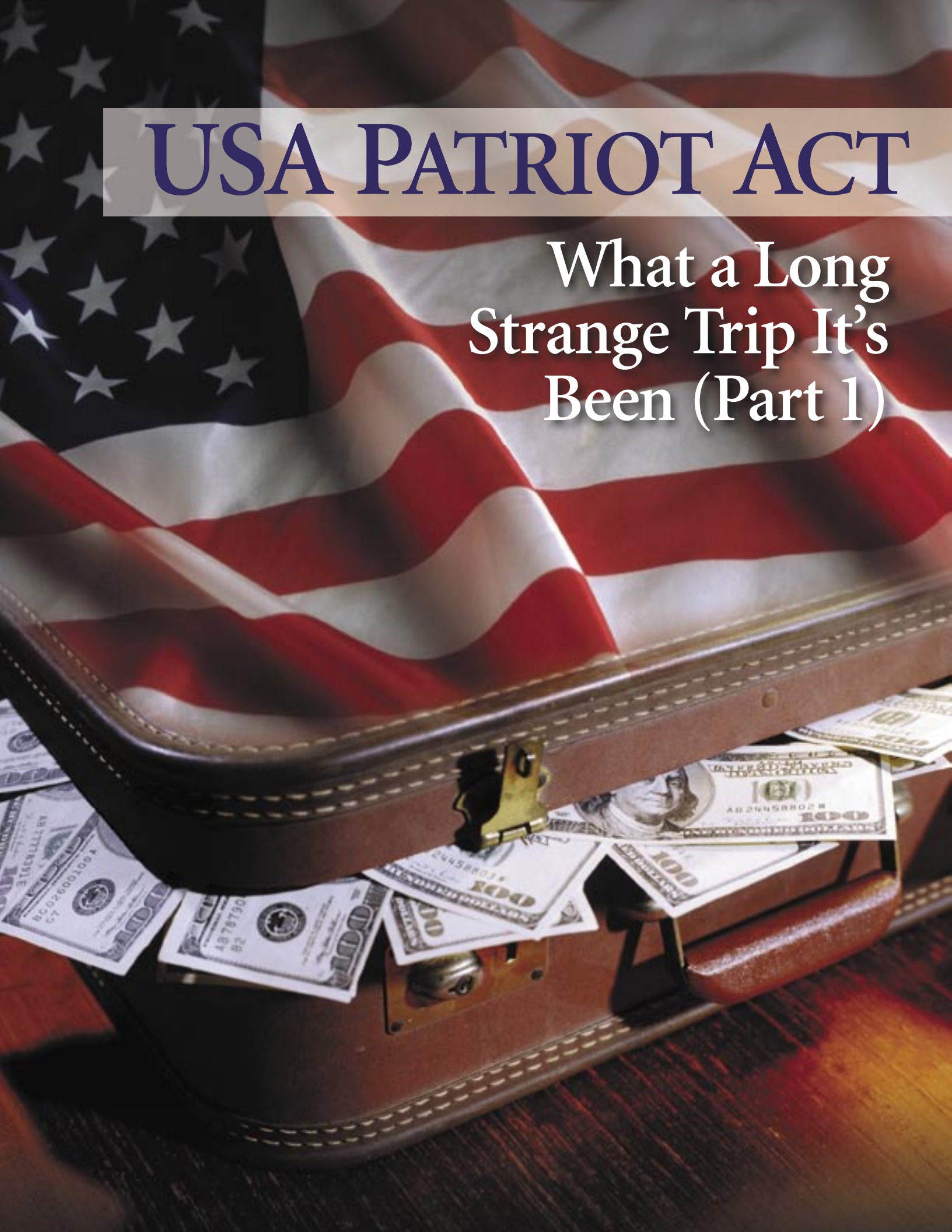


USA PATRIOT ACT

What a Long
Strange Trip It's
Been (Part 1)



Three Years Later

BY JOHN J. BYRNE AND MICHAEL D. KELSEY

October 2004 marks the third anniversary of the USA PATRIOT Act.

