Handbook of Anti Money Laundering
By Dennis Cox

9 THE US REGULATORY FRAMEWORK

This chapter provides an overview of the USA regulatory framework. Additional information on the specific rules applied in the USA is included in the USA country profile in Chapter 27 of this book (Section 27.36). This chapter provides more detailed information about the current American AML regulations.

9.1 THE US PATRIOT ACT

The 342-page US Patriot Act forms the current cornerstone of US anti-money-laundering legislation. Passed in 2001, the actual title of the legislation is:

> *"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001."*

As you will notice from the title, the Patriot Act is not actually an "all crimes" piece of legislation and restricts itself to detecting and preventing terrorist financing only. Perhaps, given the date that this legislation was passed by the House of Representatives (24th October, 2001) and signed by the then President George W. Bush (26th October, 2001), this is not surprising.

This Act adds to the existing US legislation on anti-money-laundering by extending the Bank Secrecy Act across the entire financial services industry. However, different institutions will find that the Act impacts them in different ways, since there are additional criteria that relate to the size and complexity of an institution and the nature of their operations.

9.2 THE OTHER KEY US REGULATIONS

US banks were already subject to money-laundering regulations prior to the enactment of the Patriot Act, as shown in Table 9.1.

Table 9.1 Key US regulations relating to money laundering prior to the Patriot Act

Act	*Year*
Bank Secrecy Act	1970
Money Laundering Control Act	1986
Annunzio Wiley	1992
Money Laundering Suppression Act	1994
Funds Transfer Rules	1996

It is from the 1970 Bank Secrecy Act that the rules related to record retention and the requirement to report transactions of $10,000+ emanate, and these rules continue to apply. The 1986 Act introduced the key offences resulting from money laundering.

Suspicious transaction reporting emanates from Annunzio Wiley, whereas suspicious activity reporting comes from the 1994 Money Laundering Suppression Act. While you might hope that all of this regulation might be consolidated into a single Act, there is no suggestion that such consolidation is likely in the near future.

The US is the only country we have identified which appears to have adopted such a piecemeal approach to money-laundering deterrence and terrorist financing.

9.3 KEY ISSUES IN THE US PATRIOT ACT

As we have noted, the US Patriot Act is lengthy, perhaps too lengthy, and, as discussed above, it is predicated on the existing legislation. Its focus is on the requirements with respect to terrorist financing and therefore the obligations of the Patriot Act do not apply in respect of other offences.

This is, to an extent, a complication for the Money Laundering Reporting Officer (MLRO) operating in the US, since the rules relating to general money laundering and those applying to terrorist financing will essentially be different. There are a lot of clauses which relate to the role and authority of relevant agencies and courts to authorise or undertake surveillance or prosecution. These are not discussed here. However, other clauses are of interest to financial institutions and are worthy of review.

9.3.1 Civil Rights and Safety

By making safety a paramount consideration, the general stance of the Act is set within certain bounds which do differ from legislation enacted in other countries. Remember that reference will still need to be made to the Bank Secrecy Act in respect of other issues.

9.3.2 Asset Seizure

Section 106 of the Patriot Act modifies provisions relating to presidential authority under the International Emergency Powers Act to authorise the President, when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, to confiscate any property subject to US jurisdiction of a foreign person, organisation or country that he determines has planned, authorised, aided or engaged in such hostilities or attacks.

This actually provides an interesting challenge for a firm. It will clearly need to undertake enhanced due diligence in such cases and to provide data to agencies as required. The key question is whether such jurisdictions and nationals can be identified prior to their appearing on such a list to enable enhanced due diligence to take place. To some extent you would expect US banks to identify jurisdictions that the US might become engaged in hostilities with in advance, undertaking enhanced due diligence in all such cases.

Clearly, what is required is to know the jurisdiction of all customers, and this, of course, is required by general due diligence requirements. We would expect any US bank to maintain clear records in this regard.

9.3.3 Enhanced Surveillance Procedures

The clauses here amend the Federal criminal code to authorise the interception of wire, oral and electronic communications for the production of evidence of:

1. Specified chemical weapons or terrorism offences.
2. Computer fraud and abuse.

Why are chemical weapons specifically referred to and not, for example, nuclear weapons? Again, this really relates to the way in which the legislation was enacted. The rules set out the way that the authorities can legally undertake investigation procedures and also set out the various extraterritorial implications. Interestingly, the legislation permits the seizure of voice-mail messages under a warrant.

It also expands the scope of subpoenas for records of electronic communications to include the length and types of service utilised, temporarily assigned network addresses and the means and source of payment (including any credit card or bank account number).

