

USA PATRIOT Act: Evolving Regulations Challenge Financial Institutions

integrated

Since September 11, 2001, banks have been checking names on new accounts against government lists of known or suspected terrorists. As a result, the U.S. and its partners have publicly designated a voluminous list of terrorists or terrorist supporters. Deputy secretary of the U.S. Treasury, Kenneth W. Dam, told the June 2002 Council on Foreign Relations in New York, "We have frozen over \$115 million around the world. One hundred and sixty-six countries and jurisdictions have blocking rules in force." Considered one of the world's largest businesses, money laundering is estimated to be \$1 trillion annually, with 50% of the funds passing through the U.S. at some point. The numbers speak for themselves; detecting and restricting illicit financial activities are issues transforming the worldwide financial community.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was passed in October 2001 to address tracking and limiting the financial resources fueling terrorist activities. The USA PATRIOT Act imposes strict new requirements on financial institutions with severe penalties for non-compliance. Institutions must "know their customers"—closely monitoring account ownership and usage.

Requirements for Financial Institutions

As the U.S. Treasury interprets rules for implementation, financial institutions struggle with the issues affecting compliance. All financial institutions, including depository financial institutions, such as banks and credit unions, securities dealers, investment bankers, commodity traders, money transfer agents, and companies handling "non-financial" transactions are mandated to comply with an initial four requirements.

First, they must have a compliance officer to lead the anti-money laundering (AML) program. Next, they must create internal AML policies and procedures. Third, they have to institute a training program. Finally, financial institutions are expected to create an independent audit process to test their internal procedures.

Creating a workable system for scouring the network for terrorist assets is not easy, notes Kerry Massaro of Wall Street & Technology. Given the tight timetable the U.S. Treasury has set forth, building a system is not

an option. The increasing complexity of regulations, combined with severe penalties for non-compliance, make manual processes a high-risk proposition. The answer, as advocated by TowerGroupSM, is vendor-based software.

Finding the Right Solution for Compliance

The USA PATRIOT Act accelerated the pace of new regulations; reporting and information sharing requirements are increasing, and the timelines for responding are decreasing. There are some certainties, however. "Having an exception-based system that can identify aberrant behavior is essential," says Wall Street & Technology's Massaro. Listing eight vendors who inhabit this transaction monitoring and reporting technologies space, Massaro includes Sybase. Deployed in 90 percent of the world's securities firms and in 60 percent of the world's banks, few competitors can match Sybase's breadth of experience or success in financial institutions over the past 18 years. Sybase's expertise in managing information, applications, and integrating processes soundly satisfies the USA PATRIOT Act's requirements through an automated process for continuous monitoring that is unobtrusive, secure and cost effective. Beyond extensive industry experience and lower TCO, Sybase also delivers on two important aspects identified by TowerGroup's analyst Breffni McGuire: satisfying mandated regulatory requirements and identifying potentially suspicious activity.

Experts agree that the follow-the-money and know-your-customer rules introduced as part of the new war on terrorism require diligent monitoring, auditing and record keeping. "One of the reasons Sybase got into this area is, ultimately, because it's about integration," says Sybase's PATRIOT expert John Berley, lead area architect. "You have to be able to filter a customer's identity and how they conduct their business, whether they are suspect individuals doing business with a particular company, or the beneficiaries of a transaction. So it's not just the account owner who's involved," he added. "The Sybase solution combines the detailed search and filtering required for accuracy. Our system scans every record and customer file to make sure there is no illicit activity, and if there is, identify and report it."

