

# **Legal Challenges to Incorporating Evidence in Judicial Proceedings: Email Evidence & FIU Modernization**



**Elizabeth Aloï  
Trial Attorney  
Asset Forfeiture & Money  
Laundering Section  
U.S. Department of Justice**

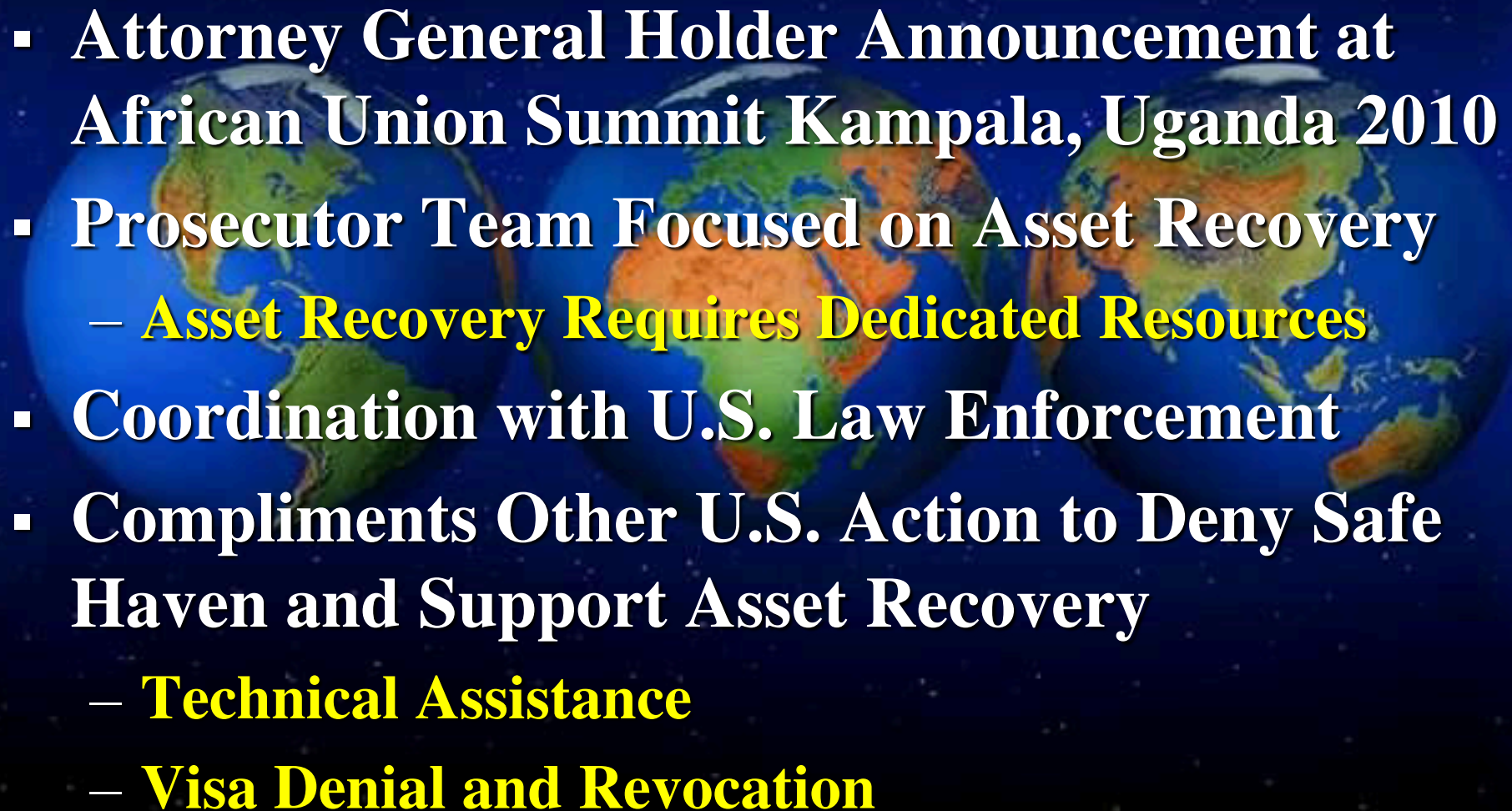
