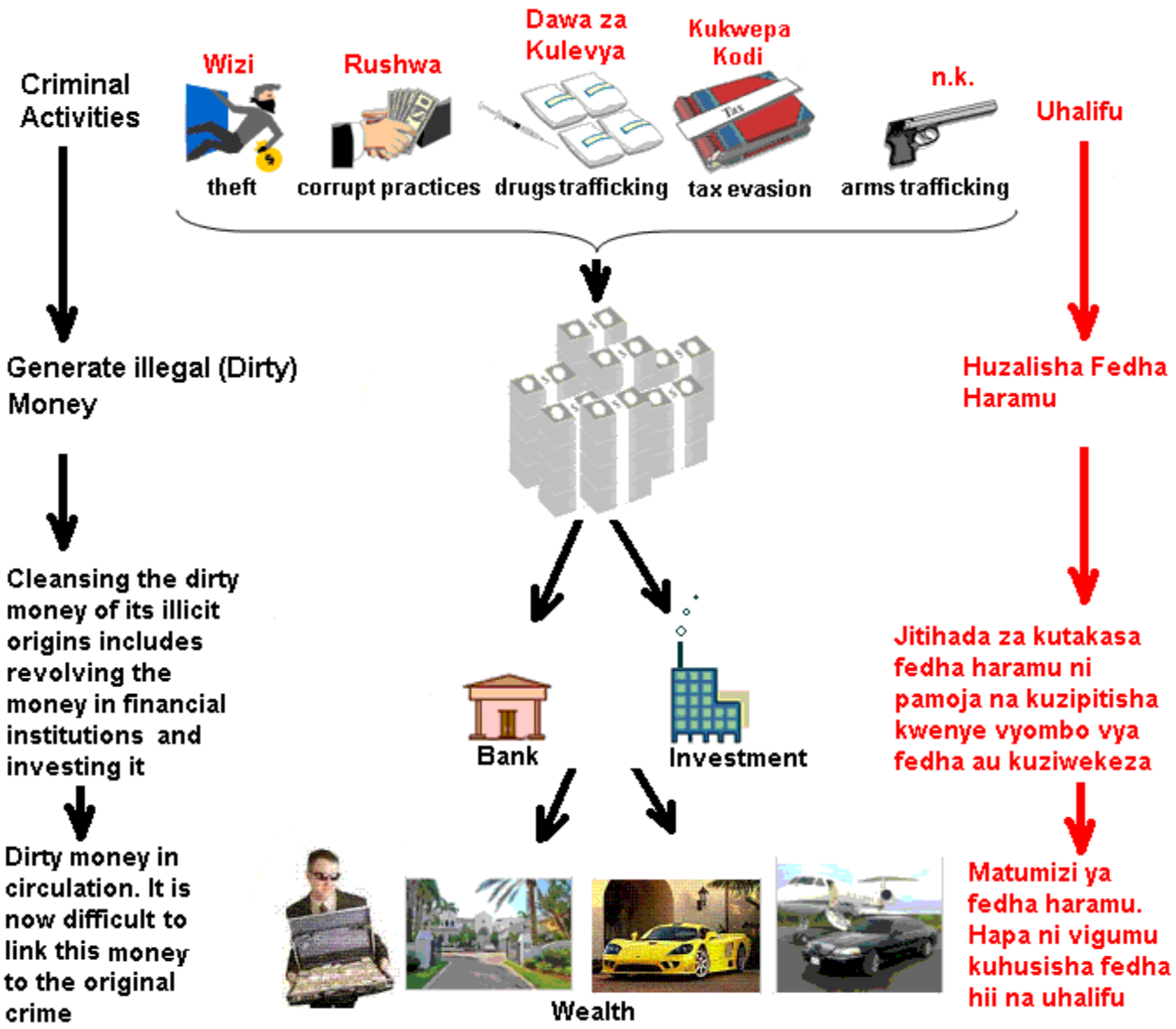
How Identity Theft Occurs

- Dumpster diving:
  - ✓ Going through trash to find documents or mails with personally identifying information.
- Skimming:
  - ✓ Stealing bank card/credit card numbers using a special hidden device when making transactions.
- Shoulder surfing
  - ✓ Listen to conversations made in the public area or watch when details are being entered on a computer.

