



16th Annual

Anti-Money Laundering Audit & Compliance Forum

VOLUME 1, ISSUE 8 AUGUST 2006 WWW.AMLAC.COM

[AMLAC Featured White Papers/Articles](#)

[Recent and notable news briefs](#)

[AML Glossary](#)

[Register](#)

IIR would like to thank its event sponsors for AMLAC 2006:



Welcome to the AMLAC Update!

While a few interesting money laundering cases and indictments occurred in July (please see the news briefs below), the story with the greatest impact on AML officers was the July 28th release of the Federal Financial Institutions Examination Council's (FFIEC) Revised Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual.

The revisions to the manual further clarify supervisory expectations and incorporate regulatory changes since the manual's initial release in 2005, and also incorporate feedback from the banking industry and bank examiners. Some of the significant changes and updates include the following:

- A new enhanced discussion on risk assessment processes designed to provide more guidance on evaluating and developing a BSA/AML risk assessment
- The inclusion of a new section on Automated Clearing House (ACH) transactions, including relevant parallel updates to the OFAC section addressing ACH activity
- Revisions to the section on Trade Finance Activities covering related examination procedures and including more guidance on trade finance from industry and subject matter experts
- New updates on changes in regulations and supervisory guidance covering the following sections in the manual: Suspicious Activity Reporting, Foreign Correspondent Account Recordkeeping and Due Diligence, Private Banking Due Diligence Program, Insurance, and Politically Exposed Persons
- The addition of information related to emerging money laundering threats taken away from the US Money Laundering Threat Assessment relating to nominee incorporation services and stored value cards
- Stylistic and organizational changes of the manual to make it user more user friendly, including the merging of the overview with the procedures sections, as well as adding more distinctive headings

According to the FFIEC's press release, teleconference calls will be scheduled in September with FinCEN and the other agencies which co-authored the changes. You can download the 2006 version of the manual at

http://www.ffiec.gov/bsa_aml_infobase/default.htm



Are you looking for increased year-round exposure to the senior AML regulators and executives at financial institutions? Why not consider sponsoring or exhibiting at AMLAC 2006? For sponsorship opportunities, please contact Andrew Borowiec at aborowiec@iirusa.com.

IIR would like thank its event exhibitors:



If you'd like to exhibit at AMLAC, please contact Jeffrey Dubs at jdubs@iirusa.com.

New to AML? Check out our online AML Glossary to get up to speed on AML terms and concepts at www.amlac.com.

New Additions to the White Paper and Articles Archives

Please enjoy the latest additions to our White Paper and Articles Archive, which can be found [here](#). This month, we've included a White Paper published by AMLAC Forum speaker **Patricia Potts, Data Framework Program, Transaction Data Warehouse Manager, WACHOVIA CAPITAL MARKETS**, and an article by counterterrorism expert **Dennis Lormel, Sr. VP, CORPORATE RISK INTERNATIONAL** and AMLAC Forum speaker. We've also included a White Paper on KYC procedures from AMLAC Forum sponsor **DAYLIGHT FORENSIC**.

Finally, we issued a revision to our **2006 AMLAC Forum Brochure**, which can be downloaded [here](#). The revised PDF includes content updates, revisions to the networking lunch roundtables, and additional speaker and sponsor information.

Until next month,

Keith Kirkpatrick
Executive Director and Editor in Chief
16th Annual AMLAC Forum

Subscribe Today for the AMLAC Update!

Mark Your Calendar! Be sure to attend the 2006 AMLAC Forum Cocktail Reception, sponsored by

Tuesday, September 19, 2006, 6:00 PM

Agenda-at-a-Glance

<i>Pre-Conference Workshop</i>	<i>Main Conference</i>		<i>Post-Conference Workshop</i>
DESIGNING AN EFFECTIVE AML PROGRAM	DAY ONE	DAY TWO	COMBATING THE FINANCING OF TERRORISM
<i>Monday, September 18</i>	<i>Tuesday, September</i>	<i>Wednesday,</i>	<i>Thursday, September</i>

