The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1359-0790.htm

The impact of terrorism on financial markets

R. Barry Johnston and Oana M. Nedelescu
Monteray and Fiscal Affairs Department, International Monetary Fund, Washington, District of Columbia, USA

Abstract

Purpose – The paper seeks to draw lessons for effective policy and regulatory responses to protect financial systems in the face of terrorist attacks.

Design/methodology/approach – The paper presents data on the reaction of financial markets to the terrorist attacks in New York (2001) and Madrid (2004). It describes the authorities' crisis management responses and analyses their effectiveness. The paper describes the subsequent regulatory responses to protect the financial systems from abuse by terrorists.

Findings – Diversified, liquid, and sound financial markets were efficient in absorbing the shocks of terrorist attacks when supported by well organized crisis management responses.

Research limitations/implications – The paper is limited in its coverage to the reaction of the financial markets to the 11 September 2001, terrorist attacks in New York, and 11 March 2004, attacks in Madrid.

Practical implications – The paper highlights the importance of effective contingency planning by the authorities and financial firms in mitigating the risks of disruption from terrorist attacks.

Originality/value – This paper provides an overview of the issues, challenges and responses in dealing with the risks posed by terrorism to financial systems. It combines empirical evidence with an institutional perspective, and notes some of the regulatory challenges in combating terrorist finance.

Keywords Terrorism, Financial markets

Paper type Research paper

1. Introduction

Financial institutions could be involved in financial crime as victim, as perpetrator, or as instrumentality: financial institutions can be subject to different types of fraud or abuse; they can directly commit financial crimes; or they can be used by third parties to commit crime (International Monetary Fund, 2001a). Similarly, terrorism can have multiple implications for financial markets. First, as demonstrated by the attacks of 11 September 2001 on the World Trade Center financial markets can be, directly and indirectly, the victim of terrorism. Second, financial institutions can be specially set up to support terrorism. Third, financial institutions can be used, without their knowledge, to channel terrorist funds.

The present paper examines cases where financial markets became, directly or indirectly, the victim of terrorist acts, the consequences of those acts on the financial markets, and the policy and regulatory responses. Section 2 discusses some of the direct and indirect economic consequences of terrorism; Section 3 reviews the reaction of the financial markets to the 11 September 2001, terrorist attacks in New York, and 11 March 2004, attacks in Madrid; Section 4 examines the authorities' crisis management

The views expressed in this paper are those of the author(s) and do not necessarily represent those of the IMF or IMF policy.

Journal of Financial Crime
Vol. 13 No. 1, 2006
pp. 7-25

1359-0790
DOI 10.1108/13590790610641233

responses to the attacks on the financial markets considered; Section 5 examines the regulatory responses; and Section 6 concludes.

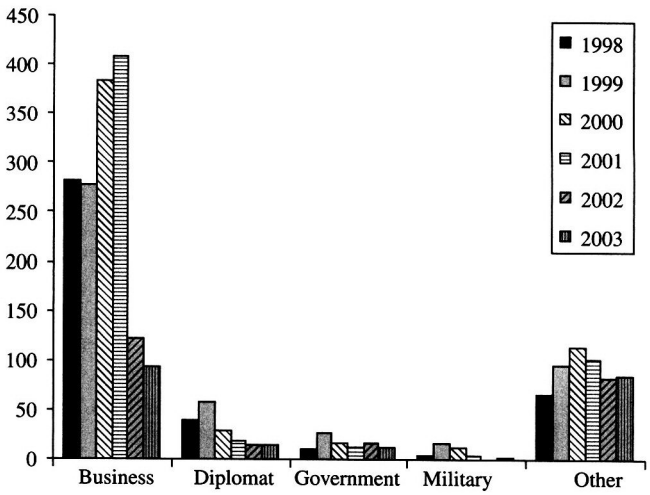
2. Economic consequences of terrorism

In recent years, terrorism has shown new patterns, shifting increasingly from military targets to civilian targets, including individuals and business activities. Figure 1 shows that business facilities have represented, by far, the preferred target of international terrorist attacks since 1998.

Recent terrorist attacks affected both the national and the global economy. The economic consequences can be largely broken down into short-term direct effects; medium-term confidence effects and longer-term productivity effects.

The direct economic costs of terrorism, including the destruction of life and property, responses to the emergency, restoration of the systems and the infrastructure affected, and the provision of temporary living assistance, are most pronounced in the immediate aftermath of the attacks and thus matter more in the short run. Direct economic costs are likely to be proportionate to the intensity of the attacks and the size and the characteristics of the economy affected. While the 11 September attacks on the United States caused major activity disruption, the direct economic damage was relatively small in relation to the size of the economy. The direct costs resulting from the terrorist attacks were estimated by the Organization for Economic Co-operation and Development at $27.2 billion ($14 billion for the private sector, $1.5 billion for the state and local government enterprises, $0.7 billion for the US federal government, and $11 billion for rescue and clean-up operations) (Bruck and Wickstrom, 2004), which represented only about 1/4 percent of the US annual GDP.

The indirect costs of terrorism can be significant and have the potential to affect the economy in the medium term by undermining consumer and investor confidence. A deterioration of confidence associated with an attack can reduce the incentive to spend as opposed to save, a process that can spread through the economy and the rest



Source: U.S. Department of State (2003), ref. 2 below

Figure 1.
Number of facilities struck by international attacks, 1998-2003

of the world through normal business cycle and trade channels. Likewise, falling investor confidence may trigger a generalized drop in asset prices and a flight to quality that increases the borrowing costs for riskier borrowers (International Monetary Fund, 2001b). The size and distribution of the effects over countries, sectors, and time would depend on a range of factors, including the nature of the attacks, the multiplier effects, the type of policies adopted in response to the attacks, and the resilience of the markets (Bruck and Wickstrom, 2004).

The 11 September attacks primarily affected the major industrial countries through a fall in demand generated by the loss in confidence about the economy and its impact on output. Emerging markets were affected by slowing external demand and a flight to quality in financial markets. Other developing countries may have been affected through commodity markets (International Monetary Fund, 2001b).

