Sibos 2016 in Review

Trends in Counter Terrorist Financing – Panel Summary

Preventing terrorist financing is a major concern across the industry – but the way in which terrorists fund themselves is changing as small cell and lone wolf attacks become more common. A panel discussion at Sibos 2016 explored how the industry can adjust to these developments, while minimising the negative impact of any measures taken on legitimate transactions.

Contents

Participants

James Freis
Chief Compliance Officer
at Deutsche Börse.

An experienced lawyer in AML and terrorist financing issues, James was previously director of FinCEN, the Financial Intelligence Unit of the US Treasury.

Tom Keatinge
Director of the Centre for Financial Crime & Security Studies, Royal United Services Institute (RUSI), a London-based defence and security think-tank.

Tom has published research on topics including the role of finance in defeating al-Shabaab; the role of financial intelligence in identifying and disrupting foreign terrorist fighters, and ISIS financing.

Troels Oerting
Group Chief Information
Security Officer, Barclays.

Troels is the former head of Europol in Denmark and is an examiner for the Danish National Police Force on cyber security issues.

Karen Walter
Head of the Economic
Sanctions Unit, Allianz.

A capital markets lawyer, Karen has worked in the US and Europe for leading law firms and now advises on compliance issues.

Session highlights

- Recent lone wolf and small cell terrorist attacks have not involved large sums of money.
- Terrorists are being financed by legitimate sources such as student loans, as well as by criminal activities.
- The financial industry needs to adapt to the different approaches being used by terrorists.
- Information sharing between private and public sectors is key.
- More information is not necessarily helpful – the goal is to focus on higher quality information.
- The possible unintended consequences of further measures need to be taken into account, from data privacy to financial exclusion.

Counter terrorist financing

As panellists at Sibos 2016 highlighted, the area of counter terrorist financing has changed considerably over the last few years. Before the 9/11 attacks, it was difficult to arrest suspected terrorists before an attack had actually been carried out. Since then, more focus has been placed on preparatory support for terrorist acts, including funding. However, the area of terrorist financing is continuing to evolve alongside the recent rise of attacks by small cells and 'lone wolf' terrorists.

In light of these changing threats, the panel agreed that preventing terrorist financing is a significant challenge: lone wolf attacks involve smaller cells of money and financial flows may be difficult to track. Alongside the difficulties involved in identifying suspicious transactions, efforts to tackle terrorist financing also need to be weighed up against the other possible consequences, from data privacy concerns to financial exclusion.

> **"There are many different sources of intelligence out there, but why is that financial component so critical for us – both in a proactive and a reactive sense? Fundamentally, you don't send people money if you don't know them."**
>
> **James Freis**, Chief Compliance Officer, Deutsche Börse

How terrorists fund themselves

As one of the panellists noted, from 9/11 to more recent attacks in Paris and Brussels, nearly every terrorist attack involves some element of funding. Following the 9/11 attacks, over $300,000 was found to have flowed through the formal banking system. Counter terrorist financing efforts tended to focus on large scale funding sources, including state sponsors, individual wealthy donors and charities.

Today, however, the situation has changed, the panel noted. Individuals can be radicalised in as little as two weeks, a panelist noted, so there may be little opportunity to identify suspicious payments before an attack is carried out. In any case, recent attacks carried out by small cells and foreign fighters have not involved large sums of money. Research carried out by the Norwegian Defence Research Establishment (FFI) found that of 40 jihadi cells that plotted in Europe between 1993 and 2013, 76% of the terror plots cost less than $10,000.

The panel went on to point out that terrorists are also tapping different funding sources for such attacks. The FFI research found that almost three quarters of the terror cells had acquired part of their financing from legitimate means, with 47% entirely self-financed. This funding can come from a variety of sources, from state-funded welfare benefits and student loans to petty crime and even short-term employment.

Likewise, this breed of terrorist may opt to use cash and prepaid cards instead of putting funds through the formal banking system, making flows more difficult to monitor. Terrorists are also adept at avoiding money transfer controls by transferring amounts lower than current reporting thresholds.

Tackling terrorist financing

In light of these trends, the panel found that the industry should be thinking differently about how terrorist financing should be addressed. The financial sector still has a role to play in preventing terrorist financing – but this role has changed over the last few years.

Sharing information

In order to keep up with current trends, the experts argued that there needs to be better exchange of information between private and public sectors, as well as within individual governments and organisations. As mentioned in the session, there are cases where

> **"We face an expanded threat, and we need to think differently. Frankly the financial industry was very late to that understanding."**
>
> **Tom Keatinge**, Director of the Centre for Financial Crime & Security Studies, RUSI

individuals who have travelled to Raqqa (Syria) continue to have benefits paid into their accounts at home – demonstrating that communication is not as joined up as it could be.

It was also noted that banks have access to financial intelligence that could be useful to the public sector, and vice versa – but information sharing tends to be inhibited by a lack of trust. In any case, it was pointed out that the goal is not necessarily to obtain more information: intelligence services are already handling vast quantities of data. Rather the goal is to obtain information that is of greater value.

