

# Leveraging Financial Intelligence

## Unleashing the Power of Cooperative Relationships with Financial Institutions

Kenneth A. Smith

Director, Anti-Money Laundering Risk Executive

Global Anti-Money Laundering and Economic Sanctions,

Bank of America Corporation

July 2011

**Bank of America**





## Background

### Company

- Bank of America is one of the world's largest financial institutions, serving individual consumers, small and middle market businesses, and large corporations with a full range of banking, investing, asset management and other financial and risk management products and services.
- In the United States, Bank of America serves approximately **57 million** consumer and small business relationships with more than **5,900** retail banking offices, nearly **18,000** Automated Teller Machines (ATMs) and online and mobile banking services with **29 million** active users. Bank of America is among the world's leading wealth management companies and is a global leader in corporate and investment banking and trading across a broad range of asset classes serving corporations, governments, institutions and individuals around the world.
- Bank of America serves clients in more than **150 countries**.



## Unleashing the Power: The Value of Financial Intelligence

- Law Enforcement and Intelligence Services have come to learn the value of financial intelligence (FININT).
  1. FININT is extremely reliable.
  2. FININT leaves a footprint or a trail.
  3. FININT establishes connections and defines networks
- The Bank Secrecy Act and the Patriot Act allow for appropriate information sharing between Financial Institutions and Law Enforcement in the United States. Remarkably similar requirements across the globe require the reporting of financial intelligence to government agencies for the purpose of making such intelligence available to law enforcement.
- Regulations have defined the information that must carry with a financial transaction; or, be gathered at the opening of a bank or investment account.

# Unleashing the Power: Two buckets of valuable information

## Typical FININT Information

- Customer Name
- Customer Address
- Customer ID Number (*e.g.*, Passport, SSN, National ID Number, etc.)
- Customer Date of Birth
- Customer's Residence (if different from Account Address)
- Customer's Stated Source of Income / Wealth
- Customer's Accounts
- Customer's Transactions (*e.g.*, deposits, payments, wires, ACH)

## Atypical FININT Information

- Customer Phone Number, including phone number utilized to access accounts or call centers
- IP Addresses and associated locations where access Customer's on-line accounts occurred
- Time, Date and Location of access to customer accounts through mobile device
- Names of other customers utilizing same phone numbers, addresses, etc.
- Identifying information from other devices accessing accounts
- Photograph identification and location for Banking Center and ATM transactions