# OVERVIEW

---

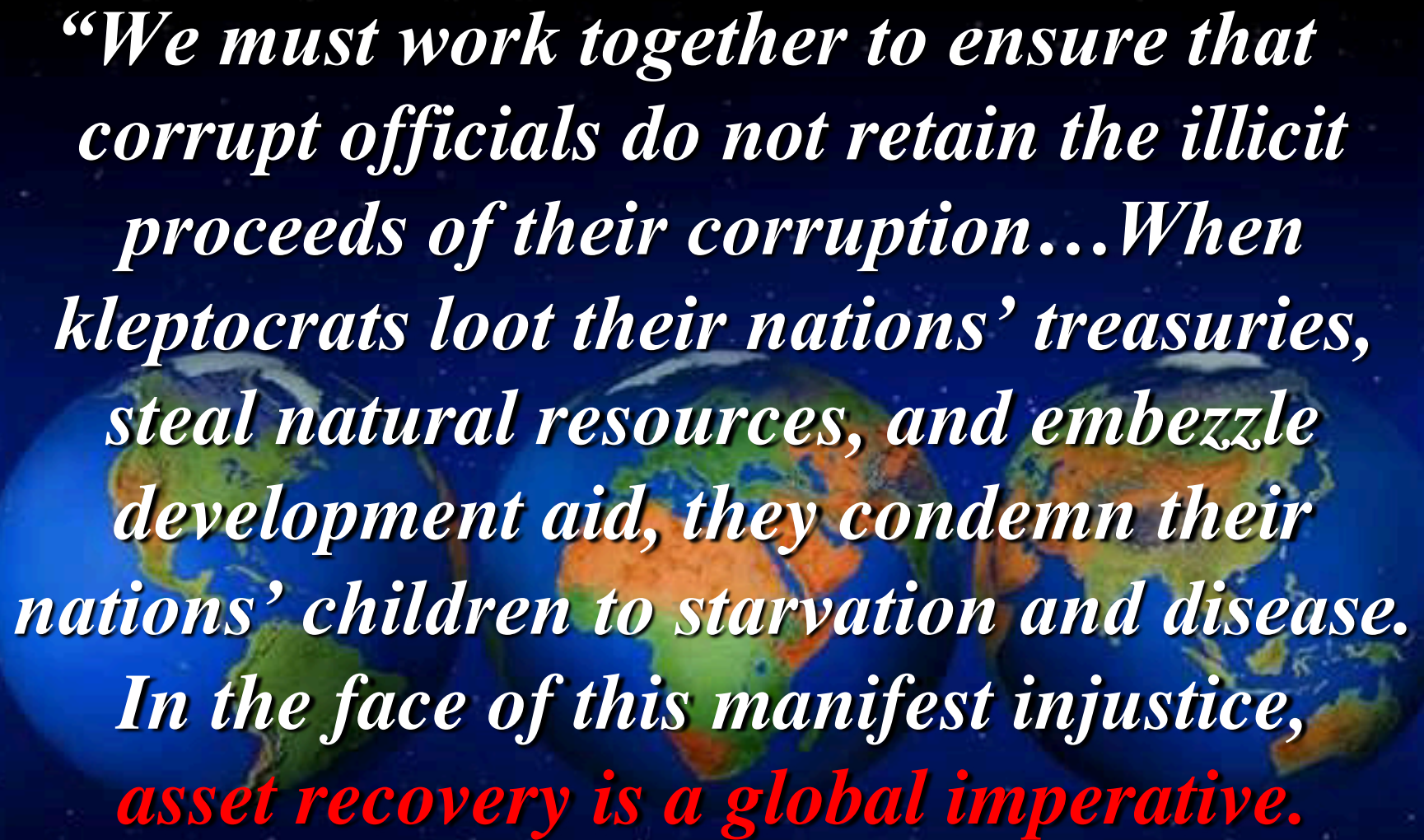
- **The Kleptocracy Asset Recovery Initiative**
- **Legal challenges associated with obtaining, and utilizing the content of electronic mail; and**
- **FinCEN's (FIU) modernization efforts**