Despite having been the direct target of terrorism, which materially affected the market infrastructure and operations, following the 11 September attacks, the financial markets demonstrated resilience and a capacity to return to normalcy quickly (see below). This allowed the financial markets to perform one of their key functions: that of digesting the information on the economic and financial impact of the terrorist attacks after an initial shock and efficiently incorporating the information into asset prices so that it could be integrated into decisions about the future.

Financial instruments involve commitments over time and, therefore, price and provide a hedge against uncertainty. While the initial effect of any major crisis may involve a financial market overreaction because of higher levels of uncertainty, as the new information is being assessed and absorbed, once the long-term impact of the crisis is assessed, markets return to their pre-crisis condition. Thereafter, financial markets shift up or down according to investors' perceptions of how the crisis will be resolved (Taylor, 2004).

Finally, over the longer term, there is a question of whether the attacks can have a negative impact on productivity by raising the costs of transactions through increased security measures, higher insurance premiums, and the increased costs of financial and other counterterrorism regulations.

3. Impact of the terrorist attacks on financial markets

As noted above, financial markets have been directly and indirectly the victims of terrorist attacks. Striking at the core of the world's main financial center, the terrorist attacks of 11 September aimed at undermining the stability of the US and international financial system. In the aftermath of the attacks, the financial markets were not only confronted with major activity disruptions caused by the massive damage to property and communication systems, but also with soaring levels of uncertainty and market volatility.

Numerous key market players had substantial operations in or around the World Trade Center that were destroyed or damaged in the attacks, causing a widespread closure of the New York financial markets. Above all, the financial industry suffered a huge and tragic loss of life, accounting for over 74 percent of the total civilian casualties in the World Trade Center attacks (Lacker, 2004).

The biggest disruption to the trading infrastructure was caused by damage to the communications system of the world's largest custodian and settlement bank, the Bank of New York (International Monetary Fund, 2001b) Both Bank of New York and J.P.

Morgan Chase, the two main clearing banks for government securities, had to relocate to backup sites as their main centers of operations were located just a few blocks from the World Trade Center (Lacker, 2004). Manual processing of securities and payment transactions resulted in significant delays in clearing and settlement, raising uncertainty about the completion of trades and demand for liquidity (International Monetary Fund, 2001b).

The government securities market was severely affected by the loss of the largest interdealer broker, Cantor Fitzgerald, and other smaller brokers whose offices were located in the World Trade Center (Lacker, 2004). While confronted with the impossibility of communicating by phone (the interdealer market operates by phone and screen-based trading systems) as phone contacts with brokers were disrupted, traders turned to online platforms, including BrokerTec, a consortium of primary dealers, and Cantor Fitzgerald's own eSpeed Inc., which was able to continue operating out of the firm's London offices (Lacker, 2004).

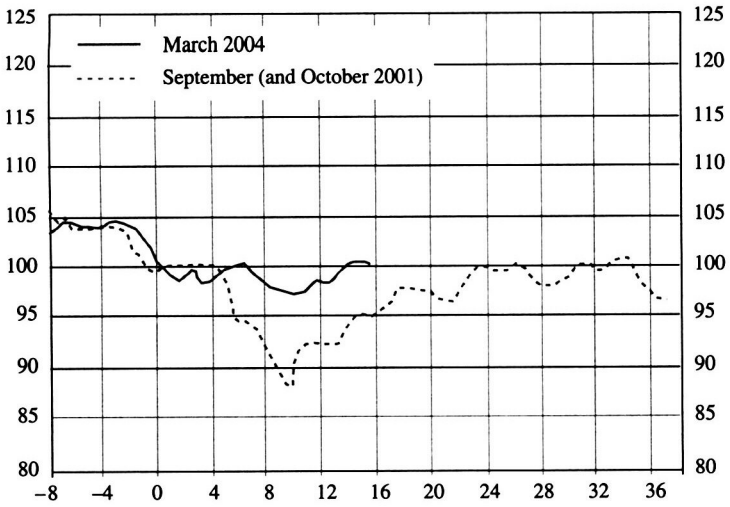
Other markets were affected as well. On the repo market, the initial incapacity to trade caused by damage to trading infrastructure, combined with the growing reluctance of market participants to lend out securities, resulted in a lack of supply that demanded immediate intervention by the authorities (International Monetary Fund, 2001b). Also, several federal funds brokers were disabled in the attacks, some ATM networks crashed entirely, and the facilities of the New York Board of Trade were destroyed (Lacker, 2004). Because of widespread disruption in the payment systems, many market participants became unable or unwilling to execute payments, causing a growing liquidity shortage.

A number of alarming signals prompted an immediate response by the Federal Reserve as discussed in the following section. First, the large buildup of Federal Reserve account balances ($120 billion – almost ten times the pre-11 September levels) was limited to a few banks, which meant that others were running huge negative positions and were in acute need of liquidity (Ferguson, 2003). Second, on 11 September, the number of transfers though the Federal Reserve's large-value electronic payment system (Fedwire) was down more than 40 percent and the total value was down 25 percent (Ferguson, 2003).

The insurance industry was also affected by large claims resulting from the attacks that generated losses estimated at more than $50 billion (PricewaterhouseCoopers, 2001). Further evidence, however, indicates that by and large insurers have suffered less as they were able to take advantage of the heightened uncertainty by raising premiums (International Monetary Fund, 2001b). In addition, some insurers were able to get exempted from paying some of the claims stemming from the attacks by using act-of-war clauses (Flynn, 2002).

On the capital markets, because of the timing of the attacks (around 9:00 a.m. eastern daylight time), the New York Stock Exchange and the NASDAQ Stock Market never opened for trading on 11 September. The US securities markets resumed trading on 17 September, following close consultations between the private sector and the Securities and Exchange Commission. The decision on when to reopen the markets took into consideration factors such as the safety of the personnel returning to work, and the viability of the infrastructure and communication systems[1].