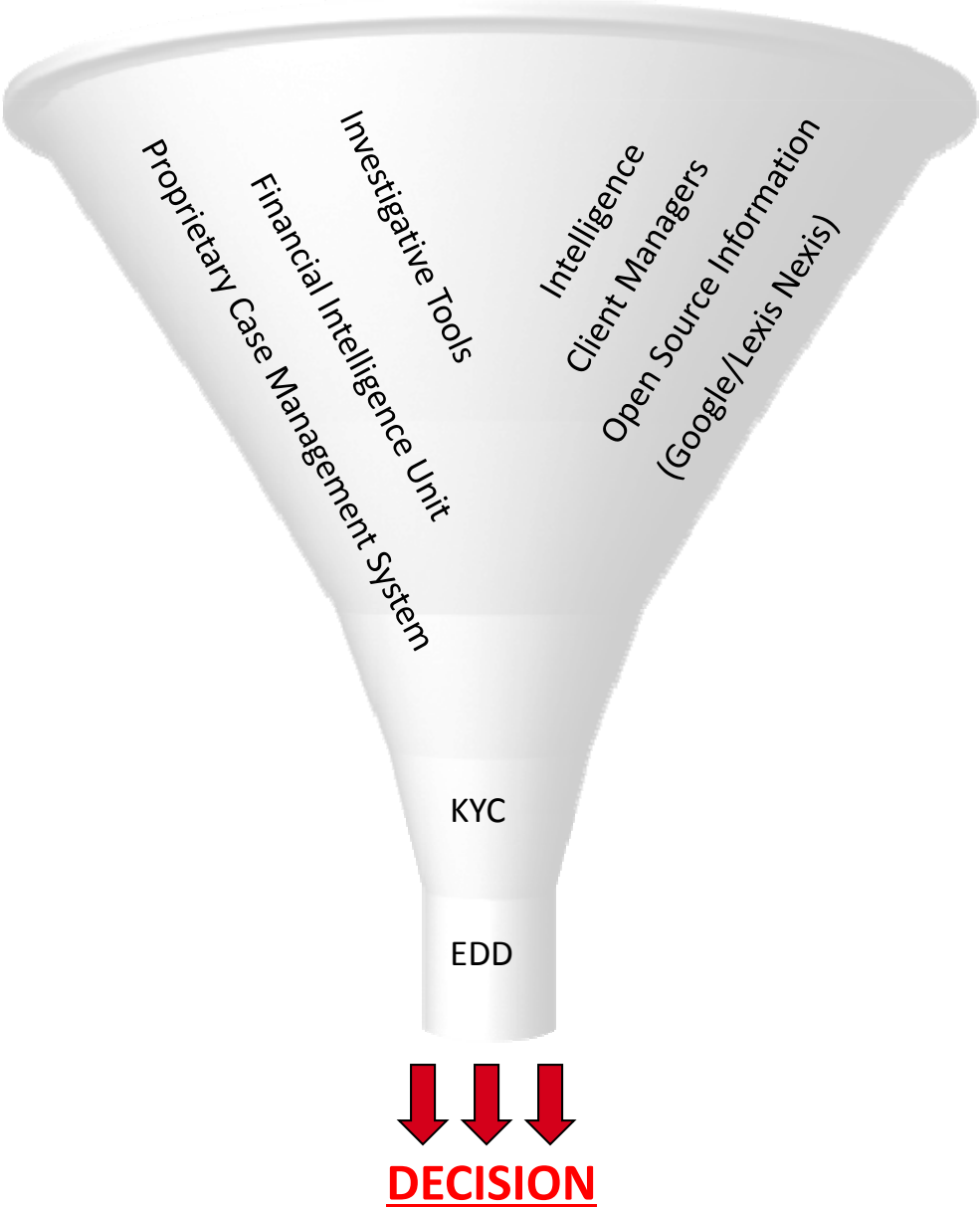
## The Challenge-Where is the Good Stuff?

- Millions of transactions per month
  - Consumer and Small Business Accounts
  - Commercial Accounts
  - Investment accounts
  - Mortgage accounts
  - Credit Card transactions
- 175,000-185,000 Currency Transaction Reports per month
- 2,000-2,500 AML referrals of unusual activity from branch personnel per month
- Bank of America sees approximately eight million wire transactions per month (over 16 trillion dollars)
- OLB Data (IP Addresses/Cookies) and Telephone Numbers

# Suspicious Event Detector



# AML Investigations-Decisioning



# Unleashing the Power: Two buckets of valuable information

## Typical FININT Information

- Customer Name
- Customer Address
- Customer ID Number (*e.g.*, Passport, SSN, National ID Number, etc.)
- Customer Date of Birth
- Customer's Residence (if different from Account Address)
- Customer's Stated Source of Income / Wealth
- Customer's Accounts
- Customer's Transactions (*e.g.*, deposits, payments, wires, ACH)

## Atypical FININT Information

- Customer Phone Number, including phone number utilized to access accounts or call centers
- IP Addresses and associated locations where access Customer's on-line accounts occurred
- Time, Date and Location of access to customer accounts through mobile device
- Names of other customers utilizing same phone numbers, addresses, etc.
- Identifying information from other devices accessing accounts
- Photograph identification and location for Banking Center and ATM transactions



