Risk Management:
Integrating AML and Anti-Fraud Efforts

2011 Mid-Atlantic AML Conference

July 26, 2011

Reality Check

- AML and anti-fraud are necessarily intertwined → the financial gain of fraudulent activity ultimately needs to be integrated into the financial system
- In 2008, FinCEN Director James Freis stated: ***"While they are often viewed as separate criminal enterprises, acts of fraud and acts of money laundering are interconnected. Therefore, money laundering is often a malignant and pernicious product of fraud. By fighting fraud, you are fighting money laundering. And in turn, by identifying money laundering, you could be alerting law enforcement to a criminal attempting to mingle the proceeds of fraudulent activity committed against innocent victims – some of whom may do business with your bank."***
- Financial Fraud Enforcement Task Force
- Sharing potential fraud information with AML compliance personnel (analysts/investigators) is critical to compliance with SAR reporting obligations
- Low value SARs may only be the tip of the iceberg

Recent Typologies and Trends – Identity Theft

- FinCEN Report on Identity Theft - Trends, Patterns, and Typologies Reported in SARs (study covered 2003-2009)
- Identity theft sixth most frequently reported characterization of suspicious activity within the period of the study
- 2004 was the first full year in which depository institutions were obliged to report identity theft as a separate suspicious activity characterization on SARs. Since January 1, 2004, the number of SAR filings reporting identity theft has increased by **123%**
- Three main types of fraud facilitated by identity theft:
  - Credit card fraud
  - All types of loan fraud
  - Depository account fraud

Credit Card Fraud

- Most prevalent type of identity theft-facilitated fraud
- Takeovers of existing legitimate credit card accounts and setting up new unauthorized accounts using identifying information of identity theft victims
  - Physical theft of credit cards from mail or person or residence of the victim
  - Skimming of credit card numbers
  - Collection of information online
- Cloned cards
- Credit card fraud was co-reported in about 45.5% of the sample SAR filings
- Reported methods:
  - Attempts to become authorized purchasers
  - Private label cards
  - Accounts opened under business names

Loan & Depository Account Fraud

- Loan Fraud: About 31% of sample SAR filings reported successful and unsuccessful attempts at loan fraud, including fraud related to loans for:
  - Automobiles
  - Mortgages
  - Student loans
  - Other types of consumer loans
  - Significant success in identifying fraudulent loans before they are funded

- Depository Account Fraud:
  - Identity thief opens a new joint account in the name of the victim and him/herself
  - Identity thief then poses as victim and directs that funds be transferred from one or more legitimate existing victim accounts into the new joint account

How was theft discovered?

- For over **27.5%** of filings:
  - Discovered when customers contacted filer to question transactions on existing accounts or to contest ownership of recently established accounts
  - Discovered when customers confirmed identity theft after filers contacted them to question anomalous account transactions
- For nearly **21%** of filings, normal account monitoring uncovered identity theft
- In **14.5%** of filings, searches of commercial databases contributed to discovery of identity theft
- In **10.5%** of filings, filer or customer review of customer credit reports
- In **5%** of filings, a federal, state, or local law enforcement agency reportedly brought identity theft to attention of financial institutions
- In **2.5%** of filings, unexpected call from a bill collector alerted victims to identity theft
- For less than **2%** of filings, credit monitoring services or receipt of an unexpected bill were each responsible for uncovering identity theft