In the three years since its passage, anti-money laundering (AML) efforts and detection of terrorist financing have moved from the front burner to the dining room table of compliance priorities, serving up many new AML requirements and reheating traditional ones. Bankers and other financial institution employees who think AML is not one of the key risk issues for their institutions need only look at the FinCEN Web site¹ to add up the millions of dollars in fines assessed against financial institutions with deficient AML programs. There can be no doubt that the USA PATRIOT Act and its implementing regulations are the most significant AML matters since the passage of the Money Laundering Control Act in 1986.

Any student of banking and criminal law understands that the lion's share of the PATRIOT Act that covers banking (Title III) addresses traditional money laundering and not terrorist financing, the activity it was supposed to attack. In fact, most of the provisions in Title III were left over from unsuccessful legislative vehicles from previous congresses. Certainly the tragedy of 9/11 led Congress to act swiftly and in many cases without extensive debate. Despite that fact, the American Bankers Association supported the proposal that eventually became this major new law for a number of important reasons:

- The industry recognized that a new law was going to occur regardless of what we advocated.
- The act attempted to level the AML compliance playing field by requiring regulations to cover a whole host of new financial services providers that previously did not have AML obligations.
- Any new rules would be implemented only after a public opportunity to comment on the changes.
- The act included several new provisions long advocated by the ABA.

On the whole, the ABA considered Title III of the USA PATRIOT Act to be a measure deserving of industry support. Let's see what that support has generated.

Congressional Intent and Reality

Through House Financial Services Committee Chair Michael Oxley, Congress had this to say when the act was signed into law:

The President's signature this afternoon may have been the final step in the legislative process, but it's an important first

step toward ridding this country of the scourge of terrorism... This bill tightens the noose on those responsible for terrorist acts against America.

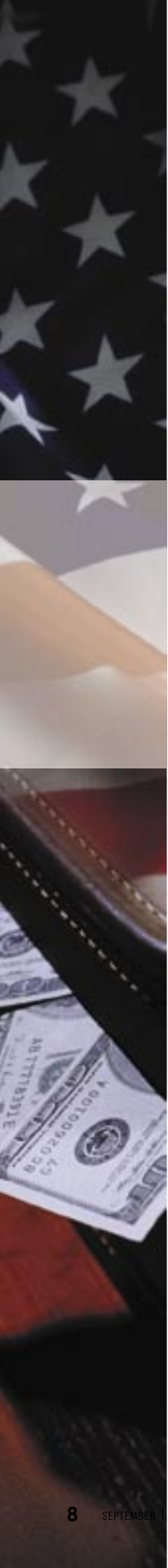
But what areas did the committee focus on when describing Title III? The committee described Title III of the USA PATRIOT Act of 2001 as a measure that includes the following:

- making bulk cash smuggling a crime and requiring registration of black market underground financial networks
- modernizing anti-counterfeiting laws to keep pace with the digital age
- prohibiting U.S. banks and securities broker-dealers from providing financial services to foreign "shell" banks
- forming a new public-private partnership to help law enforcement identify, track, and stop terrorists' financial activities
- requiring that suspicious financial activity be reported in real time to law enforcement agencies
- requiring broker-dealers to report suspicious activity
- requiring banks and other financial institutions to have formal programs for verifying the identities of customers and also require customers to provide financial institutions with truthful information when opening accounts

Perhaps most importantly to our industry, the act specifically required that for the first time, all financial institutions had to institute AML compliance programs, and ordered various regulatory agencies to issue regulations that implement this requirement.

The last provision was in direct response to comments made by the ABA such as the following:

The banking industry remains virtually alone in the pri-



vate sector as partners in the anti-money laundering effort because of the woeful lack of requirements on other financial service providers to prevent and report possible violations of law. The ABA is skeptical of the value of enacting new laws and regulations affecting the banking industry as long as there remains this regulatory “chasm” between banks and everyone else. This is not just a problem for banks; money launderers know the “holes” in the system and are certainly using non-banks for their criminal activities.