# **U.S. DEPARTMENT OF JUSTICE KLEPTOCRACY ASSET RECOVERY INITIATIVE**

---

- 
- Attorney General Holder Announcement at African Union Summit Kampala, Uganda 2010
  - Prosecutor Team Focused on Asset Recovery
    - **Asset Recovery Requires Dedicated Resources**
  - Coordination with U.S. Law Enforcement
  - Compliments Other U.S. Action to Deny Safe Haven and Support Asset Recovery
    - **Technical Assistance**
    - **Visa Denial and Revocation**





*“We must work together to ensure that corrupt officials do not retain the illicit proceeds of their corruption...When kleptocrats loot their nations’ treasuries, steal natural resources, and embezzle development aid, they condemn their nations’ children to starvation and disease. In the face of this manifest injustice, asset recovery is a global imperative.”*

– **U.S. Attorney General Eric Holder**

**Global Forum VI Doha, Qatar November 7, 2009**

# Why Asset Forfeiture?

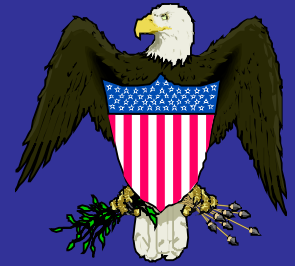
”

- Deprive criminals of the profits of their crimes;
- Break up criminal organizations, and prevent the financing of further crimes; and
- Recover stolen assets or provide restitution to victims or the government.

# Challenges Associated with Obtaining, and Utilizing the Content of Electronic Mail

- In order to access the content of email, U.S. investigators need a search warrant.
- Requests for evidence and the probable cause standard

# Why search email?



- What do we want to know?

▪make.money.fast@yahoo.com

▪Real  
identit  
y?

▪Communi  
cating with  
whom?

▪What  
are  
they  
saying?



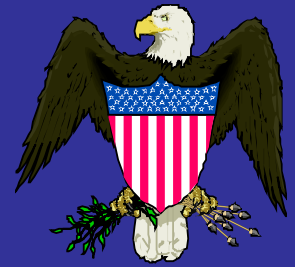
# How does this help in financial investigations?



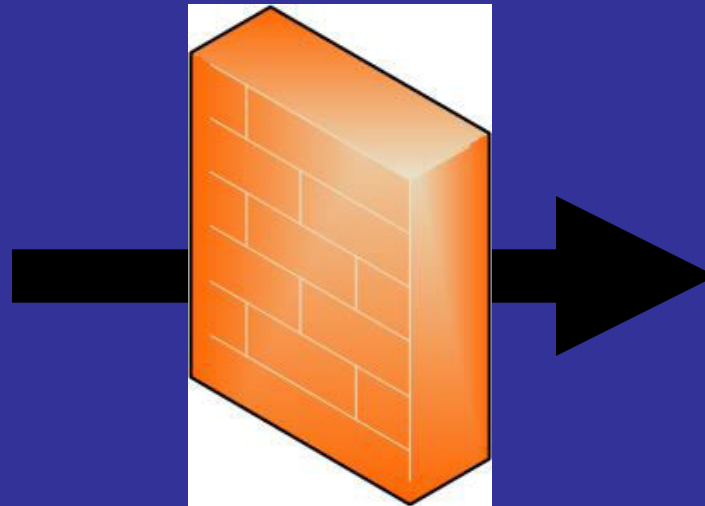
- Subjects may have bank statements sent to their email address.
- Subjects may be directing the movement of criminal proceeds by email.
- Communication between facilitators, gatekeepers, and money launderers.