How to Prevent Identity Theft?

- Class discussion:

Money Laundering



Money Laundering

- Money Laundering means transferring illegally obtained money or investments through an outside party to conceal the identity, source, and or destination.
  - ✓ It is the backbone of both domestic and international black-markets and underground economies.
  - ✓ The internet has increased both the amount of the revenue concealed and the ease in transaction disguising.
- Money laundering generally means "washing" proceeds or profits generated from:
  - ✓ Drug trafficking
  - ✓ People smuggling
  - ✓ Arms, antique, and gold smuggling

Money Laundering

- Money laundering generally means "washing" proceeds or profits generated from:
  - ✓ Prostitution rings
  - ✓ Financial frauds
  - ✓ Corruption
  - ✓ Illegal sale of wildlife products and other specified predicate offences.
- Money laundering process: whether technological or traditional, the process of money laundering occurs in three stages:
  - ✓ **Placement**: the initial point of entry for illicit funds.

Money Laundering

- Money laundering process: whether technological or traditional, the process of money laundering occurs in three stages:
  - ✓ **Placement**: the initial point of entry for illicit funds.
    - ❑ Involves movement of proceeds, frequently currency, from the scene of the crime to a place, or into a form, less suspicious and more convenient for the criminal.
  - ✓ **Layering**: the development and maintenance of complex networks of transactions designed to obscure the process and the source of illegal funds.
    - ❑ This involves the obscuring of financial and commercial transactions and/or assets.

Money Laundering

- Money laundering process
  - ✓ **Layering**:
    - ❑ "Layering of funds" is accomplished by conducting multiple transactions or by developing complex hierarchies of assets aimed toward distancing origination from laundered assets.
    - ❑ The criminals frequently use **shell corporations**, **offshore banks** or countries with loose regulation and secrecy laws for this purpose.
  - ✓ **Integration:** the return of funds into the legitimate economy.

