Financial Services and E-Commerce

The Undue Burdens of the Bank Secrecy Act

*By James M. Rockett**

The USA PATRIOT Act[1] was enacted into law in late-October 2001, less than 45 days after the horrifying events of 9/11. There was virtually no debate on the USA PATRIOT Act since during the majority of that time Congress itself was out of session due to the anthrax scare during much of the period following 9/11. Title III[2] of the USA PATRIOT Act was, in essence, a wholesale importation of the "Know Your Customer" regulation that had been proposed prior to 9/11, and which had provoked vigorous criticism. The Know Your Customer proposal had inflamed the American public resulting in more than 300,000 comments condemning the proposal as an excessive governmental intrusion into the daily financial affairs of the public. But, following 9/11 we entered a new era and Americans were prepared to sacrifice many aspects of what had been our daily lives to prevent the horrors of another terrorist attack. And Title III of the USA PATRIOT Act was enacted based on that premise; In essence, Congress told us that if banks had just watched the flow of dollars we could have prevented the events of 9/11.[3] Based on the evidence available now, this was and remains cynically disingenuous.

Lack of Balance in BSA

Title III of the USA PATRIOT Act has imposed extraordinary burdens on the banking system without any evidence that it has worked or will work to detect or deter terrorism.[4] The burdens created by Title III and the current Bank Secrecy Act[5] (BSA)/Anti-Money Laundering (AML) climate are excessive and should not be tolerated by our free society . As a factual matter, the AML regulatory process is out of balance.

Balance occurs when regulators, seeing minor flaws in compliance, identify these shortcomings in a report of examination and enter into a collaborative process to assist banks in meeting their compliance obligations. Lack of balance occurs:

- Where regulators, as is now the case, immediately proceed into an enforcement action for the slightest compliance flaws.
- When programs that were fully compliant as recently as last exam are now resulting in enforcement actions.
- When banks are automatically put in the penalty box for indeterminate periods and sit frozen with no ability to pursue any strategic growth opportunities, while banking regulators conduct a BSA compliance review.[6]
- When entire classes of customers are deemed high risk and banks must either disengage from these customers or face the likelihood of enforcement actions.
- When a regulator tells the banks it supervises that one failure to file a single Suspicious Activity Report (SAR) will result in a formal enforcement action while taking the position that filing too many SARs indicates that a bank's customer base is either too high risk or its compliance program is seriously defective.
- When the Department of Justice and local district attorneys threaten criminal prosecution for a failure to file a SAR.

Adverse Economic Impact of AML Environment

The consequences of this lack of balance are predictable but need to be examined. First, and most obviously, banks are incurring enormous compliance costs. These are not small amounts of money that can be easily absorbed. Our largest banks are investing tens of millions of dollars each and mid-size and community banks are spending proportionately even more on everything: regulatorily-required technology systems, compliance personnel, training account officers and new account clerks and tellers and loan officers and branch personnel, internal auditors, external consultants, independent auditors, executive management time, directors' time' monitoring accounts and financial transactions by customers; and filing largely meaningless SARs with the government. These monies are being taken from banks and their shareholders, under threat of regulatory enforcement penalties or even criminal prosecution, without any recompense from the government. These are not traditional "costs of doing business" nor are they routine processes of compliance that with time will be regularized. These are law enforcement expenses that should rightfully be borne by the government.

Secondly, and even more importantly, the impact of the Bank Secrecy Act and Title III on the U.S. economy is staggering. This is a fact that has not been examined with any scholarly precision and is probably immeasurable in real dollars. But, cost structures of this magnitude have to be passed on to the users of banking services either directly or indirectly. These costs are also putting U.S. banks in an uncompetitive position in the rapidly globalizing world of financial services.

There is also a significant but unquantifiable loss of foreign investment in the United States. Because of enhanced due diligence on foreign-originated transactions, many foreigners have become increasingly reluctant to do personal business or invest in the United States. This trend is rapidly accelerating and will only be greatly exaggerated by the Treasury Department's proposal to force U.S. financial institutions to collect and turn over data related to cross-border wire transfers.[7] This also comes at a time when the

U.S. economy is most vulnerable and can least afford such a foreign pullback.

