

*Leading thoughts on
issues facing the financial
services industry.*

The USA PATRIOT Act and OFAC: Myths and Realities

By Breffni McGuire
Senior Analyst, Global Payments
TowerGroup

Issue 38: August 2003

Any new piece of legislation can cause confusion in the financial marketplace. When the legislation is as lengthy, complex, and quickly implemented as the USA PATRIOT Act, the opportunities for confusion abound. As the Act is just two years old, and many of the Treasury's required regulations are even newer, the dust is still settling. Numerous unresolved issues and inconsistencies make some sections of the Act and the regulations ambiguous. In some cases, clarity is being sacrificed to hype. The intermingling of Office of Foreign Assets Control (OFAC) rules and the Act's Section 326 requirement for verification of customer identity by comparison to a government-supplied terrorist list highlights both legitimate ambiguities and those being perpetuated for other purposes.

Background

OFAC rules and Section 326 intersect in the area of account opening (although they diverge in other requirements). Both mandate consulting government-supplied lists of known or suspected terrorists or terrorist organizations to deny terrorists access to the banking system. OFAC is the US Department of the Treasury office charged with administering economic and trade sanctions against countries, entities, and individuals posing a threat to US national security and foreign policy goals. Combating global terrorism and terrorist financing is vital to its mission, but it is just one piece of OFAC's total charter. Banks' OFAC responsibilities extend beyond the account-opening process to transaction monitoring and other activities and cover all sanctions programs and list entries.

Title 3 of the USA PATRIOT Act is fundamentally anti-money laundering legislation. Because the Act was driven by the events of September 11, 2001, its major thrust is preventing terrorists from gaining access to the US banking and financial systems. Section 326 deals with verification of customer identity at account opening: Its goal is to ensure that a bank "knows its customer" to the extent of forming a reasonable belief that the customer is who (s)he claims to be *before* providing services. One of the section's three major provisions stipulates that banks must establish procedures to determine whether or not a potential customer appears on any list of known or suspected terrorists or terrorist organizations that is supplied to them by a federal government agency — and to comply with any associated directives.

OFAC requires banks to check its master list of *Specially Designated Nationals and Blocked Persons* (alternately referred to as the SDN or OFAC list), as well as

sanctioned countries' lists, as the basis for compliance. To date, the lists to be used for the Section 326 compliance have not been specified. The OFAC list has become the de facto list of choice both because it's readily available and meets the requirements and because banks already use it when opening a variety of accounts. (As noted in the May 9, 2001, Federal Register, it was the intent of Congress that the lists to be used for 326 verification were to be those "already supplied to financial institutions by OFAC, and occasionally by law enforcement and regulatory authorities, as in the days immediately following the September 11, 2001 attacks.")

Myths

Because of the overlapping requirements, the USA PATRIOT Act has already engendered its share of myths relative to OFAC. Many have to do with supposed joint requirements between the Act and OFAC's sanctions programs. Some of the more common myths are listed in the box below.

- Myth 1** OFAC rules are part of the USA PATRIOT Act.
- Myth 2** Compliance with the USA PATRIOT Act requires financial institutions to report matches to the OFAC list.
- Myth 3** Developing a Customer Information Program meets OFAC requirements.
- Myth 4** Until an institution is required to develop a Customer Information Program, it has no responsibility for OFAC compliance.
- Myth 5** The USA PATRIOT Act increases financial penalties for OFAC violations.
- Myth 6** OFAC filtering technology provides an AML solution.

Realities

Although all the myths are interesting and may be woven in part from real cloth, none is true.

1. OFAC rules were not issued as part of the USA PATRIOT Act.

Although banks should have been well aware of their OFAC obligations, the publicity around the Act made many institutions more cognizant of their full responsibilities and "introduced" OFAC into mainstream thinking among all types of financial institutions. This and a shared focus on disrupting terrorist financing activities may account for the misapprehension that OFAC rules somehow arose from the Act. The reality, however, is that while the USA PATRIOT Act was enacted into law in October 2001, OFAC was created as an office of the Treasury Department in 1950, and banks have been responsible for compliance for decades. The Act does update some of the law governing OFAC

sanctions, which perhaps played a role in the confusion. (For instance, it adds vesting of assets to the provisions of the International Emergency Economic Powers Act of 1977.)