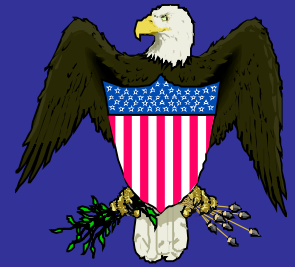
# ECPA and Email



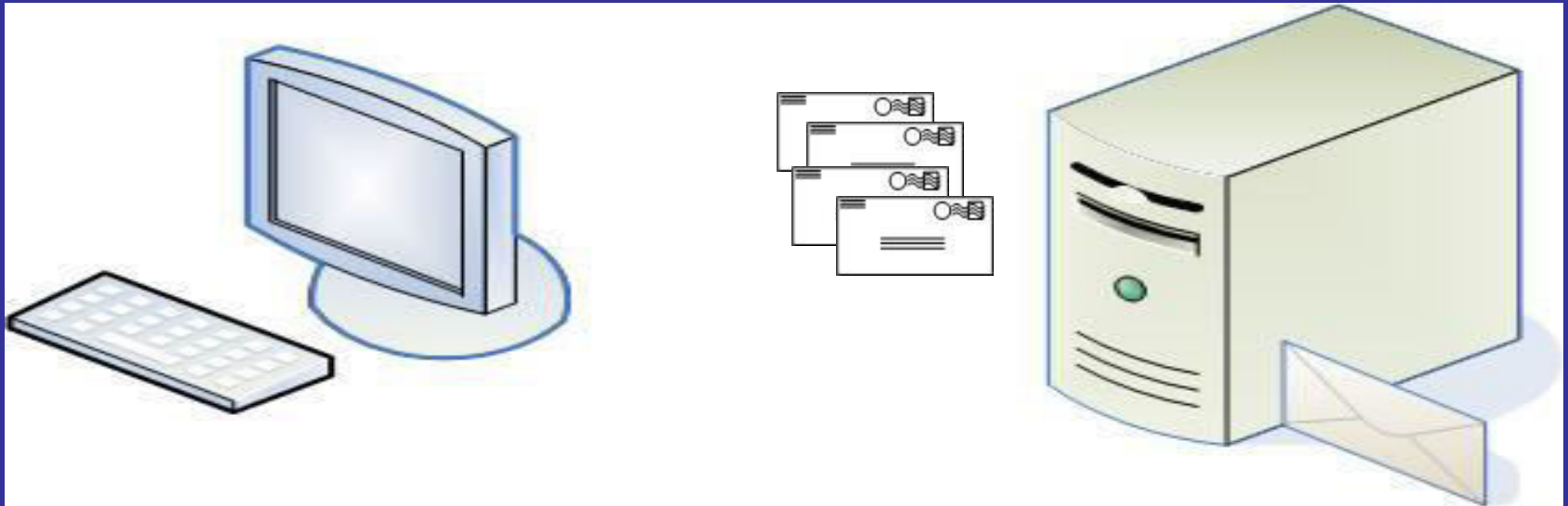
- Electronic Communications Privacy Act limits the United States' ability to obtain email evidence.



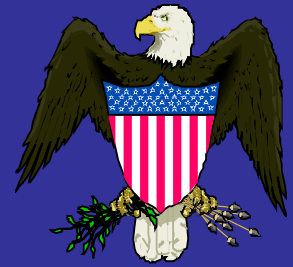
# How email works



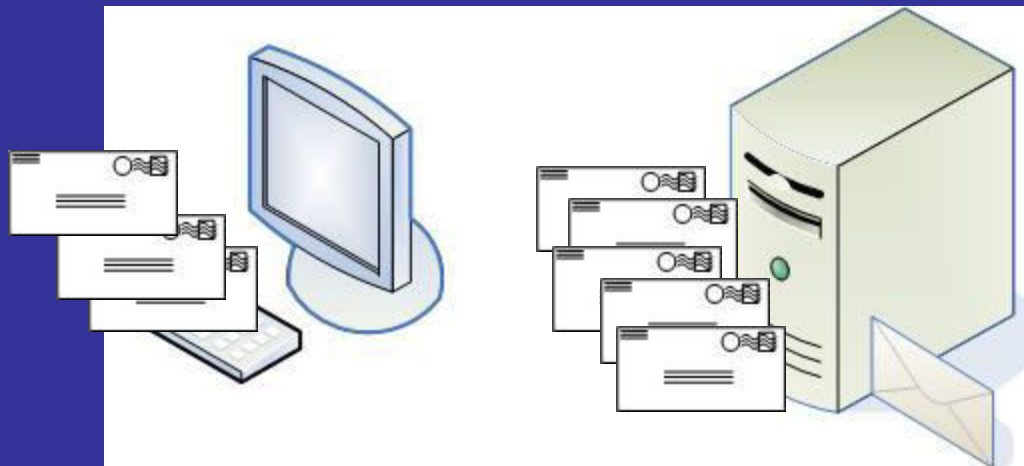
- A mail server receives and stores your e-mail