In terms of the logistical issues, there is a statement that nothing in the Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance. Furthermore, a provider of this type of service, and a landlord, custodian or other person who furnishes these facilities or technical assistance, shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance.

This means that there is nothing additional that such firms are required to do; but if they are required to do anything then they will, in principle, be adequately compensated. In this, the regulations do not actually go as far as the regulations implemented in other countries where they are requiring electronic communication service providers to maintain records for a specified time period to facilitate investigations that might be required. Of course, whether there is any real compensation is another matter.

9.3.4 International Counter Money Laundering and Related Measures

This part of the Patriot Act amends Federal law governing monetary transactions to prescribe procedural guidelines under which the Secretary of the Treasury (the Secretary) may require domestic financial institutions and agencies to take specified measures if the Secretary finds that reasonable grounds exist for concluding that jurisdictions, financial institutions, types of accounts or transactions operating outside or within the United States are of primary money-laundering concern. The requirements include mandatory disclosure of specified information relating to certain correspondent accounts. It is these sections which actually impose the greatest burden on a financial institution.

The Act mandates the establishment of due diligence mechanisms to detect and report money-laundering transactions through private banking accounts and correspondent

accounts, issues already dealt with by the Wolfsberg Principles (Chapter 8). The Act essentially makes these principles mandatory, with the obligation on detection and subsequent reporting, although this is only in relation to terrorist financing.

The systems that will be implemented in practice clearly fall into two categories – systems that look for specific attributes (or scenarios) and those that look for unusual transactions (based on some system-defined inference process). Given the level of data that is maintained by a financial institution, most financial institutions will implement software to assist such suspicion recognition. This is further considered in Chapter 26. In the absence of such software, the responsibility will be on the financial institution to justify to its regulators that it is undertaking sufficient due diligence in this respect. This will require both significant Know Your Customer-style documentation and an audit trail which addresses cases that have been identified as a result of the investigative work conducted.

The Act prohibits US banks from maintaining correspondent accounts with foreign shell banks, one of the Financial Action Task Force (FATF) requirements which also appears within the Wolfsberg Principles.

Any bank needs to recognise that the extraterritorial arrangements can become a problem, since the Act establishes Federal jurisdiction over:

1. Foreign money launderers (including their assets held in the United States); and
2. Money that is laundered through a foreign bank.

In cases involving a US bank subsidiary, or a foreign bank with a branch in the US, the MLRO will need to be aware of these extraterritorial provisions and take such actions as are necessary to meet these requirements.

9.3.5 Forfeiture Rules

Section 319 of the Patriot Act authorises the forfeiture of money-laundering funds from interbank accounts. It also requires a financial institution, upon request of the appropriate Federal banking agency, to make available within 120 hours all pertinent information related to anti-money-laundering compliance by the institution or its customer.

Firms need to have regard to this 120-hour rule and ensure that their systems have the capability to provide information in the form required on a timely basis. In practice, this means having the major documents available that would need to be supplemented by the relevant information concerning a particular transaction or relationship. Information regarding the structure of reporting, approval procedures, the role of the MLRO, reporting procedures and other policies and procedures can easily be available at any time, so it is only information concerning a specific investigation which should cause any problem with the 120-hour limit.

Section 319 further grants the Secretary summons and subpoena powers over foreign banks that maintain a correspondent bank in the United States. This type of regulation will cause banks to consider what activities they carry out in the USA and why, perhaps resulting in less business being conducted within that jurisdiction.

Finally, there is also a requirement that a financial institution that is subject to these rules must terminate within ten business days any correspondent relationship with a foreign bank after receipt of written notice that the foreign bank has failed to comply with certain judicial proceedings. The civil penalties for failure to terminate such a relationship are also set out.

Clearly, correspondent banking relationships should be under regular review such that the firm can satisfy itself that it is being operated in accordance with international best practice and local jurisdictional regulation. We would direct you to the guidance from the FATF (Chapter 3) and also the JMLSG (Chapter 7) in this regard.

9.3.6 Identification, Record and Reporting Requirements

The record and reporting requirements appear within Section 321 of the Patriot Act. It subjects to recording and reporting requirements monetary instrument transactions conducted by:

1. Any credit union; and
2. Any futures commission merchant, commodity trading advisor or commodity pool operator registered, or required to register, under the Commodity Exchange Act.

Section 325 then authorises the Secretary to issue regulations to ensure that concentration accounts of financial institutions are not used to prevent association of the identity of an individual customer with the movement of funds of which the customer is the direct or beneficial owner.

In addition, Section 326 directs the Secretary to issue regulations prescribing minimum standards for financial institutions regarding customer identity in connection with the opening of accounts.