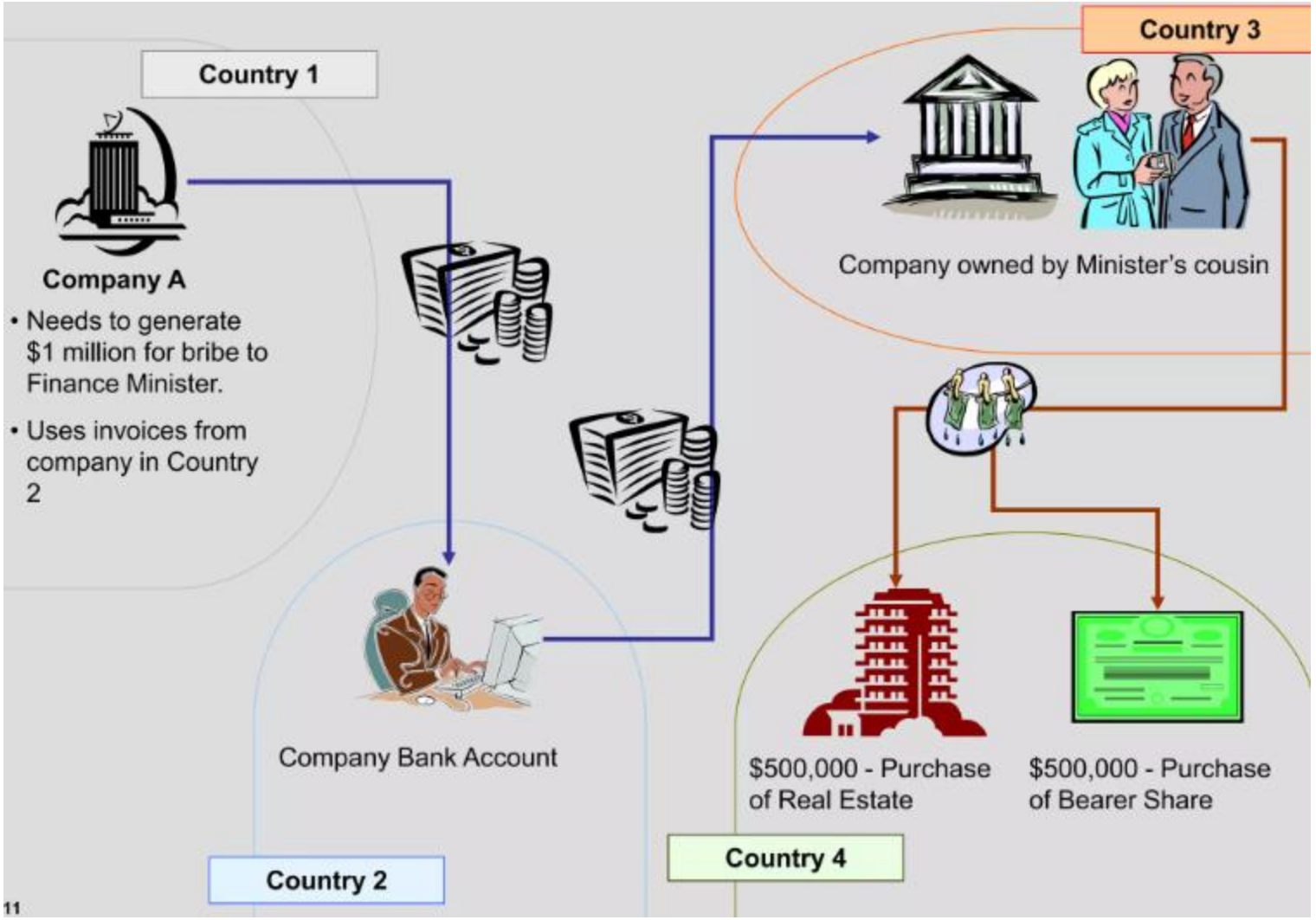
Money Laundering

- Money laundering process
  - ✓ **Integration:** the return of funds into the legitimate economy.
    - ❑ It represents the conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations.
    - ❑ Integration creates the illusion of a legitimate source for criminally derived funds and involves techniques as numerous and creative as those used by legitimate businesses.
    - ❑ For e.g **false invoices** for goods exported, domestic loan against a foreign deposit, purchasing of property and co-mingling of money in bank accounts.

Money Laundering

- Money is laundered through:
  - ✓ Banks
  - ✓ Brokerage firms
  - ✓ Financial services
  - ✓ Realtors
  - ✓ Crooked lawyers and accountants

Money Laundering Example



Money Laundering

- The internet is increasingly being used to launder money because of the following reasons:
  - ✓ Lack of **physicality** and bulk associated with e-money or e-funds.
    - ❑ It eliminates the need for the identification and maintenance of physical structures to store or otherwise conceal large amounts of cash.
  - ✓ Risk of **detection** is further reduced as criminals no longer have to physically possess the illegal "goods."
  - ✓ E-money provides criminals with a higher degree of **anonymity**—as no serial numbers or identifying marks are present.

Money Laundering Red Flags

- There are a number of observations regarding a financial transaction giving a hint of money laundering:
  - ✓ Online transactions involving parties located in high-risk countries.
  - ✓ Unusual transactional behavior such as suddenly **increased frequencies** or **volumes** of online transactions.
  - ✓ A high number of payments made with **prepaid cards** or with **virtual currencies** such as Bitcoin.

Money Laundering Red Flags

- There are a number of observations regarding a financial transaction giving a hint of money laundering:
  - ✓ Recently opened online accounts that receive **large deposits** or conduct **large transactions** that are inconsistent with the customer's profile or account history.
  - ✓ Email or social media solicitations for **fraudulent charity donations.**

Money Laundering Red Flags

- There are a number of observations regarding a financial transaction giving a hint of money laundering:
  - ✓ Charitable organizations that do not have an **in-depth history** or cannot be independently verified as legitimate organizations.
  - ✓ Correspondence sent to or from customers that indicate phishing attempts, frequent misspellings in the text of correspondence, or suspicious address credentials.

Why Combat Money Laundering?

- Money laundering has potentially devastating economic, security, and social consequences.
- Money laundering is a process vital to making crime worthwhile.
- It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises.
- Money laundering diminishes government tax revenue and therefore, indirectly harms honest taxpayers.
- It also makes government tax collection more difficult.