# How email works



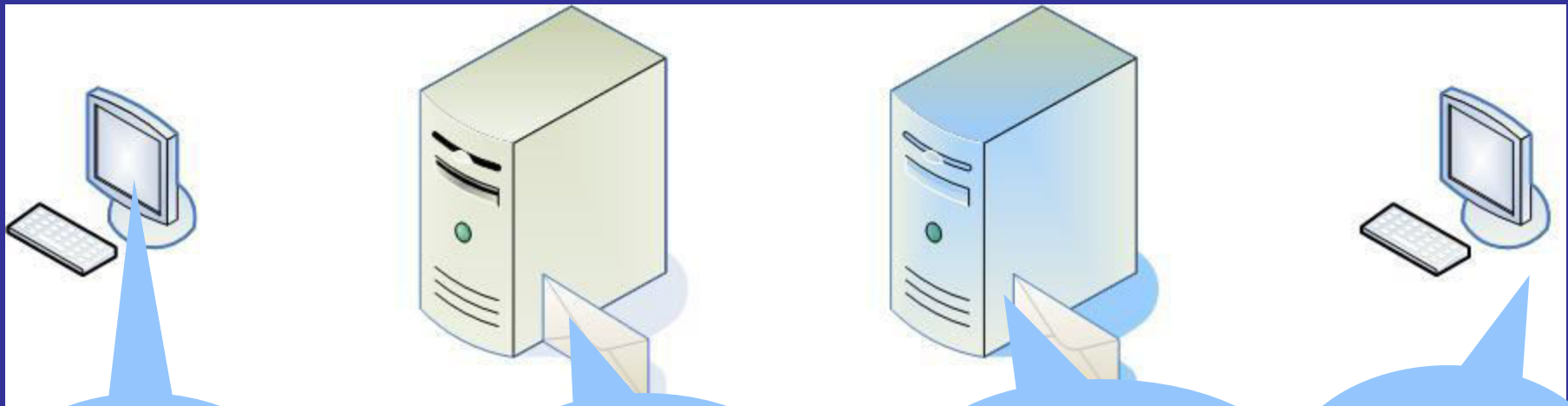
- Copies are sent to you



# Where is someone's e-mail?



- Four copies, in different places
- Usually search the receiver's server



▪Sender's  
hard  
drive

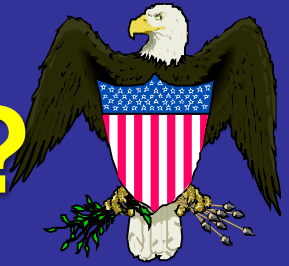
▪Sender's  
server

▪Receiver's  
server

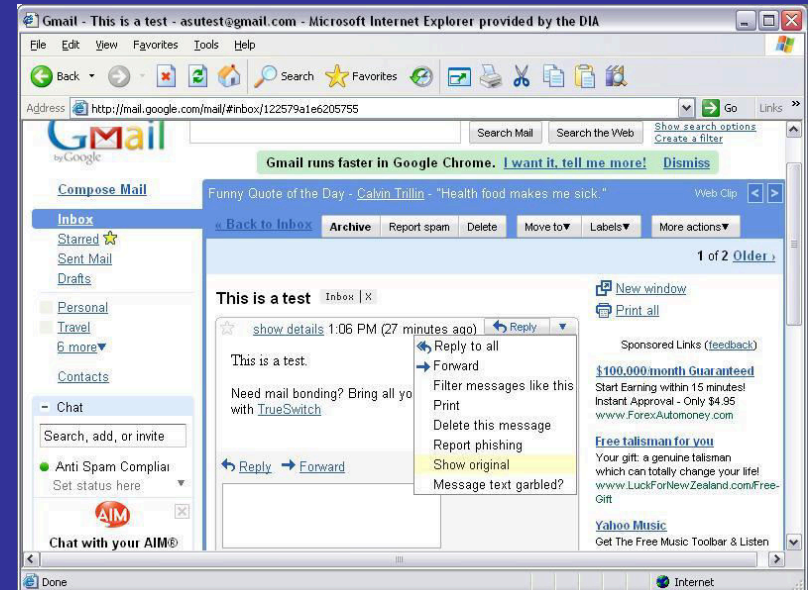
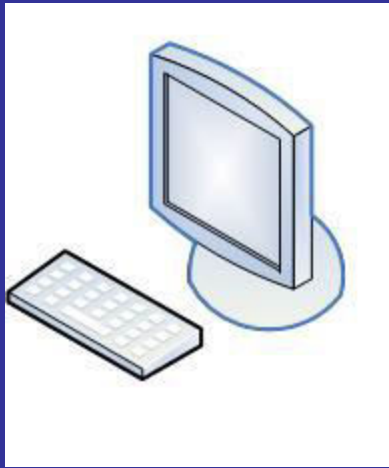
▪Receiver's  
hard  
drive