9.3.7 Bank Holding Company Act

Section 327 of the Patriot Act amends the Bank Holding Company Act of 1956 and the Federal Deposit Insurance Act to require consideration of the effectiveness of a company or companies in combating money laundering during reviews of proposed bank shares, acquisitions or mergers.

Section 328 then implements another of the FATF special recommendations by directing the Secretary to take reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the United States and other countries, with the information to remain with the transfer from its origination until the point of disbursement.

9.3.8 Bank Secrecy Act Amendments and Related Improvements

Among the various Acts that the Patriot Act amended, one was the Bank Secrecy Act, which was amended to revise requirements for civil liability immunity for voluntary financial institution disclosure of suspicious activities. For example, it authorises the inclusion of suspicions of illegal activity in written employment references. Of course,

were there to be such a suspicion then a formal report would have been made by the firm, which would normally require total secrecy. Whether anyone has actually included any such information in a reference we somewhat doubt, and suggest that the firm would instead choose to make a report to the relevant agency.

Section 356 of the Patriot Act instructs the Secretary to:

1. Promulgate regulations requiring registered securities brokers and dealers, futures commission merchants, commodity trading advisors and commodity pool operators to file reports of suspicious financial transactions.
2. Report to Congress on the role of the Internal Revenue Service in the administration of the Bank Secrecy Act.
3. Share monetary instrument transaction records upon a request from a US intelligence agency for use in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.

Section 359 then further extends these requirements to cover any licensed sender of money or any other person who engages as a business in the transmission of funds, including through an informal value transfer banking system or network (e.g. hawala).

9.3.9 Penalties

The Patriot Act also increases the penalties that may be levied in respect of terrorist financing. Section 363 increases to $1 million the maximum civil penalties (from the rather dated $10,000) and criminal fines (currently $250,000) for money laundering. It also sets a minimum civil penalty and criminal fine of double the amount of the illegal transaction. Section 365 amends Federal law to require reports relating to coins and currency of more than $10,000 received in a non-financial trade or business.

You might well consider that the new penalty is still rather low given the seriousness of the potential issue.

9.3.10 Currency Crimes

The Patriot Act also establishes a bulk cash smuggling felony of the knowing concealment and attempted transport (or transfer) across US borders of currency and monetary instruments in excess of $10,000, with intent to evade specified currency-reporting requirements.

Further extraterritorial requirements sit in Section 377. This section grants the United States extraterritorial jurisdiction where:

1. An offence committed outside the United States involves an access device issued, owned, managed or controlled by a financial institution, account issuer, credit card system member or other entity within US jurisdiction; and
2. The person committing the offence transports, delivers, conveys, transfers to or through or otherwise stores, secretes or holds within US jurisdiction any article used to assist in the commission of the offence or the proceeds of such offence or property derived from it.

This is quite a broad requirement, but do notice the use of the word "and". If the article was not held within the USA, then this rule would not apply.

9.3.11 Strengthening the Criminal Laws against Terrorism

The Patriot Act also amends the Federal criminal code to prohibit specific terrorist acts or otherwise destructive, disruptive or violent acts against mass-transportation vehicles, ferries, providers, employees, passengers or operating systems. Section 803 prohibits harbouring any person knowing, or having reasonable grounds to believe, that such person has committed, or is about to commit, a terrorism offence, while Section 804 establishes Federal jurisdiction over crimes committed at US facilities abroad.

Much of this, in effect, duplicates existing regulation.

9.4 THE BANK SECRECY ACT 1970

Remember that the Patriot Act is purely focussed on terrorist financing. It is the Bank Secrecy Act that addresses the main money-laundering deterrence regulation in the USA.

The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its implementing regulation, 31 CFR 103, is a tool the US government uses to fight drug trafficking, money laundering and other crimes. Congress enacted the BSA to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, criminal activity. The Office of the Comptroller of the Currency (OCC) monitors national bank compliance with the BSA and 31 CFR 103.

More than 170 crimes are listed in the Federal money-laundering statutes. They include drug trafficking, gunrunning, murder for hire, fraud, acts of terrorism and the illegal use of wetlands. The list also includes certain foreign crimes. Therefore, a financial institution must educate its employees, understand its customers and their businesses and have systems and procedures in place to distinguish routine transactions from ones that potentially give rise to a level of suspicious activity.

US penalties for money laundering can be severe. Individuals, including bank employees, convicted of money laundering face up to 20 years in prison for each money-laundering transaction conducted. Businesses, including banks and individuals, face fines up to the greater of $500,000 or twice the value of the transaction. Any property involved in the transaction or traceable to the proceeds of the criminal activity, including loan collateral, personal property and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate) may be subject to forfeiture. In addition, banks risk losing their charter, and bank employees risk being removed and barred from the industry.