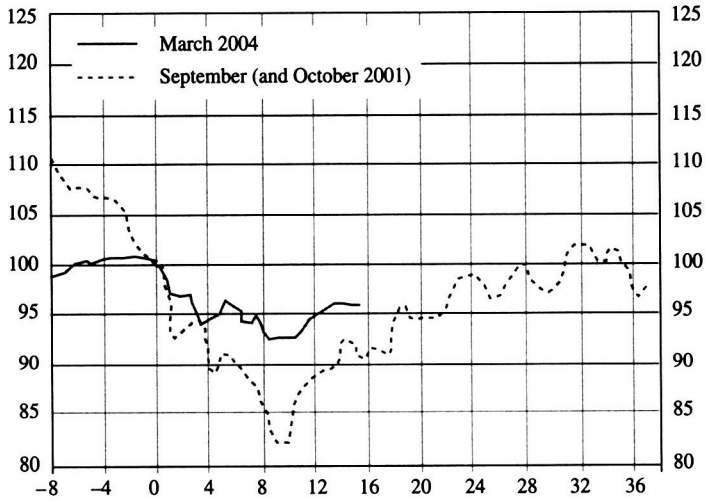
In terms of market volatility, the US stock markets were down overall during the first day of trading and continued to drop in the following days. Between 17 and



Note: "0" marks 10 March 2004 and 10 September 2001. The horizontal axis shows the number of working days.

Source: European Central Bank, Monthly Bulletin, April 2004.

Figure 2.
Standard and Poor's 500 index



Note: "0" marks 10 March 2004 and 10 September 2001. The horizontal axis shows the number of working days.

Source: European Central Bank, Monthly Bulletin, April 2004.

Figure 3.
Dow Jones EURO STOXX Index

21 September, Standard and Poor's 500 index fell by 11.6 percent (Figure 2) and NASDAQ index by 16.1 (International Monetary Fund, 2001b).

The impact of the 11 September attacks was visible worldwide on the major equity markets, which experienced sharp and rapid declines, demonstrating that market participants perceived the event as a global shock. The decline in the European stock markets, which started operating before the US markets were opened, was even greater after 17 September, because of spillover effects. All in all, the Dow Jones Euro STOXX index was down 17.3 percent between 11 and 21 September (Figure 3) (International Monetary Fund, 2001b).

In comparison with the impact of the 2001 terrorist attacks on the United States, the effects of the 11 March 2004, terrorist attacks on Spain were felt much less by the capital markets, and by the financial markets in general (Figures 2 and 3). In the euro area, the Dow Jones EURO STOXX fell by about 3 percent on 11 March, and continued to drop during the following days but recovered almost completely by the end of the month. Similarly, after a small decline, the Standard and Poor's 500 returned to the pre-11 March levels in less than a month.

Figures 2 and 3 demonstrate, however, that in the aftermath of both terrorist attacks investor confidence deteriorated beyond the national boundaries because of contagion effects. Likewise, in both cases the US markets seem to have suffered less and also recovered faster from the attacks, proving enhanced resilience. Nonetheless, once the initial shock passed, both markets bounced back within weeks to pre-11 September levels and generally continued to rise thereafter.

The differences in stock market behavior in the aftermath of the two episodes of terrorist attacks have several possible explanations. First, while the attacks in New York raised uncertainty about the stability of the global financial system, the attacks on Spain were perceived as mostly having a regional effect. Second, unlike the events of 11 September 2001, which occurred in the midst of a global economic downturn, the terrorist attacks in Madrid occurred at a time when the world economy was growing strongly (European Central Bank, 2004). The market uncertainty was even stronger in the first case as doubts raised about US capacity to drive the global economy out of recession.

Finally, the terrorist attacks in Madrid did not directly target the financial markets and, therefore, did not damage their infrastructure and communication systems. However, as noted above, despite major capital losses in the immediate aftermath of 11 September, most financial firms affected by the attacks were able to revert to backup sites and effectively resume their activity instantly or within days. The prompt intervention of the Federal Reserve in cooperation with other authorities also resolved the liquidity shortage and managed to maintain business and consumer confidence in the United States and abroad.

Further evidence on the impact of terrorism on financial markets is offered by a number of recent studies, confirming the observations above. Chen and Siems attempt to statistically test the significance of the 11 September attacks on global capital markets by measuring the deviation of index returns from their average (Chen and Siems, 2004). When the return deviation is large and statistically significant, the authors conclude that the market saw the events as important.

Table I shows the abnormal returns in the aftermath of the 11 September terrorist attacks for banking/financial sector indices from 14 global capital markets. As depicted in Table I, the event had a widespread negative impact on all the markets

Global Stock markets' banking/financial sectors	Event-day AR (percent)	6-day CAR[a] (percent)	11-day CAR[a] (percent)	Days to rebound [b]
NYSE	−4.79	−6.69	−0.45	13
London	−10.09	−8.64	−14.14	22
Frankfurt	−10.06	−14.54	−15.79	42
Europe-Bloomberg	−8.54	−11.50	−14.82	40
Helsinki	−6.17	−6.43	−11.35	31
Norway	−5.79	−14.18	−25.55	107
Tokyo	−6.50	−1.70	−12.18	6
Hong Kong	−7.87	−11.02	−14.34	30
Korea	−13.33	−13.78	−19.84	28
Jakarta	−2.83	−3.73	−6.23	86
Kuala Lampur	−5.20	−13.36	−18.68	65
Australia	−3.98	−9.46	−11.07	26
New Zealand	−3.67	−11.39	−14.93	33
Johannesburg	−5.27	−14.43	−11.00	162

Notes: [a]CAR denotes cumulative average abnormal returns; [b]Number of trading days for the market to return to pre-attack level
Source: Chen and Siems (2004)

Table I.
Average abnormal returns on global capital markets following the 11 September terrorist attacks

considered. Surprisingly, the impact was smaller on the US market, which displayed the least adverse abnormal returns 11 days after the attacks (11-day CAR), and also underwent the second fastest recovery. Chen and Siems also examine the financial markets' reaction in other periods of extreme risk aversion. They find evidence that US capital markets rebounded and stabilized quicker than other markets in the world following the 11 September attacks than in earlier periods when surprise terrorist/military attacks shocked global markets.

The authors find that one possible reason for the more limited impact of the terrorist attacks on the US markets (despite the fact that they were the actual terrorist target) stems from the Federal Reserve's accommodative policy, which was able to calm and stabilize the economy through the US banking/financial sector. Also, the authors find evidence that the increased market resilience can be at least partially explained by a banking/financial sector that provides adequate liquidity to promote market stability and stifle panic.

