Trends in Terror Finance

Part 3: The Unregulated Sector

by John Solomon - World-Check Terrorism & Insurgency Unit

This report is the third of a three-part series on emerging paths for the financing of terrorism in the unregulated sector. The first report highlighted the increasing convergence of the telecommunications and banking sectors, exemplified by the rise of mobile phone banking (m-banking), and noted that the system will probably gain a significant share of the informal payment and remittance market relative to traditional, low-tech modes of unregulated money transfer like *hawala*. Technological innovation and economic factors will fuel growth in the broader domain of e-payments which includes e-money payments and transfers made by the Internet and other electronic channels. In light of this trend, the second report detailed two additional and interrelated e-payment modes – virtual currencies and virtual worlds – in regard to the terrorist financing risks involved.

Introduction

This report explores the regulatory challenges presented by the rapid growth and proliferation of e-payment systems with respect to countering the financing of terrorism (CFT). The article first draws an important distinction between m-banking and other e-payment systems. It then proceeds by addressing two key interlocking issues that appear to cloud the regulatory environment for these systems: jurisdictional issues and definitional issues.

The core of the jurisdictional problem lies in the disconnect between the globalised nature of e-payment services, the World Wide Web and rapidly evolving information technologies on the one hand, and state-centric domestic and international legal and regulatory frameworks on the other. E-payment transactions often de-territorialize financial transactions from states and thus raise difficult questions about the legal jurisdiction of regulatory authorities.

Also contributing to the unclear regulatory situation are problematic legal definitions of key terms. The first matter is objective and pertains to whether e-payment providers should be defined as banks or non-banks or neither. This is a significant legal distinction which impacts the way the provider will be regulated. If an e-payment provider is classified as a bank, then that provider must comply with an existing set of regulations designed for traditional brick and mortar banking institutions.

If it is not classified as a bank, then new regulatory frameworks might need to be created to check the dangers of terrorist financing abuses.

The second definitional obstacle that hinders international cooperation needed on CFT is the lack of a universally accepted definition of terrorism among United Nations member states. Since defining terrorism is at its heart a more value-based exercise compared to the mere technical nature of classifying e-payment providers as banks or not, the second definitional barrier is less clear cut and a resolution probably more far off.

The terrorism definition challenge is briefly discussed later in this paper and a potentially useful legal precedent is adduced that may help bring the international community closer to a consensus.

M-banking and other e-payment systems: a distinction

Innovative technologies almost always outpace governments' regulatory responses to them. Such is the case with e-payment systems. While m-banking, virtual currencies and virtual worlds are all relatively new e-payment systems, it is worth noting an important distinction among them. These differences may impact the way each method is regulated.

M-banking is perceived to be a much more significant driver of development and economic growth in the developing world than other e-payment systems due simply to the numbers.

Three billion people have mobile phones; whereas only 1 billion have bank accounts. Many in the developing world have access to mobile phones but not bank accounts. One research firm estimates that m-banking payments will generate almost $22 billion of transactions and will be used by 204 million mobile phone users by 2012.

For example, it is well-documented that real financial transactions take place in virtual worlds such as Second Life. In theory, a terrorist financier in east Africa could buy virtual currency over the Internet and purchase virtual real estate in a given virtual world from an associate in Paris.

> **"What nation-state if any has legal jurisdiction over the virtual world of ones and zeros when the individuals concerned physically reside across the real world in a number of different countries?"**

Perhaps this is why policy-makers, banks and other stakeholders have opted to assign preponderant weight to the economic potential of this innovative service at the expense of adopting a regulatory standard that is inadequate to mitigate much of the CFT risk.

M-banking undoubtedly holds vast economic potential. And virtual currencies and virtual worlds are far from economically insignificant – after all, the Chinese Yuan was challenged and nearly devalued earlier this year by Q Coin, a popular virtual currency – yet these e-payment systems are not the darling of the international development community that m-banking is. They neither share the obvious economic potential nor the reputation advantages that m-banking currently enjoys. Therefore, it is an open question whether there is a one size fits all solution for all e-payment regulation. Regulators may be more willing to relax the rules for m-banking in the interest of the greater good than they might for other e-payment systems.