The banking industry thus supported this quickly passed measure even though there are some lingering and, to some

Finally, while we were successful in our advocacy of regulatory implementation, congressional impatience with regulatory delays on established AML laws resulted in extremely short time frames to implement regulations under many USA PATRIOT Act sections.

extent, troubling questions as to whether it will really address terrorist financing.

Finally, while we were successful in our advocacy of regulatory implementation, congressional impatience with regulatory delays on established AML laws resulted in extremely short time frames to implement regulations under many USA PATRIOT Act sections. The result was a frenzied environment where banking and other federal agencies struggled to issue their regulations on time, financial institutions worked feverishly to comply with them, and the cost of AML compliance skyrocketed.

This article is the first of a two-part look at the key USA PATRIOT Act banking-related sections to offer some thoughts on what has worked, what has not (or where the jury is still out), and considerations for improvement. We expect that the key measurement of success will be revealed when institutions are examined for compliance, which will enable us to determine whether a true “partnership” between the public and private sectors has been created in the fight against money laundering and terrorist financing.

Measuring Overall Effectiveness

At the outset, we must discard one factor that typically arises in evaluating the merits of a regulation: the so-called “cost benefit” analysis. In most compliance areas, the costs (financial and human) associated with a compliance requirement are compared with the benefits the regulations are supposed to bring, such as truth-in-lending law compliance costs’ being justified by the understanding consumers gain of the cost of their credit.

Those who suggest that AML in the post-9/11 environment can be evaluated in the same terms might compare the number of terrorist attacks prevented to the huge costs of compliance and conclude that the costs are not worth the investment. Such an analysis is flawed, of course: If all the costs of USA PATRIOT Act AML compliance prevent just one terrorist attack, then they are justified. We are not suggesting that there might not be better (and, in practice, perhaps less expensive) ways to accomplish the policy goals of some sections of the act; but we firmly believe that the ultimate goal of preventing terrorist attacks certainly justifies the costs of improved compliance processes in the financial services industry.

We will review the AML provisions of the act more or less in order of their appearance, but we will start with the area that has caused AML compliance officers the most headaches (some real, some self-generated): customer identification programs (CIPs).

Customer Identification Programs

When the proposed CIP regulations were issued for comment, the agencies, responding to clear congressional direction, stressed that for the most part, CIP would merely put into a regulation what most banks were already (or should have been) doing.²

To some extent, they were right: Banks had always conducted some form of customer identification (and certainly the various agency examination procedures required the same) and while they might not have characterized these practices as formal “programs,” they were followed as part of their business practices. However, as is usually the case, the details of the regulation showed that the “already doing” assumption was far too simplistic. In fact, the final CIP regulations contained many ambiguities that drove bankers to overanalysis and budget-busting solutions fueled in part by an exploding community of “CIP vendors” and in part by legitimate (if somewhat paranoid) debates among compliance professionals, lawyers and other “experts” about the “real meanings” of generally worded passages when applied to complex, multiparty business arrangements. The fear was that if a bank did not consider a certain party to be a “customer” or particular arrangement to be an “account,” treat the CIP notice as a disclosure requiring a signed statement from customers, or adopt less than the most conservative position on any CIP interpretation, their examiners would second-guess their decisions and a host of AML compliance woes would result.

Initial regulator concerns that the industry was reading too much into the regulations were slowly replaced by an effort to clarify the ambiguities and missing details. The bottom line is that despite the broad variety of compliance options available to a bank, CIP is not the “just write down what you already do” broad brush that some may have

initially thought or hoped it was. However, institutions with existing policies should not have that far to proceed to achieve adequate compliance.

What Has Worked

Maybe the biggest success for CIP is the general “documentary/nondocumentary” verification options that are available to a bank. While it remains to be seen whether field examiners share this flexible vision of the drafters, for the most part banks have taken advantage of using identification documents, vendor verification tools, and antifraud systems in various combinations. Banks learned that their loan underwriting processes could be leveraged for CIP, and that calling or visiting customers, determining whether mail was being received, and checking references all were nondocumentary verification tools that could be used for fashioning a reasonable knowledge of a customer’s true identity. Problems in the draft regulations were pointed out during the comment period, and the agencies listened and made appropriate adjustments. Gone were document copies (despite a last-minute effort by a minority in Congress to require them) and account signers assuming customer status. All in all, from a high level, CIP allowed banks significant leeway to reasonably verify the true identities of their customers.