# Unleashing the Power: Case Study



Suspect 1 uses OLB  
from the US and Saudi

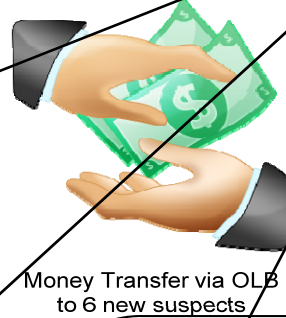



  
IP: 173.129.119.155  
Connection by IP address and Cookie

Suspect 2 uses OLB  
From the US only



Suspect 3  
Does not use OLB



Suspect 4 uses OLB  
From the US only



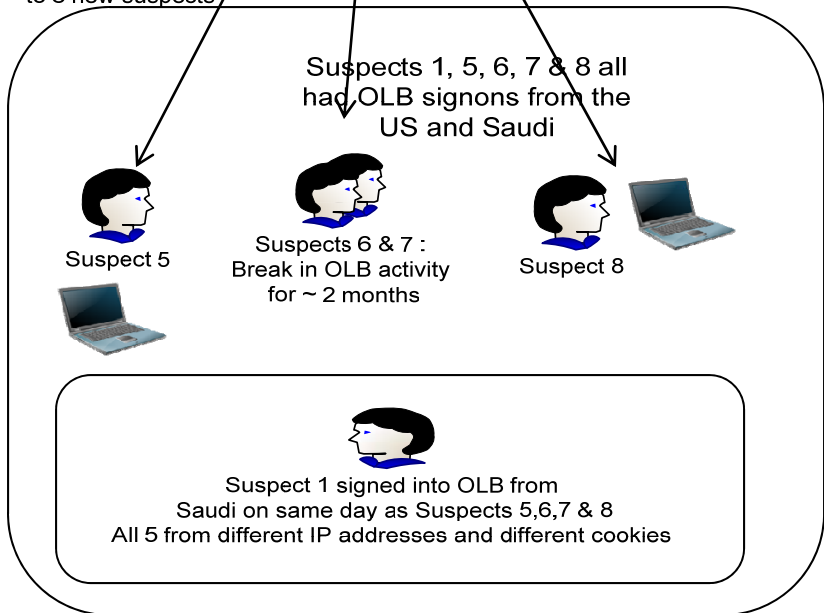
Suspects 1, 5, 6, 7 & 8 all  
had OLB signons from the  
US and Saudi

Suspect 5

Suspects 6 & 7 :  
Break in OLB activity  
for ~ 2 months

Suspect 8

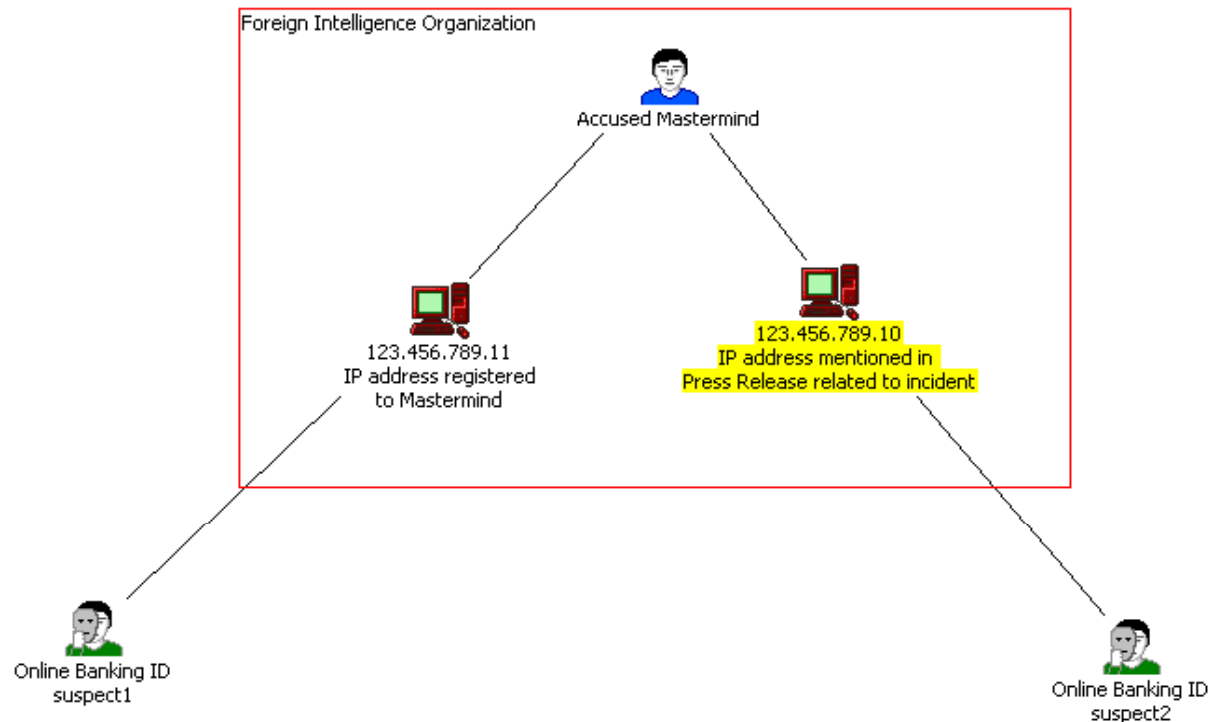
Suspect 1 signed into OLB from  
Saudi on same day as Suspects 5,6,7 & 8  
All 5 from different IP addresses and different cookies