The main conclusion, however, is that financial markets were efficient in absorbing the shocks determined by terror attacks and continued to perform their functions in an effective way. A similar conclusion is reached by Eldor and Melnick in a study on how stock and foreign exchange markets react to terror (Eldor and Melnick, 2004). Referring to the 11 September attacks, SEC notes that "[The markets] did what they do best: they assessed, and responded to the crisis rationally. Unlike human beings, capital markets are capable of absorbing great shocks quickly"[1].

In terms of the lessons that can be drawn for the financial markets, at a general level, having diversified forms of risk intermediation makes the financial system more robust (Ferguson, 2003). At a practical level, the direct attacks on the financial sector of 11 September underlined the importance of having operative business continuity plans across the financial sector as a measure to counter the operational risk arising from severe activity disruption.

In the aftermath of the 11 September attacks, most of the financial firms directly affected by the attacks were able to relocate to backup sites and resume their operations within a short period of time. Thereafter, a large majority of the financial market players recognized that the preparations for Y2 K proved to be of value in the quite different context of 11 September. The serious consideration that the Y2 K issue received throughout the financial industry brought considerable improvement in the backup IT and communication systems helping market participants withstand the 11 September crisis (Ferguson, 2003).

4. Authorities' response

The 11 September terrorist attacks on the US financial system underscored the critical importance of the authorities' response in heading off systemic concerns. In the aftermath of the attacks, the Federal Reserve acknowledged that an immediate and firm policy response was key for restoring confidence within and outside the financial markets.

One of the first messages to transcend the chaos and panic of 11 September was that "[t]he Federal Reserve System is open and operating. The discount window is available to meet liquidity needs". The Federal Reserve promptly deployed a wide range of instruments needed to provide sufficient liquidity, to ensure that the payment systems were operational, and to keep markets open (Ferguson, 2003).

The policy response of the Federal Reserve included unprecedented liquidity injections, estimated at more than $100 billion (Lacker, 2004). Liquidity instruments ranged from extensive discount window lending and open market operations to waiving overdraft fees and decreasing the intended federal funds and discount rates (for a comprehensive account of the Federal Reserve's action).

Moreover, to help foreign financial institutions cope with the liquidity shortage, the Federal Reserve arranged for the availability of reciprocal currency facilities of up to $80 billion though swaps with the European Central Bank and the Bank of England, and raised the ceiling of a preexisting swap with the Bank of Canada.

In addition, various steps were taken to render market mechanisms and systems operative. Although the US airspace was closed for several days after the attacks, preventing the timely collection of checks by their home bank, the Federal Reserve continued to provide credit for checks on the usual availability schedules (Ferguson, 2003). Likewise, the Federal Reserve encouraged state member banks and bank holding companies to work flexibly with customers affected by the disaster and contact their regulator to discuss ways to respond to the distress (Ferguson, 2003).

However, ensuring the financial markets' return to normalcy required more than the Federal Reserve's quick and efficient action. Close cooperation and coordination with other domestic and foreign authorities was necessary. The US Securities and Exchange Commission helped the markets overcome the crisis by relaxing trading rules on securities lending and share repurchases (International Monetary Fund, 2001b). Similar to the Federal Reserve, the Securities and Exchange Commission left the communication channels open and kept the public fully and timely advised[1].

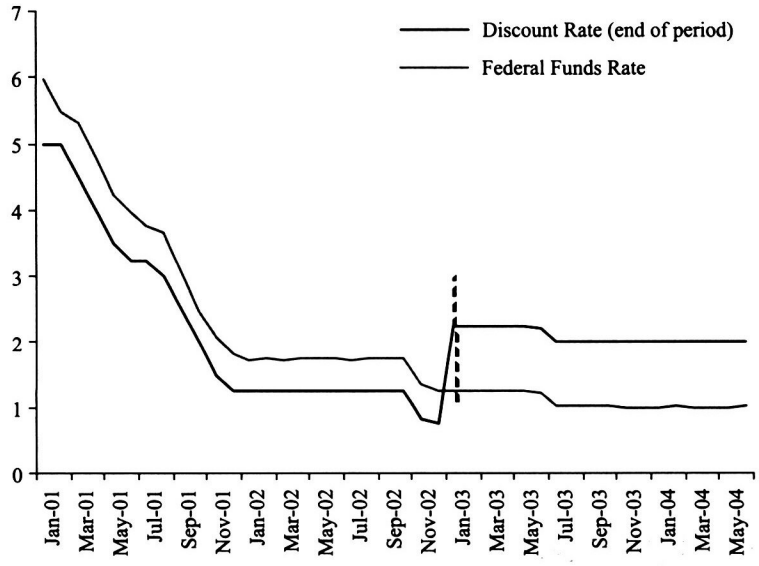
Also, while the monetary and financial authorities focused on maintaining financial stability, other government agencies took the initiative to introduce fiscal stimulus to bail out industries affected by the attacks. The insurance and airline industries received direct government assistance in the immediate wake of the attacks. The US

administration and the Congress announced their intention to act as an "insurer of last resort" to cover claims that private insurance companies could not or would not pay (Flynn, 2002). A year after the attacks of 11 September, a "Terrorism Risk Insurance Act" was passed, providing for a transparent system of shared public and private compensation for insured losses resulting from acts of terrorism.

In the short and medium terms, more economic stimulus was needed to help the economy recover as the recession deepened further after the terrorist attacks. The global slowdown that had started most prominently in the US in 2000 had, by mid-2001, become a synchronized downturn across all major regions of the world, leaving them particularly vulnerable to a negative impulse (International Monetary Fund, 2001b). The Federal Reserve continued to lower the targeted federal funds and discount rates in the following weeks an additional 1.25 points. Further downward adjustments followed in 2002 and 2003 (Figure 4). Also, expansionary fiscal policies have been implemented to help the economy recover.

At the international level, a coordinated effort was made to support the global payments system, strengthen confidence, and shore up financial markets. Monetary authorities from major economies such as Canada, the euro area, Japan, Switzerland, and the United Kingdom directly injected large amounts of liquidity and made immediate interest rates cuts in response to the Federal Reserve's measures (International Monetary Fund, 2001b). These actions were subsequently followed by a number of other economies, including Denmark, Hong Kong SAR, Korea, New Zealand, and Sweden (International Monetary Fund, 2001b).