What Hasn’t Worked

The problems with CIP are more on the ground level, often not with the compliance professionals but with the line bankers who have to actually perform the CIP. The definitions of “customer,” for example, have triggered much confusion around power of attorney accounts where, under the regulation, the beneficial owner of the account is the customer unless that person is legally unable to own the account (such as an incompetent individual). As ridiculous as it may sound, some banks have considered adding a question like “Is the beneficial owner legally competent?” to their account-opening processes in an attempt to show a good-faith effort toward compliance.

Similarly, stored-value cards, credit cards issued by businesses to their employees for expenses, and other products that involve multiple parties raise operational headaches for line bankers who are told by their compliance or legal departments that one party seemingly detached from the actual account is actually now a customer. Many compliance staff may take the “when in doubt, consider the person a customer” approach, much to the frustration of line staff.

A more universal problem concerns the status of minors as CIP customers. The agencies may not have realized that many states carve out an exception for bank deposit accounts from the “no ability to enter into a contract” status of minors, and that most banks had thousands of accounts for individuals under 18 that were not opened on their behalf

by adults. When the CIP regulations became effective, banks were left with the choice of either prohibiting minors from opening bank accounts (an unacceptable business decision in most cases), considering the minor to be a customer and thus subject to CIP (which often created verification challenges), or opening accounts for minors as some sort of noncustomers under CIP (which made little logical sense). Most have taken the second approach, utilizing more lenient verification standards for young customers that have no government-issued identification documents and no records in nondocumentary vendor databases.

There are a number of other details that bog down CIP compliance and detract from its “banks already do it” direction. One is triggered by the fact that not every customer has an active account at all times. The regulations and first set of FAQs confirmed that a person who does not have an active account when a new one is opened is a “new” customer, subject to new verification and recordkeeping requirements. This ignores the fact that deposit customers may rate shop, opening and closing promotional rate certificates of deposit so there is often no active account when a new certificate is purchased. The same is true for credit card holders who move balances among multiple banks for the best rate. While the verification requirements in these situations may leverage past experiences, establishing multiple recordkeeping periods for each account is cumbersome and expensive.

The complicated reliance provisions of the regulation are also troublesome, particularly with multiple account relationships within a holding company. However, reliance is not a requirement, it was designed to assist banks. Banks are also finding that the resolution of exceptions within the time frames they originally thought were reasonable may have been unrealistic, especially those who rely on nondocumentary verification where vendors (for valid reasons) have little or stale information about a particular customer. In some of these cases, banks may be holding themselves to too high a standard of what constitutes reasonable verification and not utilizing the flexibility that some of the FAQs seem to offer as plausible solutions (e.g., calls to customers, mail not being returned).

Most of these and other challenges that have arisen out of the CIP regulations will probably be resolved as the industry settles into a standard of “reasonableness.” Until then, it is hoped that the bank examination experiences will validate the original assumptions of most banks that for the vast majority of customers, what worked for customer verification before October 1, 2003, is still perfectly acceptable under the CIP regulations.

Section 311: Special Measures

Many banks, especially small, community banks with no international business, may believe Section 311 is a non-event

for them. This may be true, but 311 is a USA PATRIOT Act provision that no banks can ignore. Whether it is for a single bank identified by the Treasury as being off limits to U.S. banks and other persons, or a broad prohibition of accounts or transactions involving an entire country, 311 special measures are imposed only when the subject is considered to be of the highest risk for money laundering or terrorist financing.

What Has Worked

Perhaps the most successful aspect of Section 311 in the eyes of many bankers has been its selective utilization by the Treasury. With perhaps the exception of the broad provisions that were applied (and subsequently repealed) against Ukraine, 311 has not been a continuing stream of sanctions applied to every country or institution that is suspected of having a deficiency.

