

## THE IMPACT OF THE 11<sup>th</sup> OF SEPTEMBER ON FINANCIAL INSTITUTIONS

**Summary:** The terrorist attacks of September 11<sup>th</sup> have focussed the attention of legislators around the world on measures to combat money laundering and the funding of terrorism. Many of the measures introduced by governments in the US and in Europe place additional responsibilities on financial firms and markets to help in the fight against terrorism. By and large, the financial community is meeting this challenge. As one of the primary targets of the attacks, the financial services industry has been keen to assist the authorities as much as possible. Even so, banks, regulators and markets face the difficult task of striking the correct balance between the imperative of stamping out illegal practices, and respecting the interests (including privacy) of legitimate customers. Internationally active firms have the complicated task of complying with regulation in a multitude of jurisdictions. There is a genuine need for enhanced global cooperation among nations and between governments and the financial community if these efforts are to be successful.

### **What was the immediate impact of September 11<sup>th</sup> on the global financial system?**

The terrorist attacks on the World Trade Centre on September 11<sup>th</sup> 2001 impacted the financial services community on a number of levels. In terms of loss of life, destruction of physical infrastructure, and disruption of communication networks, the brunt of the attacks was borne by the financial industry. The choice of target represented a deliberate attack on the global financial system, of which the World Trade Centre was arguably the most visible symbol.

The loss of life and the damage to infrastructure in downtown Manhattan as a consequence of the September 11<sup>th</sup> attacks led to major disruptions in financial markets. US equity markets closed for four working days while markets in Europe and Asia remained open but halted trading in shares of US based companies. Damage to the operations of inter-dealer brokers, communications links, and some clearing and settlement systems temporarily disrupted the functioning of segments of US fixed income markets.

### **How did the financial system and individual firms respond to the attacks?**

Under the circumstances, the financial system responded to the crises remarkably well. Stock and derivatives markets jointly decided to open after five days, and by mid-October stock markets had returned to pre-attack levels. Swift communication between all players and authorities proved to be crucial. Firms capitalised on extensive Y2K contingency planning and were able to quickly relocate staff in temporary offices in the surrounding metropolitan area. Much business was re-routed through major financial centres in Europe so that settlement and other functions could continue smoothly: non-US markets reacted in cooperative fashion to the disaster. Competitor firms showed a remarkable degree of collegiality and rallied around those firms most seriously affected by the attacks. For example, in response to losses of personnel and equipment at some market participants, dealers agreed voluntarily to extend settlement in the US Treasury market to T+5 (trade date + 5 days). There were also well-publicised instances of firms making office space, and communication links available to competitors.

### **The regulatory/investigatory response**

Within hours of the attacks, financial institutions began working with regulatory and law enforcement agencies to establish who might have been responsible for the attacks and where

the financing had come from. The institutions quickly began searching client records against suspect lists provided by the US authorities. This has led to the freezing of assets worth approximately €90 million worldwide. Checking of records against suspect names continues. The list of terrorist suspects has grown to approximately 3000 individuals or entities. Overlapping but non-identical lists have been forwarded to financial institutions by at least 12 separate authorities including the Monetary Authority of Singapore, Swiss Federal Banking Commission and the FBI. The task has been complicated by inconsistent transliteration from Arabic and by the fact that many of the names are very common, thus making it difficult to distinguish between the intended person and innocent individuals.

In the days following the attacks, reports of alleged short-selling/insider dealing by terrorist suspects began to appear in the press, prompting wide-ranging investigations in a number of countries by both regulators and financial firms. To date, no credible evidence of such practices has been found.

A major difficulty for the authorities as well as financial institutions is the fact that little, if anything, in the funding activities of the 19 hijackers involved in the attacks could be considered “suspicious” in terms of pre-existing or newly enacted anti-money-laundering provisions. The terrorists opened bank accounts in their own names, using genuine passports and other means of identification, deposited modest sums of cash and avoided applying for credit cards or other forms of credit that might have resulted in additional checks. It is clear that future efforts to detect terrorist use of the financial system will depend upon accurate and timely information about the identity of suspected terrorists.

### **The US response: the USA PATRIOT Act, 2001**

On 26<sup>th</sup> October, the US Congress adopted the “*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*”. The Act, which represents a non-partisan agreement between both sides of Congress, was strongly supported by the US financial services industry. It refines a range of existing legislative requirements, and brings into force a number of pending anti-money-laundering (AML) provisions. In particular the Act:

- extends suspicious activity reporting obligations to the securities, brokerage, and commodities trading industries;
- prohibits the establishment, maintenance, administering, or managing of correspondent accounts with shell banks (i.e. foreign bank with no physical presence in any country);
- introduces enhanced due diligence procedures for private banking relationships;
- tightens existing “know your customer” rules;
- provides extraterritorial jurisdiction to compel disclosures and secure the forfeiture of funds; and
- increases the penalties for money laundering violations.

Further information relating to the USA PATRIOT Act can be found on the Congressional website at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@L&summ2=m&>

### **The European response: new money laundering directive and ratification of UN Convention**

The Ghent European Council in October called for the immediate adoption of the revised Directive on Money Laundering and the speedy ratification by all Member States of the United

Nations Convention for the Suppression of the Financing of Terrorism. With the European Parliament's approval of the Money Laundering Directive on the 13<sup>th</sup> November, the EU extended the obligation to notify suspicious transactions to certain non-financial professions and sectors, and widened the definition of money laundering to include the proceeds of *all* serious crime (including terrorism). The new rules will cover professions not yet covered by US AML legislation, such as accountants, auditors and lawyers. Once implemented, the Directive should prove a useful tool in the struggle against the terrorism and organised crime. On 27<sup>th</sup> December, the Council adopted a framework Regulation (27/12/2001) aligning the EU with the provisions of the United Nations Security Council Regulation 1373/2001 on combating terrorism. The measures strengthen the legal and administrative capacity of the EU and its Member States to take action against terrorists and their supporters. The Regulation allows the freezing of assets across Europe as soon as an individual or organisation has been identified as a potential source of terrorist funding. Banks and investment firms in Europe have been working very closely with regulators implementing the freeze of funds.