Within a short period of time of the attacks in New York, a majority of countries stepped up the fight against terrorism in an effort to maintain international peace and security. Further actions were taken globally in the fight against terrorism and terrorism financing, as discussed in the next section.



Source: IMF, International Financial Statistics, see ref. 40

Figure 4.
Federal reserve instruments

In contrast with the wide range of monetary, financial, and fiscal measures undertaken at the national and international levels in the aftermath of the 11 September attacks in New York, the terrorist attacks that took place in Madrid, on 11 March 2004, called for little economic policy response. While the human loss was equally tragic, the effects of the terrorist attacks on the Spanish and global financial markets were rather muted and, therefore, no special intervention was required (European Central Bank, 2004).

The European Central Bank, the monetary authority of the euro area, which includes Spain, announced on 1 April 2004, that the main intervention rates (minimum bid rate on the main refinancing operations and the interest rates on the marginal lending facility and the deposit facility) were to remain unchanged (European Central Bank, 2004). Also, in a period of strong economic recovery, no fiscal stimulus or other economic measures were deemed necessary, other than providing aid to victims and facilities directly struck by the terrorist attack.

The dramatic episodes depicted above underscore a number of key lessons related to financial crisis containment. First, the experience underlined the importance of the central bank's role in safeguarding the stability of the financial system during crisis. From acting as a lender of last resort, to maintaining an open and transparent dialogue with the regulated entities, the Federal Reserve played a paramount role in restoring the markets' confidence and helping them perform their functions.

Of particular importance in this context was the role of the Federal Reserve as lender of last resort (Ferguson, 2003). Past experience has shown that deposit insurance or suspension of payments are neither necessary nor sufficient to prevent banking crises. The Federal Reserve's prompt action as a lender of last resort in the aftermath of the 11 September attacks events allowed banks to manage the acute liquidity shortage, and to prevent public panic and possible bank runs.

A second key lesson was the critical importance of cooperation and coordination among domestic authorities and across borders. In the US markets, there was synchronized action by the US regulatory community and other stakeholders that allowed markets to return to normal functioning quickly and effectively (Ferguson, 2003). Some of these actions included non-traditional emergency measures. Both the Federal Reserve and the Securities and Exchange Commission waived the observance of a number of rules by the regulated entities and offered their expertise in helping them overcome the distress caused by the attacks. As noted above, the coordination extended internationally, as key central banks stood ready to intervene to provide the necessary liquidity to support the payments system. The timely provision of liquidity by central banks and the relatively healthier position of financial intermediaries were instrumental in containing financial contagion across industrial and emerging markets and across asset classes.

5. Regulatory perspective

Besides providing timely and effective support as needed in the aftermath of terrorist attacks, the financial markets' authorities have to undertake preventive measures on an ongoing basis. Namely, from a regulatory standpoint, the impact of terrorism on financial markets raises two challenges: first, capturing the possibility for terrorist events from an operational risk perspective; and, second, developing an adequate framework for countering terrorist financing.

5.1 Operational risk perspective

The Basel Committee on Banking Supervision identifies terrorism as one of the operational risk events that has the potential to result in substantial losses (Bank for International Settlements, Basel Committee on Banking Supervision, 2003). Consequently, the Basel Committee outlines the role of financial supervisors and institutions in mitigating the operational risk resulting from terrorist events. Supervisors must require that all banks have in place effective frameworks to identify, assess, monitor, and control or mitigate material operational risks resulting from terrorism as part of the overall approach to risk management.

Furthermore, banks themselves should take all necessary steps to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption, through adequate contingency and business continuity plans. The terrorist attacks of 11 September highlighted the importance of having operative business continuity plans across the financial system. At the same time, these attacks uncovered a number of important vulnerabilities.

A joint report by several financial market authorities in the United States[3] found that business continuity plans had not been designed to cope with wide-area disasters or with significant loss or inaccessibility of critical staff. In addition, the report notes that some critical market functions, such as the clearing and settlement of funds, securities, and financial contracts, relied on a small number of institutions concentrated in a single area. The concentration also affected the telecommunications capabilities as many firms discovered that all of the lines traveled through only a few single points of failure[3]. All these weaknesses demonstrated the need for rethinking the existing business continuity plans, possibly to encompass multiple layers of redundancy, each calibrated to a different level of emergency as needed (Ferguson, 2003).

Drawing from the lessons learned in the aftermath of the terrorist attacks, industry participants and market authorities in the United States acknowledged a number of business continuity objectives of special importance for all financial firms and the financial system as a whole: rapid recovery and timely resumption of critical operations following a wide-scale disruption or loss/inaccessibility of staff in at least one major operating location and a high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible[3].

The joint report also identified four sound practices that focus on minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets and support the resilience of the financial system:

- identify the critical clearing and settlement activities in support of financial markets;
- determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets;
- maintain sufficient geographically dispersed resources to meet recovery and resumption objectives; and
- routinely use or test recovery and resumption arrangements.

In addition, it is important that the measures aimed at mitigating the operational risk resulting from terrorist events should not be limited solely to commercial financial

services. Past experience has shown that central banks and other key official financial institutions can be targeted or threatened by terrorists. In January 1996, the central bank bombing in Sri Lanka by a local terrorist group resulted in a significant loss of life and inflicted major damage on the institution's database and computer system (International Monetary Fund, 1996). In the aftermath of the tragedy, the IMF provided considerable assistance to reconstruct the central bank's database. More recently (August 2004), information was provided that the IMF and the World Bank were also considered as potential targets for terrorist attacks.

In summary, business contingency plans should be an integral part of good business practices throughout the financial sector. In particular, the systemically important financial institutions and payments and settlement systems need to be able to continue to serve customers and financial market participants in the face of a serious disruption.

5.2 Countering terrorist financing

According to Financial Action Task Force on Money Laundering (FATF), there is little difference between terrorist and other criminal methods in the use of the financial system (Financial Action Task Force on Money Laundering, 2002). Terrorist financing shares multiple characteristics with money laundering in terms of sources, techniques, adaptability, and risks implied. Both are criminal activities attempting to disguise the sources and destination of funds, change the form of funds, or move the funds to a place where they are less likely to attract attention.