# Different Email Clients?



- Different forms, same function

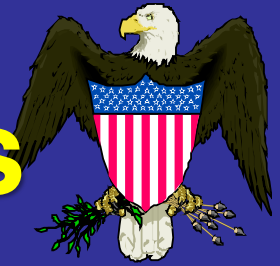


# **What is obtainable by search warrant?**

- **To/From**
- **Attachments**
- **Subject Line**
- **Content of Messages**
- **IP Addresses**



# Investigation objectives



- Content of communications

- `make.money.fast@yahoo.com`

- New, received e-mail

- Old, received e-mail

- Sent e-mail

- Drafts

- What are they saying?

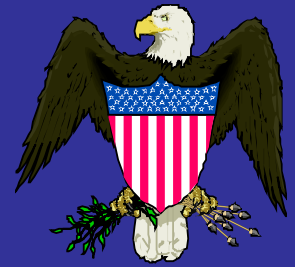
# Requests to the U.S. for Evidence: General

---

- Purpose for which evidence sought
- Summary of Facts
  - Include connection btw target and evidence
- Description of Offenses Charged or Investigated
- Detailed Description of Evidence Sought
  - Names, addresses, time period, account info...
  - Describe connection to investig/prosecution



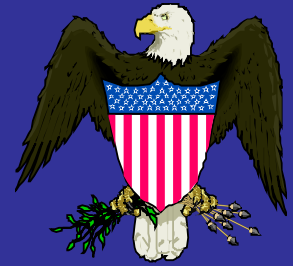
# Requests to the U.S. for Evidence: Search Warrants



## Include:

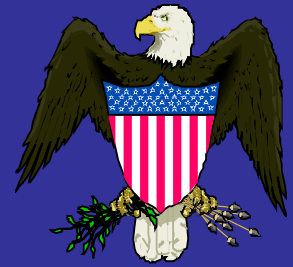
- Up-to-date facts explaining that there is “**probable cause**” to believe that the search warrant will likely elicit evidence of a crime or contraband;
- Identification of the precise location of the search;
- Identification of the particular items or types of items to be seized;
- Explanation as to why the requested search is necessary; and
- Explanation as to how the seized evidence is relevant to the case and how it might assist the investigators or prosecutors in advancing their case.

# Probable Cause: Scenarios



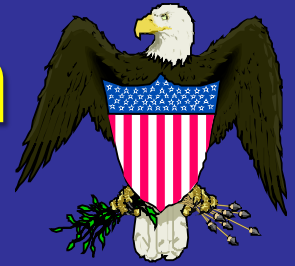
- Link the account to criminal communications
  - E-mails sent from (or to) the account suggesting evidence of a crime?
  - Account controlled by person who reasonably would use it for a crime?
  - Transactional information shows suspicious communications near an important date?
  - Account where bank statements are received?

# Bottom Line



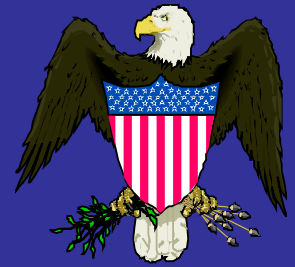
The probable cause standard means that the information necessary to obtain a search warrant in a mutual legal assistance request must be reliable, credible and specific.