What Hasn't Worked

Many bankers would argue that Section 311 added too much confusion to an already crowded collection of lists against which customers and transactions must be scrubbed. Some would argue that the distinction between 311 and OFAC sanctions didn't amount to a difference, and that it would have been far easier had the government merely carved out a place within OFAC to meet these policy demands.

Section 312: Enhanced Due Diligence

Section 312 could be characterized as a dormant volcano waiting to erupt. As of the date of this article's writing, the final "final" regulations were still not issued, leaving banks with the interim final regulations that generally implement the statute without much guidance. Banks are expected to be applying these general requirements to their foreign private bank accounts for "senior foreign political figures" and accounts maintained by foreign financial institutions.

What Has Worked

This is a tough regulation to assess, simply because it is incomplete. Feedback thus far suggests that in the absence of the final regulation, banks that made good-faith efforts to implement the statute have been at least neutrally viewed by their examiners. Keep track of this one, however, as all indications are that the final rule will impose real burdens on the industry. Banks should also not rely solely on the 312 regulations as the only word on these issues, as recent guidance regarding embassy and foreign accounts also needs to be factored into the compliance equation.

Section 314: Information Sharing

One of the most misunderstood sections of the Title III is section 314. Originally touted as a provision designed to provide the private sector with information or "feedback"

from the government, it became instead a provision that simply told the industry to look for matches to government investigative targets.

What Has Worked

In late 2002 under Section 314(a) of the USA PATRIOT Act, The Department of Treasury's Financial Crimes Enforcement Network (FinCEN) started sending e-mail messages to banks seemingly out of the blue, causing much confusion and apparently for criminal suspects who fell far below the alleged national security concern that was supposed to be the standard for the expedited search expectations of recipients. The American Bankers Association was severe in its criticism of the implementation of this process, which was suspended until a more effective and selective method could be put in place. Since that time, regulators, law enforcement, and the Treasury have made adjustments and revised the process to "address a number of logistical issues and to develop additional guidance on the information request process."

The announced changes included the following:

- Section 314(a) requests from FinCEN will be batched and issued every two weeks, unless otherwise indicated in the request.
- After receiving a 314(a) request, a financial institution will have two weeks, rather than one week, to complete its searches and respond with any matches.
- Searches will be limited to specific records and, unless otherwise noted, each will be a one-time search.
- If a financial institution identifies a match for a named subject, the institution need only respond to FinCEN that it has a match and provide point-of-contact information for the requesting law enforcement agency to follow up directly with the institution.

On the whole, these changes have been instrumental in improving the process. While we still have concerns that law enforcement does not always respond promptly to contact from financial institutions on matches, the overall consensus is that 314 is a vastly improved process.

What Didn't Work

To the extent that Congress envisioned 314 as a means of facilitating two-way communication between law enforcement and financial institutions (in the case of 314(a)), or between financial institutions (in the case of 314(b)), cannot be called a success. The only meaningful communication from law enforcement is the 314(a) e-mail process discussed above, which is essentially a demand for records searches by financial institutions.

At this time, the only feedback being received by institutions are follow-up subpoenas, although the Treasury Department has published statistical feedback from the 314 process. Also, there is no standard forum that provides

banks with general or specific information about terrorists or money-laundering risks that can be used within their institutions. Understanding that the confidentiality and sensitivity of such information is critical, because banks are accustomed to handling this information in this manner under their SAR processes there should be no reason why, with appropriate safeguards, more information cannot be shared with banks. Such mutual communication is essential if a true partnership with law enforcement is to be achieved.

If bank examiners cite banks for failing to identify situations that could have been prevented had appropriate communication with law enforcement occurred, then the adversarial nature of the public-private sector relationship will be reinforced, ultimately damaging the effectiveness of AML compliance efforts.