> **"The problem is this: the information we need to determine whether or not money should be flowing around the world does not, itself, flow around the world at the touch of a button."**
>
> **Tom Keatinge**

As one of the panellists noted, sharing information between private and public organisations is crucial when it comes to preventing terrorist financing – but the relevant organisations need to be empowered to do this effectively.

Different countries are approaching this in different ways. In the US, for example, the Patriot Act facilitates the sharing of information between the government and the private sector. The UK, meanwhile, set up the 2015 Joint Money Laundering Intelligence Taskforce (JMLIT) which creates a similar opportunity for information sharing.

> **"We have enough information. We actually need to hone down on what is really important to do our job in the best possible way."**
>
> **Troels Oerting**, Group Chief Information Security Officer, Barclays

The panel agreed that by educating the private sector more effectively, the public sector can increase awareness about themes and trends that should be taken into account during transaction monitoring. For example, some types of transaction which might appear to be a straightforward example of fraud may actually relate to terrorist financing. Insurance is one area where this can be the case: for example, a pattern of minor car accidents was recently engineered by people who are were suspected of collecting the claims money to send to terrorist organisations.

> **"Money from insurance companies is considered to be clean. If someone gets a payment from an insurance company, generally speaking, no one is suspicious about it."**
>
> **Karen Walter**, Head of the Economic Sanctions Unit, Allianz

In practice, private sector organisations may face obstacles when it comes to information sharing – but they should be taking this information and engaging with national Financial Intelligence Units (FIUs) or relevant government agencies in order to overcome information blockages.

Unintended consequences

While it is clearly important to take the necessary steps to prevent terrorist financing, the experts pointed out that attention also has to be paid to the impact of such steps on legitimate money flows. People who are sending hard earned money back to family members in their home country may actually represent a good credit risk. Developments such as limited purposes accounts may be useful in some cases, allowing specific types of transaction to take place while allowing greater monitoring to take place.

One consideration where data sharing is concerned is the conflict between security and privacy. People may be concerned about sharing details of their financial activity. The panel noted that a change in mindset might be needed so that people understand that certain transfers come with an obligation to make their information available. Although data privacy and bank secrecy laws serve an important purpose, the panel noted that certain situations require clear authorisation to share information in the context of combating financial crime. In any case, panelists agreed, the objective is not to create a system which provides full insight into everything a bank does; rather to enable work to be focused more effectively.

“I’m a big fan of private-public partnerships – not just in counter terrorist financing, but in combatting cybercrime and in other areas. I think that’s the only productive way ahead.”

Troels Oerting

“I understand that people don’t necessarily want to share their financial information. But what are you hiding? For those of us who travel around the world, my credit card can go off anywhere – but I’m happy when they question whether I was in Colombia that day.”

James Freis

One of the panellists noted that another consideration is the conflict between the competing objectives of preventing terrorist financing and supporting financial inclusion. Parts of the world are effectively becoming financially ungoverned spaces, with more people carrying cash through airports – even if they have legitimate reasons for transporting money. A decision needs to be made about what the overall objectives are and how terrorist financing measures and sustainability goals can be reconciled.

Conclusion

As the panel discussion highlighted, terrorist financing is evolving fast, and the financial industry needs to adapt to the changing threats. At the same time, due consideration needs to be given to the impact of yet more regulation on legitimate financial flows, while concerns about data privacy and financial inclusion also need to be addressed.

Above all, closer communication is needed between the relevant parties in order to share information effectively. Without this type of dialogue, the money will continue to flow while information continues to be impeded.

sibos

TORONTO
16 - 19 Oct 2017

Sibos is the premier annual event for the financial services community. The conference and exhibition are organised by SWIFT, and facilitate debate, networking and collaboration around the future of payments, securities, cash management, trade and financial crime compliance.

For one week every year, Sibos connects some 8,000 business leaders, decision makers and thought leaders from financial institutions, market infrastructures, multinational corporations and technology partners.

Sibos takes place in Toronto in 2017 as Canada celebrates its 150th anniversary.

For more information please visit www.sibos.com

@Sibos, #Sibos

linkedin.com/company/Sibos

About SWIFT

For more than 40 years, SWIFT has helped the industry address many of its biggest challenges. As a global member-owned cooperative and the world's leading provider of secure financial messaging services, we enable more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, relentlessly pursue operational excellence, and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. We also bring the financial community together to work collaboratively to shape market practice, enable the creation of global standards and debate issues of mutual interest.

SWIFT users face unprecedented pressure to comply with regulatory obligations, particularly in relation to the detection and prevention of financial crime. In response, we have developed community-based solutions that address effectiveness and efficiency and reduce the effort and cost of compliance activities. Our Compliance Services unit manages a growing portfolio of financial crime compliance services in the areas of Sanctions, KYC and CTF/AML.

Financial crime compliance is also a major theme at Sibos, the world's premier financial services event, organised by SWIFT for the financial industry.

www.swift.com/complianceservices

57233 - October 2016