# Precluding notification to the customer



- Providers are generally free to tell their customers that you've hit them a search warrant
- Government can apply for an order under that the provider not notify any person of the existence of the process
- Must show an “adverse result”





***But what happens if I don't  
have probable cause?***

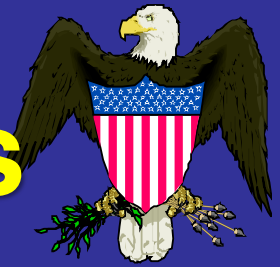
**Ask for a preservation letter.**

# Basic subscriber information available by subpoena



- Generally includes information user provided when creating an account: name, address, means of payment

# Investigation objectives



- Use a subpoena to find out real identity

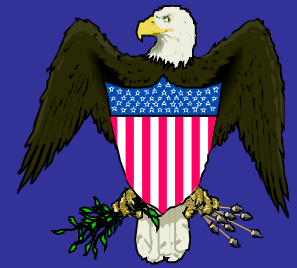
▪ `make.money.fast@yahoo.com`

▪ Real  
identity?

▪ Account  
creation  
information

▪ Subpoena

▪ Access logs with  
IP address



# Part Two: FIU Modernization



# Bank Secrecy Act (BSA) Forms

1. SAR – Suspicious Activity Reports (SARS)
2. Currency Transaction Reports (CTRS)
  - Involving \$10,000+
3. Form 8300
  - \$10,000 cash payment received by persons in trade or business.
4. Currency and Monetary Instrument Report (CMIR)
  - Transporting \$10,000+ at the border

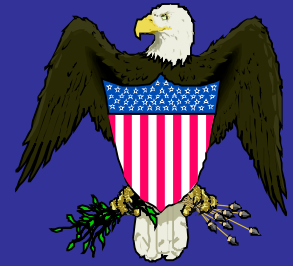
# FinCEN's IT Modernization Efforts

In May 2010, FinCEN began efforts to modernize its information technology (IT) infrastructure to improve the collection, analysis, and sharing of FinCEN data.

# What is E-Filing?

- The Bank Secrecy Act Electronic Filing System (BSA E-Filing) supports the electronic filing of FinCEN reports through a secure network. It also allows users to send and receive secure messages to and from FinCEN. Additionally, FinCEN uses the system to issue advisories and system updates to the user community.

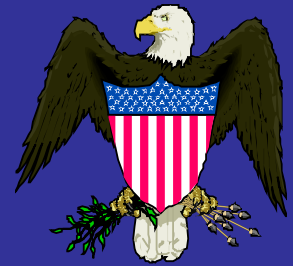
# CTRs and SARs: What's new?



- Beginning April 1, 2013, the new FinCEN reports must be used.
- Reports may not be submitted in paper format.
- It has new fields to provide law enforcement with additional information and support.
- The BSA E-Filing System will not accept filings when critical fields are left blank.



# CTRS AND SARS: WHAT'S NEW?



The new FinCEN CTR allows filer to specify the role of a person in the transaction.

Currency Transaction Report

Home Step 1. Person Information Step 2. Amount and Type of Transaction Step 3. Financial Institution Information

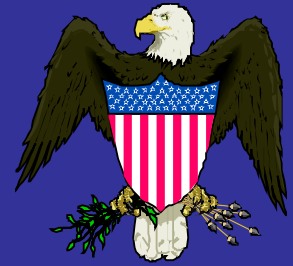
Part I Person Involved in Transaction 1 of 1

\*2 a ☐ Person conducting transaction on own behalf b ☐ Person conducting transaction for another c ☐ Person on whose behalf transaction was conducted d ☐ Courier Service (private)

3 ☐ Multiple transactions



# CTRS AND SARS: WHAT'S NEW?

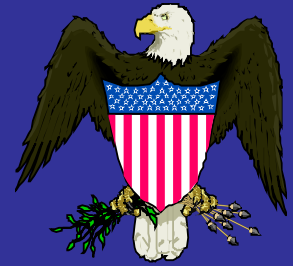


The new FinCEN SARS allows the financial institution to identify a transaction as “suspected public/private corruption (domestic)” or “suspected public/private corruption (foreign).”

# FinCEN Query

- What is FinCEN Query?
  - FinCEN Query is the new search application for authorized users to access FinCEN data.
  - FinCEN Query is designed using a search engine, similar to Google.
  - It allows users to search broadly across more fields and returns more results
  - Sorts data by date, identifiers, bank, regulator, state, type of transaction, etc.