	19	September 20	21	
Part I: Developing an Effective Risk-Based Compliance Program	Regulatory Updates: Understanding the Latest Threats, Regulations, and Enforcement Strategies	Managing Compliance with Your Customer Identification Programs by Applying the Latest Know Your Customer Techniques	The Importance of CFT	
	Analyzing Section 312 Compliance Issues for Correspondent Banks	Best Practices for Knowing When to File Suspicious Activity Reports	Overview of Terrorism	
	Overcoming the Challenges of Complying with Private Banking Operations Under Section 312	CASE STUDIES: Discussing Investigations and Criminal Prosecutions with Law Enforcement Officers	Terrorist Financing Methodologies	
	AML Regulations and Controls - An Outlook on the State of the Industry	Compliance Issues for Insurance Companies	The Proposed AML Rules for Hedge Funds	Key Indicators of Potential Terrorist Financing
Part II: Procedures and Best Practices for Preparing for Examinations Under the FFIEC AML Examination Manual Guidelines	Implementing Best Practices for Handling Your Annual AML Program Audit	AML Regulations with High-Risk Businesses	Working a SAR from Beginning to End	Research Tools & Methodologies for the CFT Investigator
	The Challenges of Global Compliance Across Multinational Jurisdictions	Effective Transaction Monitoring and Reporting Systems	How MSBs are Mitigating Money Laundering Risks	
	Latin America and the Caribbean	The Middle East	Managing Section 312 and OFAC Compliance Issues for Brokers/Dealers, Clearing Firms, Mutual Funds, and Other Institutional Businesses	Case Studies and Examples
	Europe	Additional Money Laundering Case Studies		Integrating CFT Components into your AML Program

AMLAC Featured White Papers/Articles

How to Assure Good Value from Your Investments in AML Technology

By Patricia Potts, Data Framework Program, Transaction Data Warehouse Manager, **WACHOVIA CAPITAL MARKETS**

What is it that makes a solution of good value? Is the value of a solution based on the longevity of its existence? Is the value based on the overall bottom line - return on investment? Good value comes in

many formats, and often times it plays hopscotch into all of these mentioned arenas.

Given the current Compliance climate, Anti-money Laundering is a "hot-spot" for the financial services industry. AML Technology programs within organizations are under the microscope from regulators, shareholders, and associates alike as to whether there is value in the chosen path. There are currently more questions today than there are answers - more obstacles than there are solutions. Can both the questions and obstacles in front of us be turned into value add answers and solutions? My answer to both is "yes".

Click [here](#) to read the full white paper.

Continued Debate over the SWIFT Disclosure by the New York Times

By Dennis M. Lormel, *Senior Vice President*, **CORPORATE RISK INTERNATIONAL**

Following the New York Times article disclosing the U.S. Government's SWIFT monitoring program, the Bush Administration harshly criticized the Times for publishing the article when the Government requested the story be withheld. The Times was strongly taken to task for disrupting and diminishing an important investigative tool. In response, a number of critics have argued that the Government made numerous previous disclosures about tracking and monitoring the financial activity of terrorists. Because of such disclosures, critics reason that the Times article caused minimal damage because terrorists knew that the Government monitored the formal financial system, and therefore, terrorists moved to the informal financial system or alternate remittance system such as the hawala network. This argument is overly simplistic, one-dimensional and flawed. Terrorist financing is complex and multi-dimensional.

In a one-dimensional context, the position of those that the Times SWIFT disclosure was not harmful to Government operations has an element of accuracy from a theoretical standpoint. Theoretically, it's reasonable to assume that terrorists responded to Government reports about financial monitoring and tracking initiatives by avoiding the formal financial system and moving their activities to the informal system. In actuality, an element of terrorists and their supporters did move to alternate financial channels; however, many more elements did not change their financial practices for a multitude of reasons, a few of which are addressed below. One essential ingredient of a successful terrorist organization is funding.

Terrorist groups require financial support in order to achieve their goals. They must have effective financial infrastructures to include: sources of funding, the means of laundering funds, and the availability of funding. These factors necessitate use of the formal financial system. It should be noted that terrorist organizations have had many years to perfect their methodologies.

Many elements of terrorists and their supporters have no choice but to operate in the formal financial system. This is attributable to factors to include business considerations, fundraising activities, operational requirements, financial conduits, investments and other factors. The Times SWIFT disclosure will spur many individuals and entities in this dimension to better insulate themselves from U.S. Government detection and tracking. The 9/11 Commission Monograph on Terrorist Financing discussed the challenge confronted by the Government in establishing financial links to terrorists and developing compelling evidence against them. There are numerous high profile individuals and entities who have been linked to terrorism but who continue to operate undeterred because compelling evidence is lacking. The Times SWIFT story will certainly cause those identifiable with this element to develop methodologies that better insulate them. This will create greater challenges for investigators.