# Unleashing the Power: Case Study

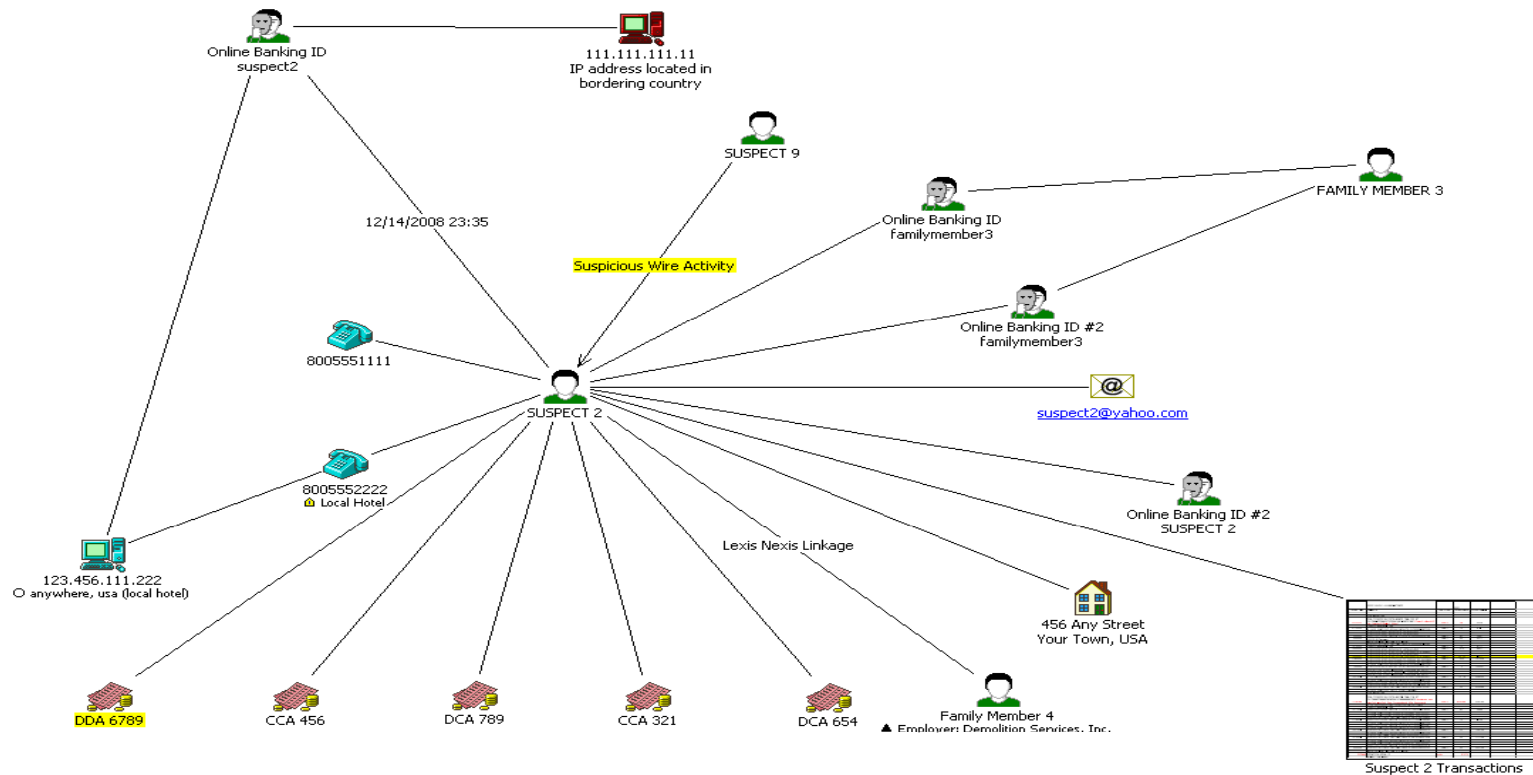
- Two “hits” on IP addresses registered to accused mastermind: Online Banking IDs belonging to Suspects #1 and #2.