Another troublesome aspect of 314(a) to many banks is the mandate to not apply the names obtained in 314(a) e-mails prospectively. Banks realize that closing or rejecting a customer account due to inclusion on a 314(a) list would be detrimental to law enforcement investigations. On the other hand, banks fear that opening such an account after a name is obtained could eventually damage the bank's reputation or even lead to financial losses. Specific feedback on 314(a) suspects would be the preferred means of managing these risks, but absent that, some guidance on how to address a new customer or transaction that is with a suspect is essential. It is difficult to imagine that law enforcement would not be interested in a new account opened by a person who is deemed to be a threat to national security interests.

As for 314(b), many believe that this section provides a safe harbor for the kinds of communications that have occurred among banks for years, and to the extent that this is the case, it is a welcome and necessary change. But some banks have found that if they volunteer for participating in the 314(b), some examiners are expecting detailed procedures that almost make participation a penalty. This leads to the last section of this first installment of our analysis.

Uniform and Consistent USA PATRIOT Act/BSA/AML Examination Procedures

The two remaining issues in this article are not directly part of the USA PATRIOT Act but are relevant in assessing the impact on the industry: overall examination focus and the review of SAR reporting.

ABA has previously emphasized to Congress and the Treasury Department that the banking agencies need to reach an agreement as to how the financial services industry will be examined for compliance under the USA PATRIOT Act and other AML requirements. As we indicated at the time, "too often, institutions of the same approximate size, in the same geographic area, and offering the same financial products are treated differently for compliance purposes. This should not continue."

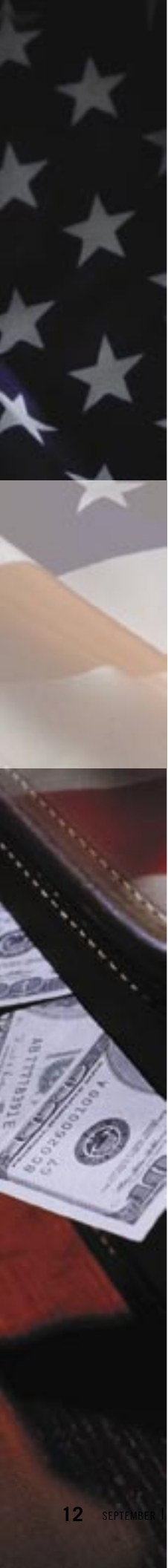
There have been recent examples of coordination of examination procedures by the agencies, but the process is not yet complete. The good news is that FinCEN Director William Fox has expressed public support for consistency by, among other things, directing the Bank Secrecy Act Advisory Group (BSAAG) to form a subcommittee on examination issues.³ This subcommittee, co-chaired by the ABA and the Federal Reserve Board, will review existing guidance and offer appropriate recommendations. We will report on our progress in the next article. In addition, Treasury Department Deputy Secretary Samuel Bodman

In some cases, filing a small number of SARs is viewed as a negative indicator of AML program effectiveness. But in others, banks that are filing many SARs are being seen as "high risk" by their examiners. Obviously, this suggests a significant and alarming development in the examination and review process.

announced a "FinCEN realignment" that will assist in improving examination consistency. The banking agencies responded to the announcement by stating they will publish interagency examination procedures. All of these announcements are good signs.

Quantity of SAR Filings Should Not Determine Adequacy of SAR Program

One major problem affecting banks in the AML exam process may or may not have arisen due directly to the USA PATRIOT Act—but it's here nonetheless. Recently, several financial institutions have contacted the ABA about examiner criticisms in reviews of their suspicious activity report (SAR) programs, due in large part to the number of SARs filed. These financial institutions expressed the concern, which we share, that this may reflect new criteria for evaluating the adequacy of SAR programs—namely, that the number of SARs filed meets a minimum threshold, or that institutions are not filing the same number of SARs as "peer" institutions. The concern expressed is that there might be a new requirement in the form of a "quota" for determining the adequacy of SAR programs consisting, in large measure, of counting the number of SARs filed and, in some instances, comparing the number of SARs filed by "peer" institutions. In some cases, filing a small number of SARs is viewed as a negative indicator of AML program effectiveness. But in others, banks that are filing many SARs are being seen as "high risk" by their examiners. Obviously, this suggests a significant and alarming development in the examination and review process.