However it is not just the American consumer of banking services, or foreign investors, or the banks themselves that are paying the price. An entire industry of money services businesses is being driven out of the banking system and, in most instances, affecting those who can least afford it: the poor migrant and immigrant workers who come to the U.S. to perform labor at low wages and who want to cash a check or send funds back home to their families. Despite the Financial Crimes Enforcement Network (FinCEN) and the bank regulators having protested that they do not intend to create this result, the facts speak for themselves: money transmitters are viewed as "high risk" customers and the enhanced due diligence requirements are so onerous that bankers are faced with the Hobson's choice of either undertaking ongoing monitoring (of not just the bank customer but the customer's customer) at great expense or risking regulatory enforcement action. The only prudent decision is to withdraw from providing banking services to such money transmitters.[8]

But the money transmitters aren't alone in being deemed to be "high risk." In a list that on its face is preposterous, the bank regulators have identified the following "high risk" banking customers:

- Foreign banks
- Money Services Businesses (currency dealers or exchangers, check cashers, money transmitters, and issuers, sellers, or redeemers of travelers' checks, money orders and stored value cards)
- Non-bank financial institutions (casinos (tribal and non-tribal), card clubs, brokers and dealers in securities)
- Senior foreign political figures and their family members and close associates
- Non-resident aliens and accounts of foreign persons
- Foreign corporations with transaction accounts, particularly offshore corporations in high-risk geographies
- Deposit brokers, particularly foreign deposit brokers
- Cash intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATM operators, vending machine operators, and parking garages)
- Non-governmental organizations and charities (domestic and foreign)
- Professional service providers (attorneys, accountants, doctors, real estate brokers)
- Import-export companies
- Jewelry, gem and precious metal dealers
- Travel agencies
- Car, boat and airplane dealerships

With this guidance for "high risk" is there any wonder banks are filing hundreds and thousands of useless SARs which are ignored by the very government that mandates them?[9] Each new SAR builds an even denser haystack in which the needle becomes more imperceptibility embedded. And, if and when a terrorist attack actually takes place, somewhere an ignored SAR will be languishing among the hundreds of thousands of SARs filed because of the current indiscriminate regulatory environment.

Fighting Terrorism or Financial Spying?

This brings us to another question about the whole BSA/AML construct and that is: why has this been sold to the American public in such a disingenuous manner? The American public largely believes the PATRIOT Act was passed under anti-terrorism rubric. In fact, the banking system is not and will never be an effective vehicle to combat terrorist financing. The 9/11 terrorists used approximately $500,000 over a period of several years to finance their horrifying acts. During that time hundreds of trillions of dollars flowed through the banks of this country. There were no characteristics or patterns that would have distinguished the 9/11 terrorists from any other foreign students in the U.S. who received money from home and paid tuition and living expenses with those funds. Nothing that U.S. banks are now being required to do will actually identify terrorists; that job must be done by old-fashioned investigative work by intelligence agencies. And we could certainly craft laws that will allow them access to financial records if they have good cause to suspect terrorist financing is taking place.

What this highlights is what I will call the "equivalency" flaw of the current BSA/AML construct. By this I mean that the laws and regulations and the manner of their enforcement make no distinction between, and basically equate terrorist financing with, maintaining an account for Augusto Pinochet[10] or a common crime, such as check kiting or a Ponzi scheme.[11] It is one thing to say that we are preventing terrorist financing by setting up this elaborate, costly, intrusive bank account spying network; it is quite another to burden our society with a blatantly ineffective regulatory scheme in order to prevent current or former foreign government officials from maintaining U.S. bank accounts. That could be handled much like Office of Financial Asset Control regulations. And to have check kites or Ponzi schemes governed by the same rules is just plain silly.

Finally, the American public has to be told candidly that every financial transaction that they undertake is being monitored for suspicious characteristics and anything that they do that is out of pattern is reported to the government. At a time when financial privacy has become a rallying cry, our citizens should know the truth about the unprecedented government scrutiny of their financial activities by deputizing their banks to indiscriminately spy on them. And this spying

is not limited to "terrorist financing;" it is a general spy network that reports any unusual financial activity to the of abuse inherent in such a scheme.