- Suspect #2’s logons originated from the IP (123.456.789.10) listed in an open-source report as the source of the email claiming responsibility for terrorist attacks.
- IP’s are registered to an individual known to be associated with a foreign intelligence agency. This information was obtained via open-source research and WHOIS lookups.

# Unleashing the Power: Case Study

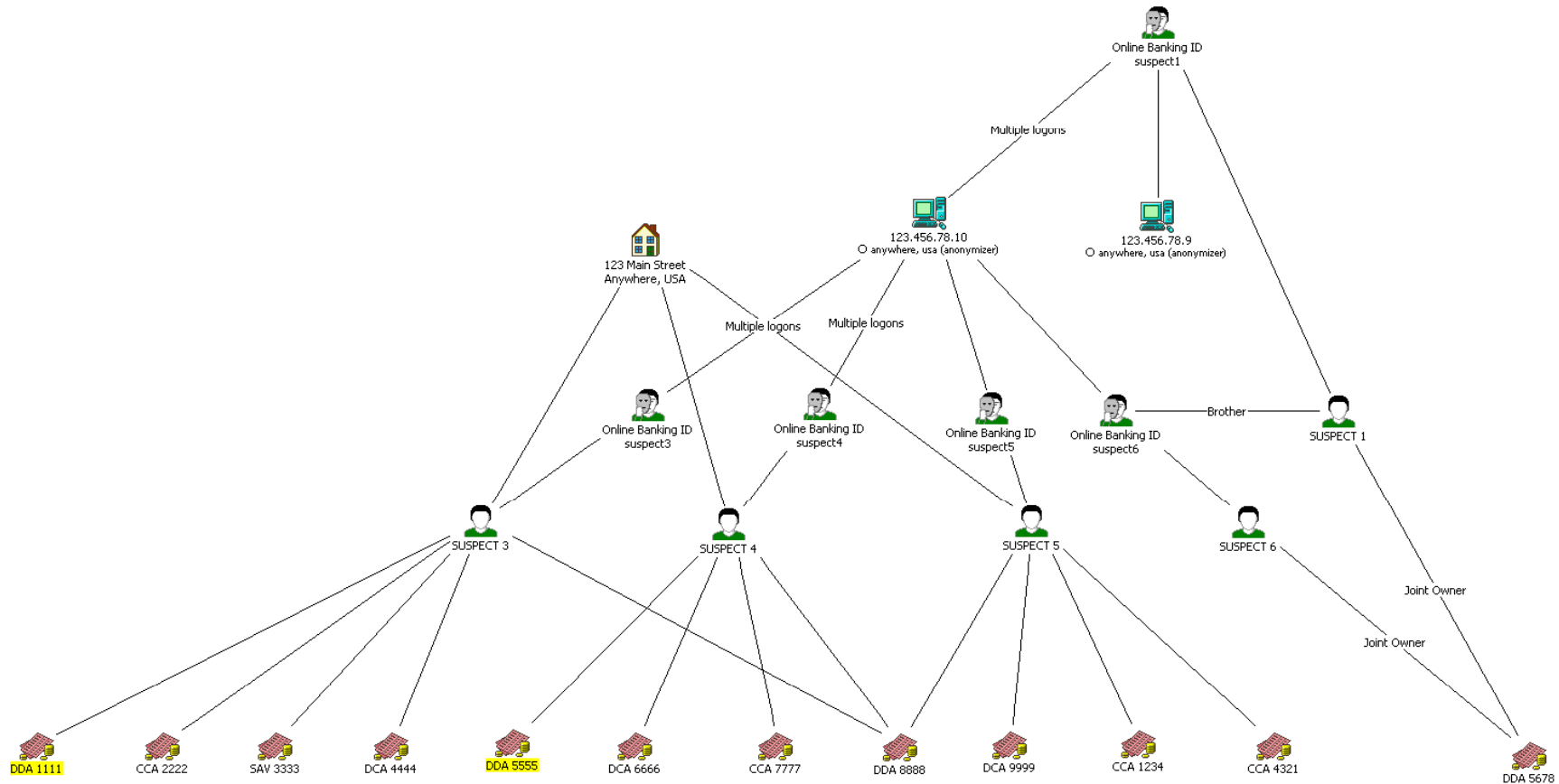
- Suspect #2 had two credit cards, two debit cards and one checking account. A review of account activity revealed suspicious transactions including debits negotiated at the ABC Hotel, near site of attacks.