### **The international response: FATF, Wolfsberg Group**

Financial Action Task Force (FATF): At an extraordinary plenary meeting on the financing of terrorism held in Washington, DC, on 29-30 October 2001, the FATF expanded its mission beyond money laundering. It will now focus its expertise on the worldwide effort to combat terrorist financing. The FATF has issued new international standards to combat terrorist financing which it calls on all countries to adopt and implement. Further information on the FATF's recommendations can be found at: <http://www1.oecd.org/fatf/index.htm>.

The 'Wolfsberg Group': In the wake of September 11<sup>th</sup>, the Wolfsberg Group (a private sector group working in conjunction with Transparency International) convened a working group to study issues arising from the attacks. The Group has made recommendations regarding the appropriate response for governments and financial institutions in the form of a Wolfsberg Statement on the Suppression of the Financing of Terrorism. According to the Group, industry needs governments to: provide detailed information and context; to give unambiguous directions; to share intelligence on a timely basis; and to foster enhanced global cooperation on this issues. For its part, the financial services industry needs to: employ genuine vigilance and robust know your customer procedures; exercise careful judgment; provide full details to regulators and genuinely cooperate with government. For more information about the Wolfsberg Group's work, see: <http://www.wolfsberg-principles.com>.

### **What else could be done?**

Enhanced global cooperation: To effectively deal with the challenge of international terrorism, there needs to be much more effective cooperation among governments on a global level. There is a need to provide meaningful information in relation to patterns, techniques and mechanisms used in the financing of terrorism and clear guidelines on appropriate levels of heightened scrutiny in relation to sectors or activities identified by competent authorities as being widely used for terrorist financing.

More sharing of intelligence: The ability of financial institutions to assist the battle against terrorism depends greatly on the quality of the information provided to them by the authorities. It is possible that had the FBI passed on to banks the same information regarding the terrorist suspects that they passed to US Customs and Immigration in August of 2001, the suspects would have been tracked down prior to September 11<sup>th</sup>. Whether this would have prevented the

attacks is a moot point, but it highlights the sort of cooperation that could prove invaluable in the future.

Global safe harbour: Generally speaking, financial institutions are granted a “safe harbour” from prosecution under AML rules in a given jurisdiction when they can show that they have notified suspicions relating to the transaction to the relevant authorities in that jurisdiction. However, such “safe harbours” generally do not extend beyond the borders of that jurisdiction. In an increasingly globalized market, this places financial institutions at risk of incurring substantial liabilities in one jurisdiction for complying with the AML laws of another.

Effective enforcement: The importance of not only the private sector complying with the law but also the need for authorities to devote attention and resources to effective enforcement needs to be highlighted. Legislation is important but effectiveness of implementation and enforcement are crucial too. There is the need for continued attention to contingency planning and mutual information exchange between all levels.

Striking the correct balance between data protection concerns and effective AML due diligence: According to some authorities, certain data protection legislation requires financial institutions to disclose to a client full details regarding the filing of any suspicious activity reports notwithstanding the anti-tipping provisions of most AML laws. In other words, in some instances a bank may be compelled to elect between defying the data protection law or placing itself at risk of criminal prosecution by notifying the client of a confidential report regarding possible money laundering activity.

Briefing notes are prepared by the Industry Advisory Committee to the European Parliamentary Financial Services Forum. For further information on the subjects raised in the briefs please contact the Chairman, Members or Secretariat of the Advisory Committee.

**Steering Committee**

Robert Goebbels, MEP  
Chris Huhne, MEP  
Giorgos Katiforis, MEP  
Piia-Noora Kauppi, MEP  
Alexander Radwan, MEP  
Peter Skinner, MEP  
Theresa Villiers, MEP

**Chairman Advisory Committee**

Paul Arlman  
Federation of European Securities Exchanges  
Rue du Lombard 41  
B – 1000 Brussels  
Tel: 0032 2 551 01 80  
Fax: 0032 2 512 49 05  
E-mail: arlman@fese.be

**Secretary**

John Houston  
Houston Consulting Europe  
Avenue de la Joyeuse Entrée 1-5  
B – 1040 Brussels  
Tel: 0032 2 504 80 40  
Fax: 0032 2 504 80 50  
E-mail: info@houston-consulting.com

Founding Members

Richard Balfe MEP	C.A. Gasoliba I Bohm MEP
Robert Goebbels MEP	Chris Huhne MEP
Othmar Karas MEP	Giorgos Katiforis MEP
Piia-Noora Kauppi MEP	Astrid Lulling MEP
Ria Oomen-Ruitjen MEP	Karla Peijs MEP
John Purvis MEP	Alexander Radwan MEP
Karin Riis-Jorgensen MEP	Olle Schmidt MEP
Peter Skinner MEP	Charles Tannock MEP
Theresa Villiers MEP	

Advisory Committee

ABN AMRO Bank  
Banco Bilbao Vizcaya Argentaria  
Barclays  
Deutsche Bank AG  
European Banking Federation (FBE)  
Federation of European Securities Exchanges  
Futures and Options Association  
Goldman Sachs  
International Swaps and Derivatives Association  
San Paolo IMI Bank  
Société Générale  
Svenska Handelsbanken  
UBS AG