Under the provisions of the Controlled Substances Act of 1978, the Money Laundering Control Act of 1986 and the Anti-Drug Abuse Act of 1988, real or personal property traceable to illegal drug sales or purchased with laundered money is subject to government seizure and forfeiture. Occasionally, seized property is collateral for bank loans.

Therefore, a bank must obtain and confirm enough information about its customers to protect its loan collateral from loss due to government forfeiture.

9.4.1 Independent Testing of Compliance

The bank's internal or external auditors should be able to:

- Attest to the overall integrity and effectiveness of management systems and controls, and BSA technical compliance.
- Test transactions in all areas of the bank, with emphasis on high-risk areas, products and services to ensure the bank is following prescribed regulations.
- Assess employees' knowledge of regulations and procedures.
- Assess adequacy, accuracy and completeness of training programmes.
- Assess adequacy of the bank's process for identifying suspicious activity.

Internal review or audit findings should be incorporated into a board and senior management report and reviewed promptly. There then needs to be appropriate follow-up. Of course, the guidance on internal audit is best found in the Bank for International Settlements paper *The Internal Audit Function in Banks* published in June 2012 and available at: http://www.bis.org/publ/bcbs223.pdf.

Of course, the Bank for International Settlements, just like the Financial Action Task Force and the Wolfsberg Group, does not have any direct legal status, meaning that its requirements do not need to be implemented into local law or regulation. It does, however, represent international best practice in this area and is a useful form of reference.

9.4.2 Compliance Officer

Under the BSA, a US national bank must designate a qualified bank employee as its BSA Compliance Officer, to have day-to-day responsibility for managing all aspects of the BSA compliance programme and compliance with all BSA regulations. The BSA Compliance Officer may delegate certain BSA compliance duties to other employees, but they must not delegate compliance responsibility.

The bank's board of directors and senior management must ensure that the BSA Compliance Officer has sufficient authority and resources to administer effectively a comprehensive BSA compliance programme.

Notice that the term used is Compliance Officer, not the more internationally recognised term Money Laundering Reporting Officer (or MLRO).

9.4.3 Training

The BSA requirement in this regard is that banks must ensure that appropriate bank personnel are trained in all aspects of the regulatory requirements of the BSA and the bank's internal BSA compliance and anti-money-laundering policies and procedures.

An effective training programme includes provisions to ensure that all bank personnel, including senior management, who have contact with customers (whether in person or by phone), who see customer transaction activity or who handle cash in any way, receive appropriate training.

Those employees include persons involved with:

- Branch administration
- Customer service
- Lending, private or personal banking
- Correspondent banking (international and domestic)
- Trusts
- Discount brokerage
- Funds transfer
- Safe deposit/custody
- Vault activities.

Training is required to be ongoing and must incorporate current developments and changes to relevant regulations. New and different types of money-laundering schemes that have evolved in the market and might involve customers and financial institutions should also be addressed in this training. It also should include examples of money-laundering schemes and cases, tailored to the audience, and the ways in which such activities can be detected or resolved.

Training should focus on the consequences of an employee's failure to comply with established policy and procedures (e.g. fines or termination). Programmes should provide personnel with guidance and direction in terms of bank policies and available resources.

There are, of course, online products available, but in our opinion they would need to be supported by documented examinations (perhaps also online) to formally document that the knowledge gained from the online training had been assimilated properly.

9.4.4 Reporting Requirements

The BSA regulations require all financial institutions to submit five types of report to the government:

1. **IRS Form 4789 Currency Transaction Report (CTR):** A CTR must be filed for each deposit, withdrawal, exchange of currency or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of more than $10,000.

   Multiple currency transactions must be treated as a single transaction if the financial institution has knowledge that: (a) they are conducted by, or on behalf of, the same person; and, (b) they result in cash received or disbursed by the financial institution

of more than $10,000 (31 CFR 1010.100(t), formerly 31 CFR 103.11(n)) (31 CFR 1010.311, formerly 31 CFR 103.22(b)(1)).