Although the primary motivation of terrorism is not financial gain, which stands in sharp contrast to most crime, terrorists still need to use the financial infrastructure to mobilize and channel their funds. Like money launderers, terrorists raise their funds through various money-making activities that may include criminal acts, such as kidnapping, extortion, large-scale smuggling, narcotics trafficking, robbery, and theft (Financial Action Task Force on Money Laundering, 2002). Consequently, terrorists need to launder the illicit funds in order to move them without drawing the attention of authorities.

FATF's findings point out that terrorists use the same laundering methods as other criminal groups, including cash smuggling, structured deposits and withdrawals from bank accounts, purchases of various types of monetary instruments, use of credit or debit cards, and informal remittance networks. Like money launderers, terrorists have developed new techniques for mobilizing and using their funds as the old ones are detected. Terrorists have been able to switch from traditional methods to disguising and transferring value in the form of precious gems and metals, or through charities and non-profit organizations. Also, there is evidence that terrorist financing networks operate globally, being capable of infiltrating the financial systems of both developing and developed countries.

Besides the multiple common characteristics shared with money laundering, terrorist financing presents a number of specific features, which in practice tend to raise the complexity of countering measures. A distinct trait of terrorist financing is that it includes – besides illegal sources of funds – legally earned funds. This adds to the difficulty of tracking terrorist funds and enforcement, since regulatory and law enforcement authorities have to prove that the use of the funds is for terrorist activities.

In addition, the sums needed to conduct terrorist attacks are often tiny compared with amounts laundered, for example, from drug trafficking, and, therefore, harder to detect.

For example, the sums that circulated between the 11 September 2001, hijackers and their overseas accounts amounted to less than $10,000, and, in most cases, the operations were simple wire transfers (Financial Action Task Force on Money Laundering, 2002). Nevertheless, the amounts needed to run terrorist organizations and networks are acknowledged to be considerable, and thus more susceptible to detection and control.

Finally, fighting terrorist financing requires a multidisciplinary approach. More than in other cases of financial crime, countering terrorist financing has to rely extensively on intelligence sources and requires a very close cooperation between intelligence and law enforcement agencies and other stakeholders, such as financial institutions and market supervisors.

The first attempt to raise global awareness and develop a unified approach to counter terrorist financing came ten years after FATF developed its 40 Recommendations, setting out the measures national governments should take to implement effective anti-money-laundering programs. Thus, in December 1999, "deeply concerned about the worldwide escalation of acts of terrorism in all its forms and manifestations", the General Assembly of the United Nations adopted the UN International Convention for the Suppression of the Financing of Terrorism. While this Convention was initially ratified by a few countries, in the aftermath of the 11 September 2001, terrorist attacks, a large number of states stepped up to reaffirm their determination in the fight against terrorism.

The number of countries that ratified the UN Convention for the Suppression of the Financing of Terrorism increased from 4 before 11 September to 117 states today. Also, according to the 2003 US Treasury report, "Progress in the War on Terrorist Financing", since 11 September 2001, 173 countries have issued blocking orders freezing terrorist assets; 100 countries have passed new laws, strengthening their safeguards against terrorist financing; and more than 100 countries have established financial intelligence units.

By the end of 2001, the mandate of FATF was also expanded beyond money laundering, to combat terrorist financing. During the extraordinary Plenary held in October 2001, the FATF issued new international standards to combat terrorist financing, which call on all countries to adopt and implement the "Special Eight Recommendations" (expanded to nine Recommendations in October 2004, with the adoption of a Recommendation dealing with cash couriers), denying terrorists and their supporters access to the international financial system. Also, in September 2001, the UN Security Council adopted Resolution 1373 that called on states, inter alia, to prevent and suppress the financing of terrorist acts, criminalize terrorist financing, and freeze terrorist assets.

Subsequently, a number of important regional and international bodies and international organizations, including the FATF-style regional bodies, the Egmont Group of Financial Intelligence Units, the IMF, and the World Bank, moved toward supporting and contributing to international efforts against terrorist financing. The extensive international participation helped to increase significantly the number of countries in the fight against terrorist financing and also to develop a global, consistent and integrated approach to anti-money laundering (AML) and combating the financing of terrorism (CFT) measures.

While, as shown above, there are some differences between how money laundering and terrorist financing are conducted, in terms of the measures and capacity building

that are required to counter them, there is no appreciable difference. Therefore, the AML/CFT standards require an adequate legal and institutional framework, which should include the following:

- laws that create money laundering (ML) and financing of terrorism (FT) offenses and provide for the freezing, seizure, and confiscation of the proceeds of crime and terrorist funding;
- laws, regulations, or other enforceable means that impose the required obligations on financial institutions and designated non-financial business and professions;
- an appropriate institutional or administrative framework, and laws that provide competent authorities with the necessary duties, powers and sanctions; and
- laws and other measures that give a country the ability to provide the widest range of international cooperation.

The FATF Special 8 (subsequently 9) Recommendations on Terrorist Financing, combined with the previous 40 Recommendations on money laundering, became the international standards for detecting, preventing, and suppressing the financing of terrorism. They commit countries to:

- take immediate steps to ratify and implement the relevant UN instruments;
- criminalize the financing of terrorism, terrorist acts, and terrorist organizations;
- freeze and confiscate terrorist assets;
- report suspicious transactions linked to terrorism;
- provide the widest possible range of assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations;
- impose anti-money-laundering requirements on alternative remittance systems;
- strengthen customer identification measures in international and domestic wire transfers;
- ensure that entities, in particular non-profit organizations, cannot be misused to finance terrorism; and
- detect the physical cross-border transportation of cash and bearer-negotiable instruments.

In 2002, the IMF and World Bank adopted the FATF Recommendations as one of 12 standards that are important to their operational work. The fund/bank work has focused on conducting assessments to identify the strengths and weaknesses in countries' AML/CFT regimes in collaboration with the FATF and FATF-style regional bodies; providing technical assistance to strengthen AML/CFT legal and regulatory arrangements and capacity to implement such systems; and regional training and outreach.