- Suspect #2 had two Online Banking IDs for himself and two for his wife (Family Member #3). One additional ID belonged to another individual living at the same address. Logons originated from locations near the site of attacks, with one logon from bordering country.
- Suspect #2 also received several suspicious large-dollar wires from another individual (Suspect #9).

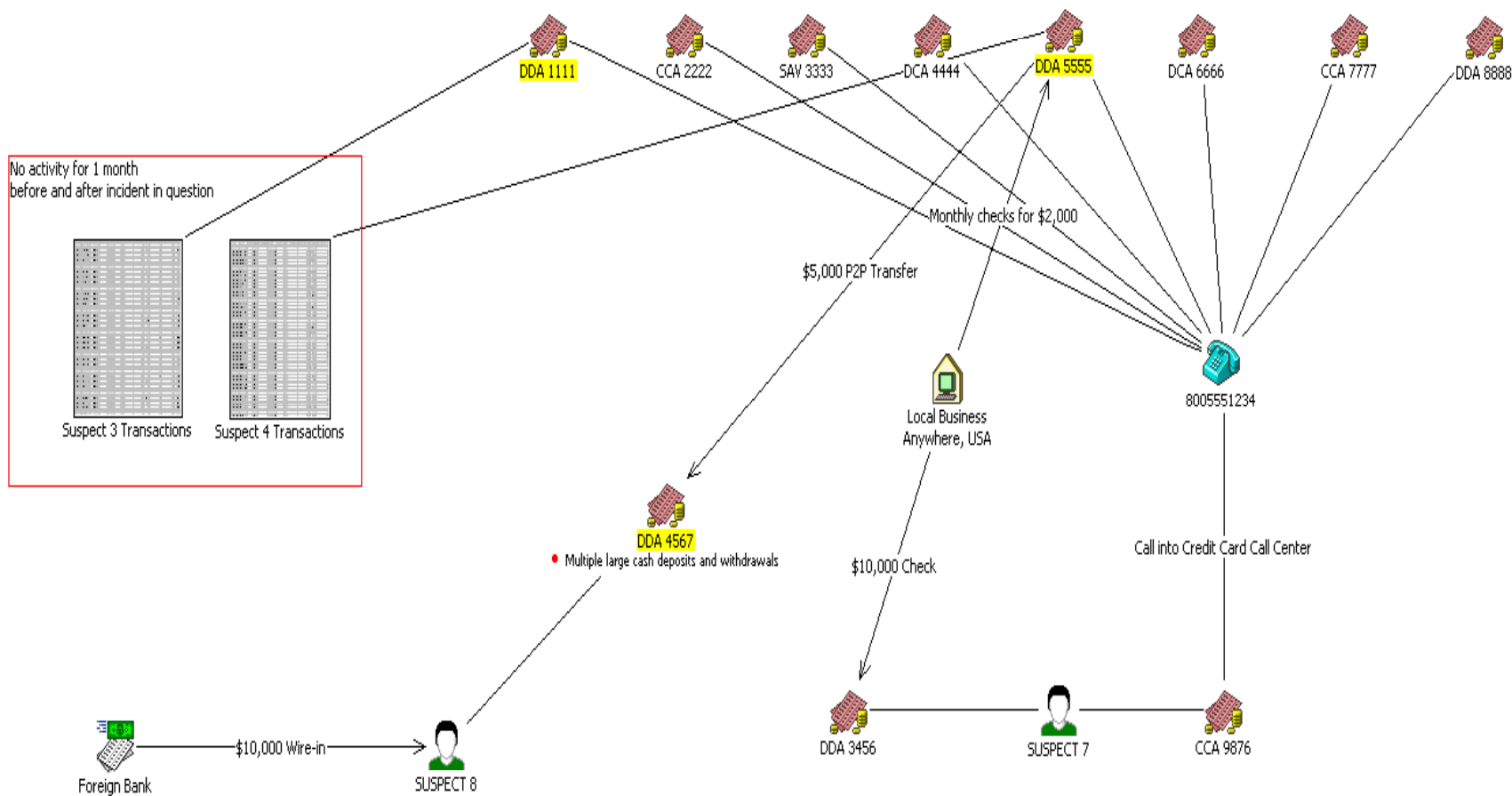
# Unleashing the Power: Case Study

- The IP address commonly used by Suspect #1 revealed additional relationships for investigation: **four Online Banking IDs, four new associates and twelve accounts.**
- Transactional activity on highlighted accounts was suspicious, in that it stopped approximately one month before attacks and resumed one month after.