Another element of terrorists and their supporters believe that in spite of Government financial tracking and scrutiny as long as they operate with a sense of anonymity and without causing suspicion they will avoid detection. In that context they are right, when considering the totality of daily financial transactions. This element has been expert at operating by moving smaller and non-descript amounts of funds and commodities that avoid suspicion. These operatives did not consider the operational proactive tracking mechanisms articulated by the Times. The Times disclosure will likely change that mind set with realization that intelligence information was used for financial tracking. This will cause terrorists and their supporters to adapt new financial methodologies, seek to exploit new areas of

vulnerability in the financial system, or to use informal financial mechanisms to a greater extent.

Returning to the simple argument, one of its flaws was resonant in the Times article itself. The Times article mentioned select operational investigative SWIFT program successes, to include the capture of Jamaah Islamiah leader Hambali. How could that happen if terrorists had stopped using the formal financial system because of Government disclosures of financial tracking mechanisms? Another factor is that many of the skeptics lack operational familiarity with the SWIFT program and do not understand its operational capability or more importantly its continuous operational success up until publication of the Times article.

In taking the argument out of the realm of the theoretical and into the operational, and coupling it with specific and not generic factors, one can better identify the multi-dimensional considerations that should be factored into the debate. The reality is the Times SWIFT disclosure has been harmful. At a minimum, it has disrupted an innovative and productive investigative tool. One fact is certain... the disclosure has received intense media coverage and has caused terrorists and their supporters to sit up and take notice. This will cause terrorist operational changes and significant new challenges for the Government in identifying and countering evolving terrorist financing methodologies.

Mitigating Customer Risk: Important Considerations When Implementing a Know Your Customer ("KYC") Remediation Project

By Scott Moritz, Ana Alonso and Kevin Caulfield, **DAYLIGHT FORENSIC**

I. Introduction

Section 326 of the USA PATRIOT Act requires financial institutions to have a Customer Identification Program ("CIP") to verify customer identification in connection with the opening of accounts and to apply a "risk based approach" when seeking to verify customer-provided information. Increasingly, U.S. and foreign financial services regulators have been meting out severe penalties for deficiencies related to customer identification, risk scoring and enhanced due diligence. Many of these regulatory actions required institutions to "remediate" their customer identification files to ensure adherence with the bank's CIP and Section 326. While it has been a requirement since October 1, 2003, many financial institutions still struggle with Customer Identification, Risk Scoring and Enhanced Due Diligence. To make matters worse, those that have insufficient CIP programs are frequently compelled to implement far reaching KYC remediation programs, sometimes across their entire customer base, under a compressed timetable.

This article discusses the critical success factors and potential pitfalls that financial institutions face when planning for the assessment and remediation of customer identification files. At a high level, the most frequent challenges include organizational barriers, customer frustrations, lack of an appropriate strategy, poor project coordination and inconsistent application of the Bank's policies and procedures governing CIP. In particular, this article analyzes the opposition received from both the bank's own relationship managers and from the customers themselves when contacting them for information or missing documentation. This analysis also provides some methods and tools to overcome such opposition significantly increasing the likelihood of success of the remediation project. [CLICK HERE](#) to read the full article.

Do you have a White Paper on AML you'd like to share? Send it to Keith Kirkpatrick, Editor, *AMLAC Update*, for inclusion in the next AMLAC Newsletter, at kkirkpatrick@iirusa.com .

RECENT NEWS BRIEFS

July 31, 2006 -- According to a July 31 report published by *Diamond Intelligence Briefs Online*, an Atlanta-area jeweler was indicted by a federal grand jury for his role in a money laundering scheme that allegedly funneled illegal drug profits through his two jewelry stores in the Atlanta area. Toros Seher's jewelry stores, "Chaplin's" and "Chaplin's Midtown," were allegedly used to launder cash drug proceeds, at many times exceeding US \$10,000, \$20,000, and even \$30,000 in single transactions. An undercover investigation found that Seher allegedly didn't report these large cash transactions,

knew that the jewelry sales were being used to launder the money from criminal activity, and intentionally failed to file the required CTR forms. Seher could face up to 20 years imprisonment on each of the four counts of money laundering or conspiracy to launder money, as well as up to 5 years imprisonment on each count of failing to file a required form required for large cash transactions.

July 28, 2006 -- A six-month undercover investigation yielded the indictments of two New York men for running a multimillion-dollar money laundering scheme and illegally transmitting funds, according to a July 28, 2006 *Associated Press* report. The report stated that Arthur Budovsky and Vladimir Kats received and illegally transmitted at least \$30 million through their company, Goldage, between January and June 2006, and sometimes charged six-figure fees to launder the money. Each of the men were charged with engaging in the business of transmitting money without a license, a felony violation of state banking law.