2. **US Customs Form 4790 Report of International Transportation of Currency or Monetary Instruments (CMIR):** Each person (including a bank) who physically transports, mails or ships, or causes to be physically transported, mailed, shipped or received, currency, traveller's cheques and certain other monetary instruments in an aggregate amount exceeding $10,000 into or out of the United States must file a CMIR (31 CFR 1010.340, formerly 31 CFR 103.23).
3. **Department of the Treasury Form 90-22.1 Report of Foreign Bank and Financial Accounts (FBAR):** Each person (including a bank) subject to the jurisdiction of the United States having an interest in, signature or other authority over, one or more bank, securities or other financial accounts in a foreign country must file an FBAR if the aggregate value of such accounts at any point in a calendar year exceeds $10,000 (31 CFR 1010.350, formerly 31 CFR 103.24).
4. **Treasury Department Form 90-22.47 and OCC Form 8010-9, 8010-1 Suspicious Activity Report (SAR):** Banks must file a SAR for any suspicious transaction relevant to a possible violation of law or regulation (31 CFR 1020, formerly 31 CFR 103.18) (12 CFR 12.11).
5. **Designation of Exempt Person Form TDF 90-22.53:** Banks must file this form to designate an exempt customer for the purpose of CTR reporting under the BSA (31 CFR 1020.315, formerly 31 CFR 103.22(d)). In addition, banks use this form annually to renew exemptions for eligible non-listed business and payroll customers (31 CFR 1020.315).

9.4.5 Record-keeping Requirements

The BSA regulations require banks to maintain a variety of records to ensure, among other things, that transactions can be reconstructed. Two of these record-keeping requirements are discussed below. Detailed descriptions of these and other record-keeping requirements for banks can be found in 31 CFR 103. The retention period for all records required to be kept under the BSA regulations is five years.

Monetary Instrument Sales Records

A bank must retain a record of each *cash* sale of bank cheques, drafts, cashier's cheques, money orders and traveller's cheques between $3,000 and $10,000 inclusive. These records must include evidence of verification of the identity of the purchaser and other information (§ 1010.415, formerly 31 CFR 103.29).

Funds Transfer Record-keeping and Travel Rule Requirements

A bank must maintain a record of each funds transfer of $10,000 or more which it originates, acts as an intermediary for or receives. The amount and type of information a bank must record and keep depends upon its role in the funds transfer process. Also, a bank that acts as an originator or intermediary for a funds transfer must pass certain information along to the next bank in the funds transfer chain (§ 1010.311, formerly 31 CFR 103.33 (e) and (g)).

Under the phase II rule, twelve months of account history must exist before the customer can be exempted. The months do not have to be consecutive, but should be recent.

- The customer must engage frequently in large currency transactions (eight or more a year).
- The customer must be incorporated or organised under the laws of the United States or a state, or registered or eligible to do business in the United States.
- Annually, banks must verify whether each exemption continues to meet the exemption eligibility requirements. Banks may develop their own methods and procedures for this annual review.
- Biennially, banks must file the "Designation of Exempt Person" form for each non-listed business and payroll customer.
- As part of the biennial filing of the "Designation of Exempt Person" form, the bank must certify that, as part of its BSA compliance programme, it has policies and procedures in place for identifying, reviewing and reporting suspicious activity in accordance with the SAR filing requirements (31 CFR 1020, formerly 31 CFR 103.18).

9.4.6 Suspicious Activity Reporting Requirements

An effective BSA compliance programme must also include controls and measures designed to identify and report suspicious transactions in a timely manner. A financial institution must apply due diligence to be able to make an informed decision about the suspicious nature of a particular transaction and whether to file a suspicious activity report (SAR).

SARs must be filed with the appropriate authority within prescribed time frames following the discovery of:

- Insider abuse involving any amount.
- Violations of Federal law aggregating $5,000 or more when a suspect can be identified.
- Violations of Federal law aggregating $25,000 or more regardless of a potential suspect.
- Transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA if the bank knows, suspects or has reason to suspect that the transaction:
  - involves funds from illegal activities or is intended or conducted to hide or disguise illicit funds or assets as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law;
  - is designed to evade any of the BSA regulations; or
  - has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The rules continue to provide additional guidance regarding the identification of potential money laundering, repeating much of the material already included within this handbook.

Clearly, the policies and procedures implemented within a US bank need to comply with all of these rules and regulations. The complexity of the changing regulatory structures in the US and the lack of consolidated legislation does provide a higher level of complexity than occurs in other markets. A consequence of this is that it is more likely that a US bank will employ specialist legal resources in this arena than would be the case in other countries.

It is, of course, the board that remains responsible for the operation of the bank, regardless of the business area that it is involved with. Accordingly, the board should be trained with regard to these requirements, actively involved with the programme and, in particular, should approve the policies and procedures adopted.

At the time of writing there is discussion of new regulations being implemented in the UK to ensure that the FATF Recommendations are clearly and fully implemented into US legislation, but at present the legislative changes have not been drafted.