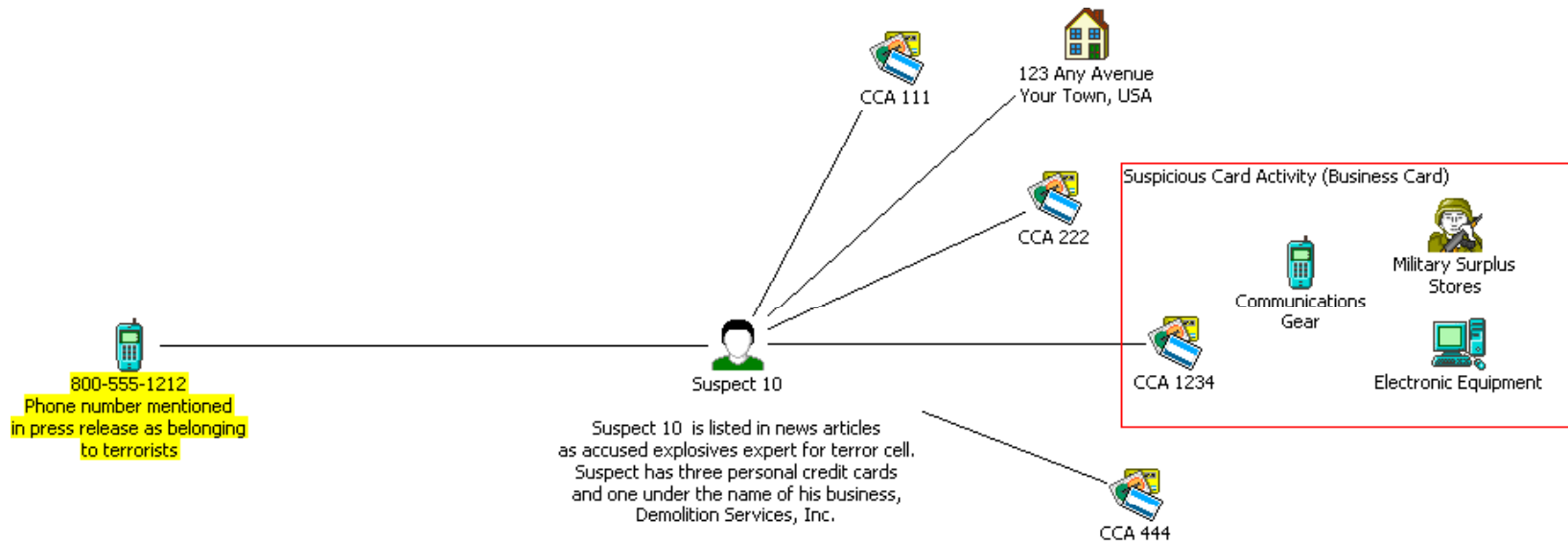
# Unleashing the Power: Case Study

- Transactional research and phone database searches for Suspects #3 and #4 revealed **two new associates** and **three new accounts**.