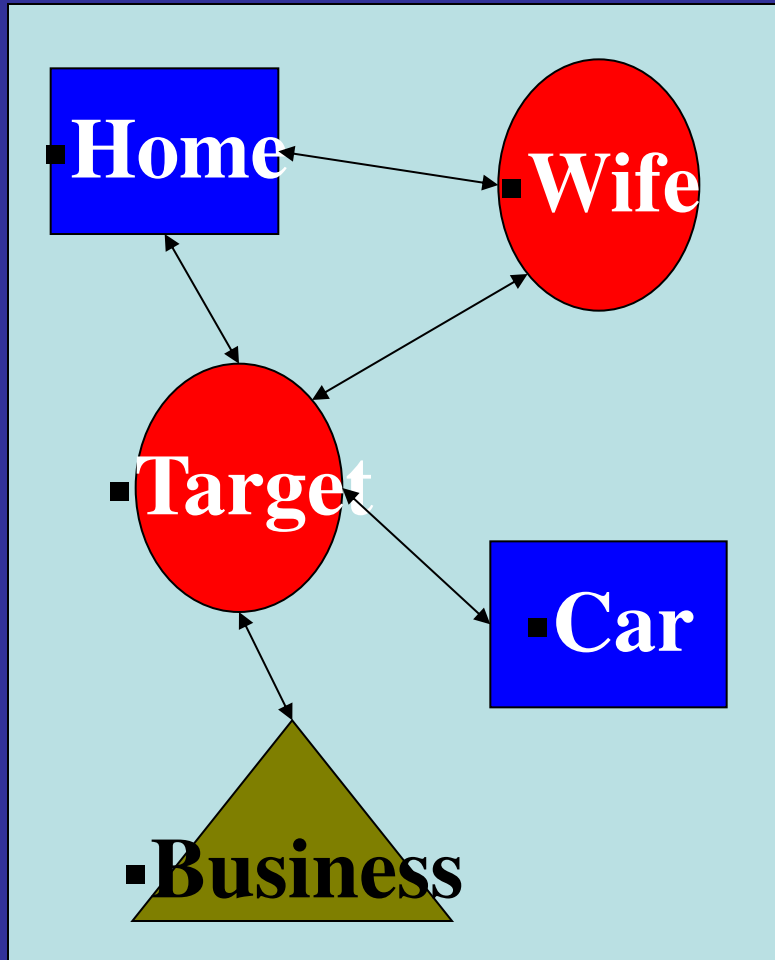
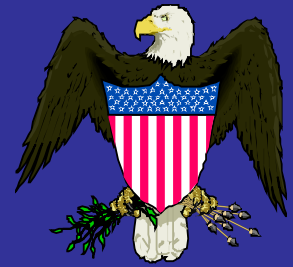
# What do we do with Financial Intelligence?



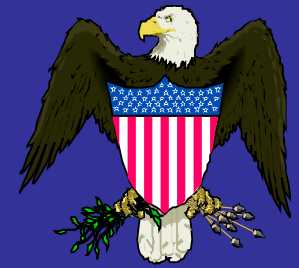
- Link Analysis
  - Software that integrates with FIU data
  - Used by FBI and other law enforcement
  - Several versions, for example –
    - IBM i2 Intelligence Analysis
    - Palantir

AND MOST IMPORTANTLY, we use it to collect evidence via subpoena and search warrant.

# Link Analysis



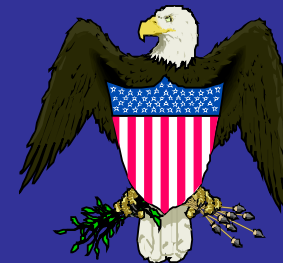
Graphically illustrates interrelationships among individuals, assets, and organizations



# Take away:

- With a showing of probable cause, the United States can obtain email account information from public internet service providers.
- Ask the United States and each other for financial intelligence.
- Use the information you receive to send mutual legal assistance requests and conduct link analyses.





# Questions or Comments?

Elizabeth Aloï  
Trial Attorney  
Asset Forfeiture & Money  
Laundering Section  
U.S. Department of Justice  
(202) 598-2525  
[elizabeth.aloi@usdoj.gov](mailto:elizabeth.aloi@usdoj.gov)