The FATF standards require that all banks, insurance companies, and securities dealers be fully regulated and supervised for AML/CFT purposes. Provisions call, inter alia, for effective know your customer (KYC) measures and enhanced customer due diligence (CDD) in high-risk cases; and record keeping and suspicious transaction reporting (STRs). In June 2003, the FATF revised its 40 Recommendations and

expanded the coverage of AML/CFT provisions to a range of new sectors (non-financial business and professions – namely, casinos, real estate agents, dealers in precious metals and stones, lawyers, notaries and other independent legal professionals, accountants, and trust and company service providers).

5.3 Regulatory challenges

Implementation of a regulatory framework to counter terrorist finance poses a number of regulatory challenges, related to the fact that to be effective the regulatory framework needs to be comprehensive across countries and financial institutions, and the regulatory "bar" set at a rigorous level to ensure effective detection.

Economic research has shown that antiterrorist policies are more successful if conducted across the entire spectrum of potential terrorist activities, including their resource endowment, so as to reduce substitution possibilities, with terrorists moving from hard to soft targets or shifting their activities over time (Sandler and Enders, 2004). Consequently, the efforts to disrupt terrorists' ability to fund their operations have to go beyond the formal banking or mainstream financial sector, and encompass the alternative financing mechanisms and any other emerging methods.

It is widely recognized that, as with formal financial systems, informal funds transfer systems present a ML/TF risk because they allow rapid, inexpensive international transmission of funds without adequate scrutiny of originators and beneficiaries of remittances. Recent international initiatives in the field of informal funds transfer systems (i.e. The Second International Conference on Hawala, Abu Dhabi, April 2004, jointly organized by the International Monetary Fund and the Central Bank of the United Arab Emirates) have underscored the importance of remittances to certain segments of the population and the need to raise the awareness of the regulated community and public to ML/FT risks, and engender an effective dialogue among various stakeholders to help develop constructive solutions.

A particular challenge in designing appropriate regulatory and supervisory mechanisms for informal funds transfer systems is avoiding driving remittance providers further underground and thereby making the transactions more difficult to detect and potentially excluding certain individuals, such as migrants and unbanked, from financial services. This issue is particularly relevant to developing countries, where the informal funds transfer systems represent an important source of external funding as well as an essential gateway to banking for migrants[4].

Within the regulated financial system there is evidence of significant increases in costs related to AML/CFT regimes. Supervisors have taken decisive action against financial institutions, including a number of high profile institutions, mostly banks, for violation of AML/CFT requirements. The evidence shows that supervisors from the advanced countries have taken the lead in enforcement of AML/CFT compliance in the financial sector. The most prominent cases involve large/multinational banks from the United States and Europe (e.g. Riggs Bank, Citigroup, Abbey National, ABN Amro, Union Bank of California).

Riggs Bank was fined $25 million dollars in 2004 by the US Office of the Comptroller of the Currency. The bank was scrutinized mainly in connection with money laundering and terrorist financing concerns involving accounts of foreign governments and politically exposed persons. Citigroup was ordered in 2004 by the Japan Financial Services Agency to close its private unit in Japan. Regulators cited a

long list of infractions, including improper client screening and failing to prevent suspected money laundering.

Abbey National was fined £2.3 million in 2003 by the UK Financial Services Authority for AML/CFT compliance failures. Regulators found that the bank failed to ensure that suspicious activity reports were promptly considered and reported to the National Criminal Intelligence Service. Finally, ABN Amro and Union Bank of California were recently required to terminate banking relationships with about 550 banks in Russia, Eastern Europe, and the Caribbean mainly because of ML/FT risk concerns in their correspondent banking businesses.

In addition to direct costs associated with fines and litigation, the adverse publicity associated with supervisory enforcement has damaged their reputation, customer base, and, in some cases, market capitalization. In one instance, for example, the shares of a major international bank fell nearly 3 percent the day after a prominent Wall Street analyst downgraded the bank, citing ethics problems.

Driven by enhanced national and international efforts to combat crime in the financial system, banks and other financial institutions around the world have been upgrading their AML/CFT systems and have experienced a significant increase in compliance costs. This increase largely reflects the implementation of legal and regulatory measures for enhanced customer due diligence, staff training, and monitoring and reporting of suspicious transactions. For some institutions, investment in new information technology (IT) systems and software has been a key expenditure. In a recent KPMG survey, 83 percent of respondent banks indicated that AML/CFT compliance costs have risen, on average, about 61 percent over the past three years[5].

Nevertheless, despite the increase in compliance costs, a vast majority (84 percent) of respondents regarded the regulatory burden as acceptable, indicating a high degree of commitment by the financial industry to protect the integrity of their own firms. For example, adequate KYC policies and procedures are important from a wider prudential and financial integrity objective, not just anti-money laundering or terrorist financing, perspective. Without adequate customer due diligence, financial institutions can become subject to reputational, credit, operational, legal, and concentration risks, which can result in significant financial costs. The AML/CFT framework incorporates a risk-based component, thus providing the scope for financial institutions to tailor their CDD measures to the circumstances of their customers and counterparties.

An area where the survey participants noted the need for improvement is achieving a better feedback from governments and financial intelligence units. Enhanced intelligence is needed by financial institutions to "red flag" potential terrorist transactions for checking against the financial institutions' records. In addition, financial institutions need feedback on the usefulness of the suspicious transactions reports they provide to financial intelligence units (FIUs). Respondents also attached a high degree of importance to standards and guidance by supranational bodies, and called for improved coordination of AML policy at the global level.

The increased regulatory requirements and enforcement actions are beginning to have ripple effects. Some major banks have cut their overseas customer and correspondent banking relationships because of ML/TF concerns and enforcement actions. Several banks have also closed the accounts of money service providers due to money laundering and terrorist financing concerns, resulting in disruption to the money service business and remittance transfers.

There is a risk that counties and financial institutions with weak AML/CFT regimes will face exclusion from access to the major financial institutions and markets. At the same time, given the rigorous legal and regulatory requirements necessary to achieve effective compliance with the international standards, there is a question whether the least developed economies and smaller financial institutions from advanced countries will have the capacity to meet the higher regulatory standards. If they do not or cannot, there is a risk of their exclusion form the major financial markets and segmentation in financial markets between the wealthier jurisdictions and institutions that can comply with international standards and the weaker jurisdictions and institutions that cannot.