# Unleashing the Power: Case Study

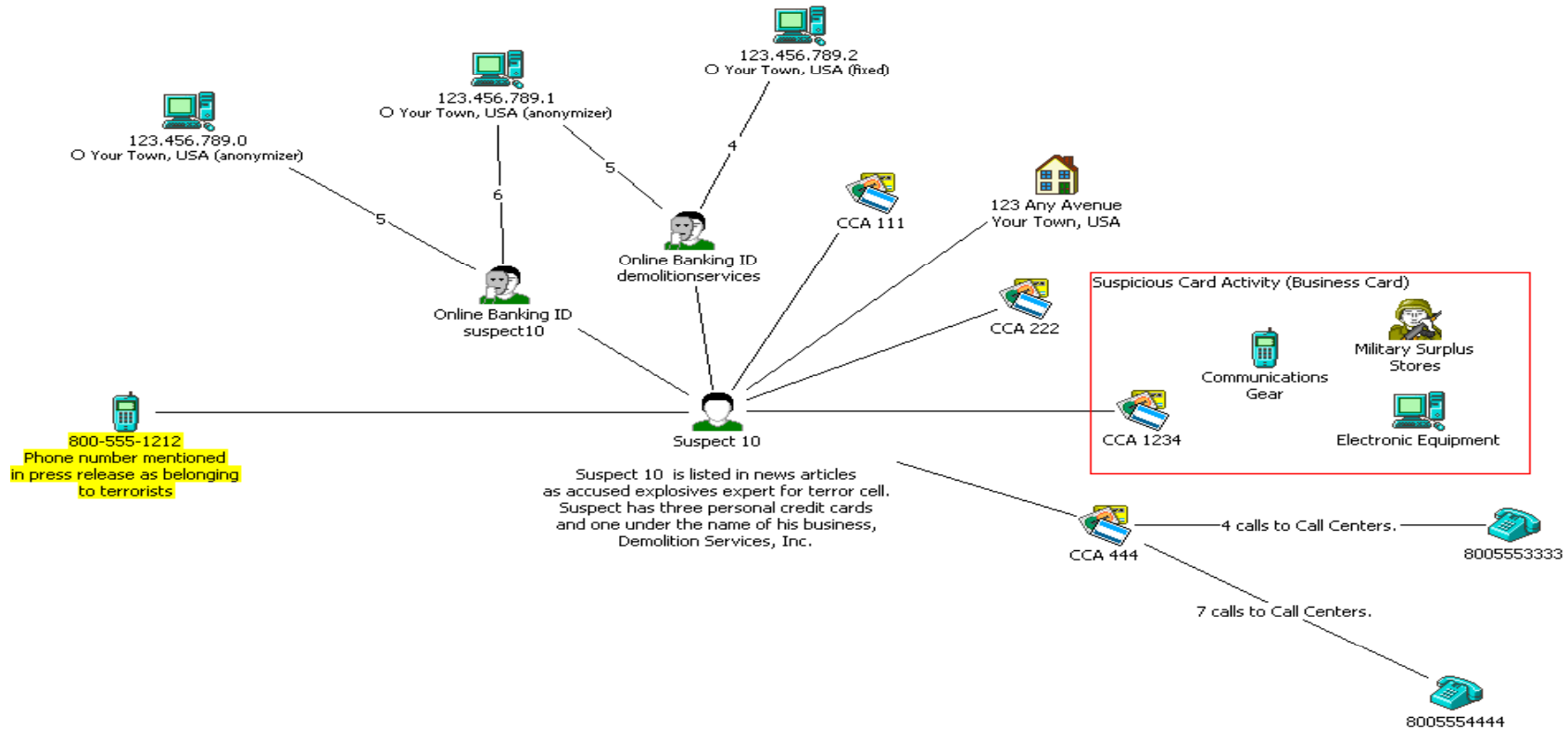
- Suspect #10 used the phone number listed in the open-source report to call and check on his credit card account.



- Suspect #10 had four credit cards with Bank of America; one in the name of his business, Demolition Services, Inc.
- Among the suspicious purchases noted on Suspect #10's credit cards were large-dollar purchases from companies specializing in military surplus, communications gear and electronic equipment.

# Unleashing the Power: Case Study

- Suspect #10 had two Online Banking IDs; one personal and one under the name of his business, Demolition Services, Inc. These IDs were logged onto from three separate IP addresses out of Your Town, USA.



- Additional calls were placed to Call Centers on his accounts from landlines in neighboring states.





## Unleashing the Power: Sharing of Information

- The real power of financial data can be unleashed when the right information can be shared in a timely manner. Financial Institutions should be searching for ways to share data and information in house; between institutions; and with law enforcement.
- Law Enforcement has vast data stores of valuable information directly relevant to the investigation and successful prosecution of financial and other crime.
- Financial Institutions have vast data stores of equally valuable but different information directly relevant to the investigation and successful prosecution of financial and other crime.
- By sharing the **right** data with Financial Institutions, Law Enforcement can protect confidential sources and methods of investigation, while unleashing the power of valuable information housed in the financial institution.



## Contact Information

Ken Smith

[kenneth.a.smith@bankofamerica.com](mailto:kenneth.a.smith@bankofamerica.com)

(980) 386-2797

Law Enforcement Liaison Team

[backupdocs@bankofamerica.com](mailto:backupdocs@bankofamerica.com)

(980) 683-9606