It is without question that the continuing importance of filing SARs is to inform governmental authorities of the existence of suspicious activity that may merit further investigation by law enforcement or supervisory agencies. As was stated recently by FinCEN in the "Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative":

The purpose of the Suspicious Activity Report (SAR) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA). In many

Clearly, an institution that has not filed SARs or has a track record of minimal filings deserves greater scrutiny of its SAR program. However, a lack of filings or a limited number of filings should be nothing more than a signal to the supervisory agency that a closer review of the SAR program is warranted.

instances, SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also presents FinCEN with a method of identifying emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

One of the primary reasons for an institution to have an adequate SAR program is to ensure that potentially suspicious activity is appropriately identified and managed within an institution. The adequacy of a SAR program cannot be judged by the number of SAR filings, but rather must be evaluated with regard to the institution's ability to identify potentially suspicious activity, evaluate whether the activity rises to the level of requiring the filing of a SAR, and ultimately, lead to a process to determine how the activity is dealt with within an institution.

The notion that the number of SAR filings can determine the adequacy of a SAR program is, by any measure, faulty. Clearly, an institution that has not filed SARs or has a track record of minimal filings deserves greater scrutiny of its SAR program. However, a lack of filings or a limited number of filings should be nothing more than a signal to the supervisory agency that a closer review of the SAR program is warranted. A determination of this type should be the result of a comparison of the number of filings of a particular institution with that institution's pattern of SAR filings rather than a comparison of filings between institutions. As an example of

focusing on a particular institution's SAR filings rather than comparing filings between institutions, the Federal Reserve Board instructs its examination staff as follows:

... continue the process of assuring that SARs are reviewed prior to the commencement of an examination or inspection. As the Reserve Banks have learned, a pre-examination/inspection review of SARs assists the supervisory staff in assessing compliance with the SAR requirements and provides useful information regarding potential problems that may require special attention during the course of an examination or inspection.

Variation in the number of SAR filings between like or peer institutions can be attributed to numerous factors and, therefore, is not itself a reliable indicator of the adequacy of a particular SAR program. The type of customer base an institution maintains (for example, retail vs. corporate clientele), the markets in which an institution operates, or differences in the parameters applied in monitoring customers and their transactions are all factors that may lead to wide variations in the numbers of SAR filings between institutions. Additionally, contrary guidance or direction provided by an institution's functional regulator could have a significant impact on the way the institution views suspicious activity. For example, several financial institutions have reported to the ABA that examiners have instructed institutions to file SARs if they believe they have information that may be of interest to the government, such as identifying an account or transaction related to an investigation that has appeared in the press, *without regard* to whether suspicious activity actually exists.

Furthermore, regulatory scrutiny of SAR filings and the recent civil penalties assessed against banks for SAR deficiencies have caused and will cause many institutions to file SARs as a purely defensive tactic (the "when in doubt, file" syndrome) against unwarranted criticism or "second guessing." If that continues, the legitimacy of the information in the SAR database will be called into question.

The SAR process should be addressed as the Federal Deposit Insurance Corporation (FDIC) examination procedures cover the area, by explicitly recognizing that there may be a variety of legitimate reasons for variations in the number of SARs filed by the same institution:

Determine if the institution or any branches had significant changes in the volume or nature of SARs filed, and investigate the reason(s) for these change(s). . . (Note: Increases in SARs may be caused by an increase in high-risk customers, entry into a high-risk market or product, or an improvement in the bank's method for identifying suspicious activity. Decreases may be caused by deficiencies in the bank's process for identifying suspicious activity, the closure of high-risk or suspicious accounts, personnel changes, or the failure of the bank to file SARs.)

With the increased focus on SAR programs and the

number of SAR filings by institutions, the financial services industry is becoming increasingly concerned about the regulatory review of the SAR process. We believe that there is no correct number of SARs that should be filed in order for a determination that an institution has an adequate SAR program. A comparison between institutions of the number of SARs filed is wrong.