The above issues point to the need to achieve the right balance between costs and benefits in implementing the AML/CFT measures. The major benefit for the financial system stability derives from the positive impact of AML/CFT measures in strengthening the integrity of financial systems and helping to protect them from abuse. Over the longer term this should improve the efficiency of resource allocation and thus boost economic growth and development.

In this regard, the implementation of the standards will need to be sensitive to national economic circumstances, in particular the specific integrity risks posed by the jurisdictions, the importance of different channels for legitimate payments, and the speed with which jurisdictions can develop their legal and regulatory capacities. Technical assistance from international organizations and bilateral donors will play a key role. An assessment of the benefits and the effective approaches also needs also to take into account the volumes of money laundering and terrorist financing that are detected/prevented and the impact of AML/CFT regimes in identifying or contributing to criminal or terrorist investigations, but these are matters beyond the scope of this paper.

6. Conclusions

This paper found that diversified, liquid, and sound (including from a contingency plans for business continuity point of view) financial markets were efficient in absorbing the shocks of terrorist attacks. However, the timely and flexible response of the competent authorities was also critical in stabilizing the markets. The central banks' lender-of-last-resort functions were effective in stifling panic in the aftermath of terrorist acts, and cross-border cooperation among the central banks helped mitigate global contagion effects. Coordinated efforts among the national regulators and the industry also helped to stabilize the situation quickly.

The terrorist attacks on the US financial sector underscored the importance of having in place operative business continuity plans. Business continuity plans should be an integral part of good business practices across the financial system. Systemically important financial institutions and systems should be able to ensure rapid recovery and timely resumption of critical operations following the loss or inaccessibility of key staff and systems in major operating locations or in the aftermath of wide-scale disturbances.

At a general level, a coordinated effort is required from the various stakeholders (financial industry, regulators and supervisors, intelligence and prosecuting agencies, governments, international organizations, etc.) to achieve the common objective of safeguarding the soundness and the integrity of financial systems from terrorism. A global and comprehensive approach is now in focus and increasing attention is being

given to effective implementation of the standards by national supervisors and regulators, and financial institutions.

Implementation of a regulatory framework to counter terrorist financing poses a number of regulatory challenges, related to the fact that to be effective the regulatory framework needs to be comprehensive across countries and financial institutions, and the mechanisms set at rigorous level to ensure effective detection. A key challenge going forward will be to achieve the right balance between the costs and benefits in applying the regulatory framework, and to avoid unnecessary segmentation and exclusion in financial markets.

Notes

1. Securities and Exchange Commission (2001) "Testimony Concerning The State of the Nation's Financial Markets in the Wake of Recent Terrorist Attacks, Harvey L. Pitt, Chairman, US Securities and Exchange Commission Before the Committee on Financial Services United States House of Representatives, September 26".
2. International Monetary Fund, International Financial Statistics (2003). Note that January 2003 marks a change in the Federal Reserve discount rate calculation methodology (change to "primary-secondary" discount rates, www.frbdiscountwindow.org/discountwindowbook.cfm?hdrID = 14&dtlID = 43). Although not apparent because of the change in methodology, the discount rate was further decreased after January 2003.
3. US Federal Reserve System, Department of the Treasury, and Securities and Exchange Commission (2002) "Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System".
4. Ratha (2003) notes that transfers through informal channels (including Hawala) are believed to be significant in many developing countries, ranging from 10 to 50 percent of total remittances (in 2001, worker remittance receipts of developing countries totaled $72.3 billion).
5. KPMG International's "Global Anti-Money Laundering Survey 2004. How Banks are Facing Up to the Challenge". The KPMG survey included banks from the major sectors (retail, corporate, private, investment, and wholesale banking) that were largely drawn from the top 1,000 global banks and supplemented with local banks. There were 209 respondent banks from 41 countries.

References

Bank for International Settlements, Basel Committee on Banking Supervision (2003), "Sound practices for the management and supervision of operational risk", Bank for International Settlements, Basel, February.

Bruck, T. and Wickstrom, B.A. (2004), "The economic consequences of terror: guest editor's introduction", *The European Journal of Political Economy*, Vol. 20, pp. 293-300.

Chen, A.H. and Siems, T.F. (2004), "The effects of terrorism on global capital markets", *The European Journal of Political Economy*, Vol. 20, pp. 349-66.

Eldor, R. and Melnick, R. (2004), "Financial markets and terrorism", *The European Journal of Political Economy*, Vol. 20, pp. 367-86.

European Central Bank (2004), *Monthly Bulletin*, April.

Ferguson, R.W. Jr (2003), "11 September, the federal reserve, and the financial system", *BIS Review*, No. 5.

Financial Action Task Force on Money Laundering (2002) *Report on Money Laundering Typologies 2001-2002*, February, pp. 2-7.

Flynn, P. (2002), "Financial bailout of September 11: rapid response", *Challenge: The Magazine of Economic Affairs*, January-February, Vol. 45 No. 1.

International Monetary Fund (1996) *Sri Lanka*, IMF Staff Country Report No. 96/100, IMF.

International Monetary Fund (2001a), "Financial system abuse, financial crime and money laundering", background paper, available at: www.imf.org/external/np/ml/2001/eng/021201.htm

International Monetary Fund (2001b), "World economic outlook – the global economy after 11 September, December 2001: a survey by the staff of the international monetary fund", World Economic and Financial Surveys.

Lacker, J.M. (2004), "Payment system disruptions and the federal reserve following September 11, 2001", paper prepared for the Carnegie-Rochester Conference on Public Policy, 21-22 November.

PricewaterhouseCoopers (2001), *Insurance Digest*, Americas edition, December.

Ratha, D. (2003), "Workers' remittances: an important and stable source of external development finance", *Global Development Finance 2003*, World Bank, Washington.

Sandler, T. and Enders, W. (2004), "An economic perspective on transnational terrorism", *The European Journal of Political Economy*, Vol. 20, pp. 301-16.

Taylor, B. (2004), "The historical impact of crises on financial markets", Global Financial Data, available at: www.globalfindata.com

US Department of State (2003), "Patterns of global terrorism", Appendix G – Statistical Review, available at: www.state.gov/s/ct/rls/pgtrpt/2003/33777.htm

Corresponding author
R. Barry Johnston can be contacted at bjohnston@imf.org