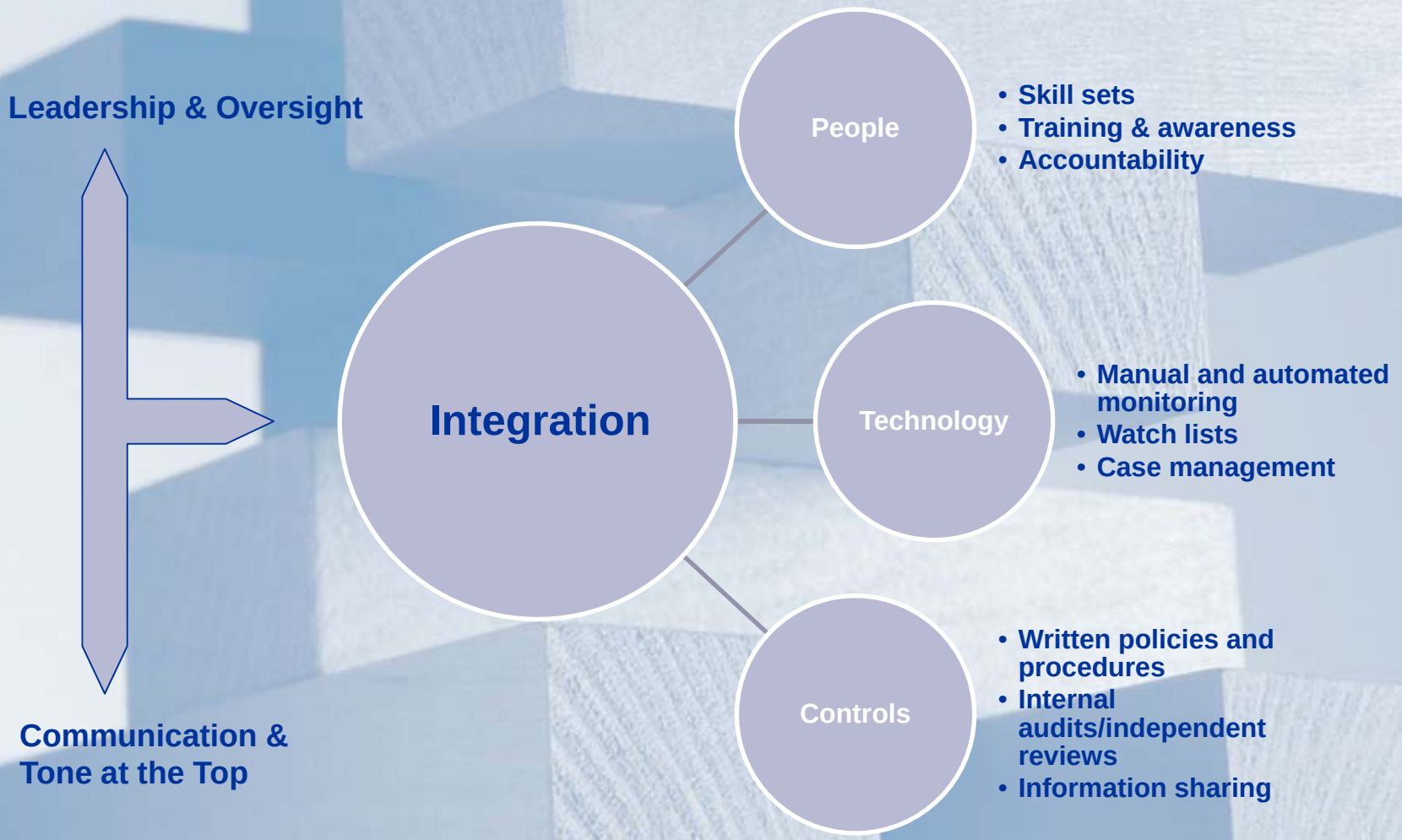
Red Flags

- Two most common:
  - "The financial institution or creditor is notified by a customer, victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft"
  - "The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account"
- Other red flags reported included:
  - "Social Security number provided on application is assigned to individual other than the applicant"
  - "The Social Security number has not been issued, or is listed on the Social Security Administration's Death Master File"
  - "Shortly following the notice of change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account"
  - "The customer fails to make the first payment or makes an initial payment but no subsequent payments"

Integrating AML & Anti-Fraud Efforts - Challenges

- Culture - anti-fraud and AML departments typically think differently
- Fraud and AML investigators independently investigate the same cases
- SAR filing responsibilities are segregated
- Data disparities
- Separate systems, red flags and watch lists
- Centralized versus decentralized functions
- Path to integration can be costly, particularly for large institutions
- Specialized skill sets require cross-training
- Different backgrounds (e.g., former bankers versus former law enforcement)
- Fear of creating more inefficiencies when resources are scarce

Integration Approach



Leading Practice Solutions

- Integrated risk assessment, CIP, monitoring
- Leverage KYC from other business units
- Required communication between AML and Fraud departments
- Cross-training and awareness
- Integrated internal audits
- Quality assurance procedures around non-AML SARs
- Shared case management platform
- File for attempted transactions
- Take advantage of 314(b) information sharing program
- Shared meetings and participation in committees
- Commitment and support from senior management
- Long-term view: successful integration won't happen overnight!

Presenter's Contact Details:

Edwige Sacco, Director

Forensic Advisory Services

KPMG LLP

Mobile: (703) 855-0803

Email: esacco@kpmg.com

KPMG website: www.kpmg.com

LinkedIn: http://www.linkedin.com/in/edwigesacco