It would be helpful if the government would re-state that SAR reporting obligations are based on an institution's analysis of potentially suspicious activity. If an institution has a SAR program that allows for a reasoned analysis of potentially suspicious activity and the institution's program is being followed, there should be no need for discussions regarding the numerical threshold of SAR filings and no comparisons between institutions.

The good news is that regulators are scrambling to prove our theory false. Let us hope we do not have to report on this problem again.

Conclusion to Part 1

The USA PATRIOT Act was passed three years ago, and industry, government, and policy makers (not to mention the public) are still assessing its success. There are clearly more positive signs than negative. The problems we have raised are being addressed and the partnership atmosphere (despite some outside influences) remains strong.

Part II, slated for publication in the November/December 2004 issue of *ABA Bank Compliance*, will address the struggles with Section 319, the need to actually use the section permitting the sharing of information on terminated employees, the 312 burdens sure to come, and the process to utilize technology to file reports. Until then, document, document, document! BC

¹ www.fincen.gov/reg_enforcement.html

² See original Federal Register notice on the proposal, which stressed, "Rather than imposing the same list of specific requirements on every bank, regardless of its circumstances, the proposed regulation requires all banks to implement a Customer Identification Program (CIP) that is appropriate given the bank's size, location, and type of business." Vol. 67, No. 141, p. 48292 (July 23, 2002).

³ Fox told the Senate Banking Committee in April, "We must find ways to ensure that these regulatory programs are implemented in a fair and consistent manner that is focused on achieving the goals of the Bank Secrecy Act. Although difficult, this is an issue that must be resolved."

ABOUT THE AUTHORS

John J. Byrne is director of the Center for Regulatory Compliance in the Regulatory and Trust Affairs Section of ABA's Government Relations Division. He has more than 20 years of experience in lobbying, regulatory, and educational efforts on money laundering, asset forfeiture, computer security, privacy, and other general electronic banking

and compliance issues. He has represented the ABA before Congress, state legislatures, and various regulatory agencies as well as in the electronic and print media.

Mr. Byrne has been a member of the Treasury Department's Bank Secrecy Act Advisory Group since its inception and co-chairs the American Bar Association/American Bankers Association Annual Money Laundering Enforcement Seminar (now in its 16th year). He also co-chairs the "SAR Activity Review" project, advises the Association of Certified Anti-Money Laundering Specialists (ACAMS), staffs ABA's Fraud Prevention Oversight Council, Payment Systems Committee, and Compliance Executive Committee. He has written extensively on money laundering and privacy issues and is a frequent contributor and adviser to Money Laundering Alert, Bankers Hotline, ABA Bank Compliance magazine, and other publications. He is also the editor of ABA's Money Laundering and Terrorism Issues Update, a weekly e-mail newsletter.

Mr. Byrne has been a faculty member of the ABA's Graduate Compliance School, the Association's Bank Security School, speaks at dozens of conferences each year, and has done several overseas money laundering deterrence programs for the U.S. Customs Service and the State Department. He was the first private-sector recipient of the Director's Medal for Exceptional Service from the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

Prior to this position, Mr. Byrne was an assistant general counsel in ABA's Office of the General Counsel. He received his undergraduate degree from Marquette University in Milwaukee, Wis., and his J.D. from George Mason University in Arlington, Va. He is a member of the District of Columbia and Pennsylvania Bars. He can be reached by telephone at (800) BANKERS or via e-mail at jbyrne@aba.com.

Michael D. Kelsey is PNC Financial Group's director of retail and wholesale bank compliance as well as its corporate anti-money laundering compliance officer. He joined PNC in 1985 and has held a number of positions in its legal and compliance departments. He currently serves on the ABA Compliance Executive Committee, writes and speaks frequently on money laundering and other compliance issues, and is a member of the Widener University School of Law adjunct faculty in Wilmington, Delaware. Mr. Kelsey became a member of the Delaware Bar in 1983 and lives in Wilmington with his family. He can be reached by telephone at (302) 429-1775 or via e-mail at michael.kelsey@pnc.com.