2. Compliance with the USA PATRIOT Act does not require financial institutions to report matches to the OFAC list.

Although Section 326 of the Act requires that covered financial institutions check a government-supplied list of known or suspected terrorists, the determination of what list to use was remanded to Treasury to include in required regulations. Treasury and the industry regulators have yet to do this: “OFAC” was not designated as the list to be used for 326 purposes in the final rules issued in April 2003. Nonetheless, as noted above, the OFAC SDN list is being used and has spawned its own myths. In most cases, there is honest confusion; in others there is some self-interest. The Act clearly does not require reporting “OFAC matches,” although ambiguities or other suspicious behavior detected during the account-opening process could result in generation of a suspicious activity report (SAR). Section 326 also allows institutions some flexibility to open accounts before all verification information is complete. Flexibility is not an OFAC concept: According to the rules, banks must report any match to OFAC and freeze or reject the relevant account.

3. Developing a Customer Information Program does not meet OFAC requirements.

The Customer Information Program (CIP) was created as part of Treasury’s mandated requirement to develop regulations for Section 326 and was introduced in April 2003. OFAC has existed for decades and has broad reach across the industry relative to sanctions programs and blacklisted entities, which extends well beyond account opening to transaction monitoring and other activity. Banks, securities firms, and insurance companies (among others) are targets of OFAC regulation. (OFAC publishes regulations on its Web site specifically for these types of institutions.) The CIP has no direct relationship to OFAC compliance. Its only incidental connection to OFAC rules is verification of customers to a terrorist list. The CIP is also concerned with a variety of know-your-customer issues at account opening that have nothing to do with foreign policy considerations and everything to do with protecting the bank and preventing criminals from gaining access to bank services.

4. An institution does have responsibility for OFAC compliance even when it may not yet be required to develop a Customer Information Program.

The notion that a bank is not responsible for OFAC compliance until a CIP is required is another misconception mistakenly tying together CIP and OFAC compliance. As noted, Treasury developed the CIP to meet mandated provisions of Section 326. In April 2003, seven federal industry regulators issued similar CIP rules for their respective industries. However, not all types of financial institutions are currently obligated to have a CIP. For example, neither anti-money laundering programs nor CIP requirements have yet been drafted for insurance companies. All these financial institutions, however, are responsible for compliance with OFAC sanctions today. Compliance is not optional, nor does it depend on a CIP or any new regulation.

5. The USA PATRIOT Act does not increase financial penalties for OFAC violations.

One of the reasons for the myth that the PATRIOT Act increases penalties for OFAC violations is that vendors commonly cite OFAC violation penalties in discussions on anti-money laundering. In fact, penalties for AML violations and OFAC violations are distinct, and the Act does not affect OFAC penalties. The Act does introduce new civil and criminal penalties for money laundering. Penalties vary by the type of violation. OFAC penalties depend on which of the relevant statutes is violated and whether civil or criminal actions are being sought. Civil penalties are assessed by OFAC. Theoretically, a given instance could give rise to both OFAC and money laundering violations, but the penalties would be determined separately.

6. OFAC filtering technology does not provide an anti-money laundering solution.

A number of institutions are not clear what type of product is needed to address the requirements of OFAC and the Act. Vendors can be part of the confusion here. Companies have rushed to label any technology that can be used to attack any piece of the Act as being USA PATRIOT Act-compliant. While this is completely legitimate given the diverse requirements of the Act, it does not always add to a bank's understanding of what is needed. OFAC technology is a case in point. OFAC interdiction software can, and often should be, used to filter a variety of lists or databases in addition to the SDN list to ensure that a bank is not only complying with OFAC rules but is also interdicting transactions with other undesirable entities. OFAC technology may also be used as a search tool. Because OFAC states on its Web site that use of technology is a mitigating factor in its penalty assessments, vendors promote the OFAC capabilities of their products. When OFAC products are presented in the context of the Act's requirements, however, some banks are left with the idea that filtering technology is an AML solution. In and of itself, it is not. Filtering is not sufficient for detecting ongoing activity or patterns indicative of money laundering. True AML solutions monitor transactions to detect potentially suspicious activity across multiple systems, generally at an enterprise level, and they address "know your customer" requirements through continuous analysis of transaction activity. Given the importance of OFAC, however, AML vendors routinely offer filtering technology as a component of their solution or as an add-on capability (through another vendor). And, in some cases OFAC products have been labeled as USA PATRIOT Act solutions, further muddying the waters.

Conclusion

Today the "fear of God" message is a strong sales tactic in the market. Penalties and publication of violations are also strong motivators. It is undeniable that this increased focus on regulatory issues, compliance, and technology is good and has expanded market awareness, but myths and confusion are not helpful. Confusion detracts from real needs, can cause inappropriate actions, and ultimately translates into increased costs. Both OFAC sanctions and the USA PATRIOT Act pose major challenges for banks. In the short term, myths gain attention and can help sell software. But in a complex regulatory environment, financial institutions need clarity to address the issues that confront them. Regulation is a serious issue and requires serious attention from all participants in the market.