International Contacts

Argentina +5411 4313 4488	Korea +82 2 3451 5200
Australia +612 9936 8800	Malaysia +603 2142 4218
Austria +43 1 504 8510	Mexico +52 5282 8000
Belgium +32 2 713 15 03	Netherlands +31 20 346 9290
Brazil +5511 3046 7388	New Zealand +64 4473 3661
Bulgaria +359 2 986 1287	Nigeria +234 12 62 5120
Canada +905 273 8500	Norway +47 231 621 45
Central America +506 204 7151	Panama +507 263 4349
Chile +56 2 330 6700	Peru +511 221 4190
China +8610 6856 8488	Philippines +632 750 2550
Colombia +57 1 218 8266	Poland +48 22 844 55 55
Croatia +385 42 33 1812	Portugal +351 21 424 6710
Czech Republic +420 2 24 31 08 08	Puerto Rico +787 289 7895
Denmark +45 3927 7913	Romania +40 1 231 08 70
Ecuador +59 322 508 593	Russian Federation +7 095 797 4774
El Salvador +503 245 1128	Slovak Republic +421 26 478 2281
Finland +358 9 7250 200	Slovenia +385 42 33 1812
France +33 1 41 91 96 80	South Africa +27 11 804 3740
Germany +49 69 9508 6182	South Korea +82 2 3451 5200
Greece +30 1 98 89 300	Spain +34 91 749 7605
Guatemala +502 366 4348	Sweden +46 8 568 512 00
Honduras +504 239 5483	Switzerland +41 1 800 9220
Hong Kong +852 2506 6000	Taiwan +886 2 2715 6000
Hungary +36 1 248 2919	Thailand +662 618 8638
India +91 22 655 0258	Turkey +90 212 325 4114
Indonesia +62 21 526 7690	Ukraine +380 44 227 3230
Israel +972 3 548 3555	United Arab Emirates +971 2 627 5911
Italy +39 02 696 820 64	United Kingdom +44 870 240 2255
Ivory Coast +225 22 43 73 73	Venezuela +58 212 267 5670
Japan +81 3 5210 6000	Asian Solutions Center +852 2506 8700
Kazakhstan +7 3272 64 1566	

For other Europe, Middle East, or Africa inquiries:
+33 1 41 90 41 64 (Sybase Europe)

For other Asia Pacific inquiries:
+852 2506 8700 (Hong Kong)

For other Latin America inquiries:
+925 236 6820



Sybase, Inc.

Worldwide Headquarters

One Sybase Drive
Dublin, CA 94568-7902 USA
Tel: +800 8 SYBASE
www.sybase.com

Berley, a veteran of 26 years in the financial services and IT industries, says that in talking with clients there are three groups: those whom he calls ostriches—people who hope it will go away; those who are nervous about what's involved and will move slowly; and the early adopters who want to stay ahead of the curve. "This issue is not going to go away," says Berley. "The financial institutions that are addressing overall integration issues as well as USA PATRIOT Act compliance gain competitive advantage for the long-term," Berley concludes.

Financial institutions should be able to identify, track, and, in some senses, control terrorist funds—not just by blocking assets but also through tougher identity verification against government-supplied lists.

A compliance solution needs to conduct checks not only when accounts are opened, but throughout the life of the account, tracking ongoing transactions (including all parties to the transaction) as well as sources of funds. Financial institutions should be able to identify, track, and, in some senses, control terrorist funds—not just by blocking assets but also through tougher identity verification against government-supplied lists. This requires integrated scanning and filtering technology. As part of this effort, the U.S. Treasury now requires brokers and dealers of securities to report suspicious activity. Under a rule published on July 1, 2002, these firms are required to "report suspicious transactions that are conducted or attempted, by, at, or through a broker-dealer and involve or aggregate at least \$5,000 in funds or other assets."

A Long-Term Perspective: Compliance and Integration

Sumitomo Mitsui Banking Corporation, a \$24 billion company ranked 137 on Fortune's Global 500 list, conducted extensive due diligence before it selected the Sybase PATRIOT compliance Solution. Peter McCormick, Sumitomo's chief information officer explains, "Sybase has coupled many of its

innovative products to provide an end-to-end solution which strengthens our ability to meet current and ongoing compliance requirements. The component-based solution differentiates Sybase from the other offerings in the marketplace."

"Sybase has coupled many of its innovative products to provide an end-to-end solution which strengthens our ability to meet current and ongoing compliance requirements. The component-based solution differentiates Sybase from the other offerings in the marketplace."

— Peter McCormick, CIO, Sumitomo Mitsui Banking Corporation

Sumitomo's McCormick adds that the robust architecture of the product gives the bank the confidence to tackle the new business challenges of the law while integrating and leveraging its existing information systems investments. Therein lies the real value of the solution: extending the USA PATRIOT Act requirements to act as an integration impetus for existing systems. Connecting different islands of information throughout the organization is essential not only for compliance, but also for ongoing success.

As the clock ticks and compliance dates come closer, the question of time to get a USA PATRIOT Act compliance solution in production becomes very critical. With possible penalties up to \$1 million, and criminal charges for bank officers—the risks are large for non-compliance. An even greater deterrent is the potential damage to an organization's reputation for failure to comply. Industry pundits warn against complacency in a world where aggressive tactics against corporate malfeasance are increasingly seen as a way of setting an example.

Financial services institutions have strong incentives to take the necessary steps to comply with the letter and spirit of the law. But finding and implementing the right technology solution for compliance are the real challenges facing financial institutions. And that is something not even an "ostrich" can ignore.