Back some 30 years ago, a quaint regulation called Reg Q allowed banks to give out toasters to new customers who opened bank accounts. How far we have come? Now, under the guise of the USA PATRIOT Act, the Bank Secrecy Act and the AML regulations, instead of toasters banks are required to give customers the equivalent of ankle bracelets to monitor their every move. This is not progress and should not be viewed as consistent with the freedoms that the U.S. Constitution was established to protect.

* James M. Rockett is a partner of Bingham McCutchen LLP where he co-heads the Financial Institutions Corporate and Regulatory Group. He is the 2005 chair of the California State Bar Financial Institutions Committee and the 2005 recipient of the California Bankers Association Frandzel Award for noteworthy service by an outside counsel to the California banking industry. He is the Immediate Past Chairman of the Federalist Society Financial Services and E-Commerce Practice Group.

Footnotes

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, USA PATRIOT Act of 2001, P.L. 107-56 (2001).

[2] International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, Title III, USA PATRIOT Act of 2001 (2001).

[3] For example, on September 27, 2001 United Press International quoted Senator Paul Sarbanes, then-Chairman of the U.S. Senate Banking Committee as follows: "We meet, of course, in the shadow of the terrorist attacks of September 11. It is more urgent now than ever before for us to develop and put into place the array of tools necessary to trace and interdict the funds on which terrorists like Osama bin Laden rely for their operations."

[4] Senator Norman Coleman, Chairman of the Senate Permanent Investigations Committee, which investigated the Riggs Bank matter, stated during a speech to The Federalist Society on April 26, 2005 at the National Press Club that he was unaware of any evidence that bank compliance with Title III or the Bank Secrecy Act had resulted in identifying any terrorist activities.

[5] The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act, 31 U.S.C. Sections 5311-5330 and 12 U.S.C. Sections 1818(s), 1829(b), and 1951-1959.

[6] The "penalty box" is a phrase currently in common use referring to the fact that USA PATRIOT Act Section 327, which amended the Bank Merger Act (12 U.S.C. Section 1828(c) to require that: "In every case, the responsible agency shall take into consideration the effectiveness of any insured depository institution involved in the proposed merger transaction in combating money laundering activities, including in overseas branches." In general, bank regulators have interpreted this provision to require that they withhold approval of any expansionary application where deficiencies in BSA compliance are believed to exist. The institution so affected is said to be in the "penalty box" where they remain for an indeterminate period, usually a minimum of one year and in many instances more. During this period, the bank's strategic growth opportunities are stifled and the adverse economic impact on the bank can be severe.

[7] On April 10, 2005 the New York Times reported that: "The Bush administration is developing a plan to give the government access to possibly hundreds of millions of international banking records in an effort to trace and deter terrorist financing, even as many bankers say they already feel besieged by government antiterrorism rules that they consider overly burdensome. The initiative . . . would vastly expand the government's database of financial transactions by gaining access to logs of international wire transfers into and out of American banks." Eric Lichtblau, *U.S. Seeks Access to Bank Records to Deter Terror,* N.Y. TIMES, April 10, 2005.

[8] On April 26, 2005, FinCEN and the five principal federal banking agencies issued an "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States." This document purports to clarify the expectations of the regulators and to confirm that banks have "the flexibility to provide services to a wide range of money services businesses while remaining in compliance with the Bank Secrecy Act." Time will tell whether this document will have its intended effect. However, the document repeats the onerous, time-consuming and expensive due diligence requirements applying to "high risk" money service business customers of banks.

[9] For example, *see* Rob Blackwell, *FinCEN Figures Show SAR Glut Is Worsening*, THE AMERICAN BANKER, April 15, 2005. According to this article American banks are filing an average of 36,000 SARs per month for the 6-month period ending March 31, 2005.

[10] The maintenance of accounts for foreign government officials, including former Chilean president Augusto Pinochet, resulted in civil and criminal penalties assessed against Riggs Bank. This has been widely reported and is summarized in a report of the U.S. Senate Permanent Subcommittee on Inve stigations. For example, *see* Rob Blackwell, *OCC, Fed, Citi Take Hits in Levin Report*, AMERICAN BANKER, March 16 2005.

[11] The widely reported case in which AmSouth was fined $50 million involved the failure to file a SAR based on the existence of a Ponzi scheme.