Regulatory challenges: jurisdictions

However different these e-payment systems might be from one another, they present similar challenges to government regulators. The crux of the matter centers on two interlocking issues: the first is jurisdictional and the second is definitional. Information technology increasingly de-territorializes financial transactions from individual nation-states, obscuring the state-centric regulatory and legal concept of jurisdiction.

E-payments are a manifestation of this trend. Financial transactions in virtual worlds using virtual currency and commodities illustrate the ambiguity faced when laws and regulations fail to sufficiently address rapidly evolving scenarios.

The associate could then transfer the virtual money online to an operative in the United States through another virtual world before the sum is withdrawn and converted into a real national currency and used for an attack.

What nation-state if any has legal jurisdiction over the virtual world of ones and zeros when the individuals concerned physically reside across the real world in a number of different countries?

Bank or non-bank?

Connecting with the jurisdictional problems are definitional questions pertaining to how e-payment services should be classified. For instance, should regulators treat m-banking providers as banks or non-bank financial institutions? Or is that logical construct flawed from the start?

The implementation of m-banking in Kenya, the Philippines and South Africa provides examples of each. The Kenyan Banking Act [SEC. 2(1)] defines a bank as a business that accepts money from the public on deposit or on current account and uses this money "by lending, investment or in any other manner for the account and at the risk of the person so employing the money."

By simply failing to meet the second part of the definitional requirement, m-banking providers in Kenya are not legally considered banks and thus may not need to comply with domestic or international financial regulations and standards.

Philippine m-banking providers also found a similar definitional lacuna. The General Banking Law [SEC. 3.1] stipulates that banks are "entities engaged in the lending of funds obtained in the form of deposits." Since m-banking services merely store and move value without taking part in lending activities, these providers technically do not fulfill the legal definition of a bank. However it must be noted that the Central Bank of the Philippines now classifies some m-banking providers as remittance agents which allows for minimum regulatory oversight and continued growth of the service.

While there is at least some regulatory oversight present, the level of oversight with respect to KYC generally appears inadequate for CFT purposes. The Financial Action Task Force (FATF), the international standard setting body for CFT and AML, strongly recommends robust KYC procedures including the verification of identification information and source of funds.

Due to a reasonable expectation that poor customers will be unable to comply with even the minimum KYC standards regarding identification verification, some central banks have allowed for a relaxation of the rules. A voucher from an existing customer is treated by domestic regulators as sufficient KYC in at least some countries supporting the growth of m-banking.

There is a paucity of data currently available on the topic but the Republic of South Africa appears to be following this model and its experience should be monitored closely. Currently the banks are licensed to offer m-banking services through agents such as mobile phone operators and point-of-sale retailers.

Defining terrorism: a legal and definitional precedent

Over and above the debates regarding the classification of e-payment services within a state is the supreme and more value-laden challenge of reaching an international consensus on the definition of terrorism. This definitional ambiguity impinges directly on the challenge of reconciling international legal and regulatory frameworks on e-payment systems. When the risks and challenges are inherently domestic and international, then the solutions to adopting a robust, international CFT framework must be agreed and implemented on a global basis.

If some countries do not cooperate with CFT regimes on the grounds that the definition of terrorism is not acceptable, then the integrity of the entire system is undermined.

> **"Surprisingly, some of the world's largest telecommunications and financial services firms have not proactively adopted a robust KYC screening method to identify potential terrorists and criminals."**

While acknowledging that there will be some new challenges in the KYC process for e-payment services, it is somewhat surprising to note that the principals behind these initiatives – some of the world's largest telecommunications and financial services firms – have not proactively adopted a robust KYC screening method to identify potential terrorists and criminals.

Some of the clients may indeed be poor country folk; yet the business interests behind m-banking initiatives certainly are not and should have the capacity to take more effective CFT measures.

If defining m-banking providers as non-banks is a problem, is the alternative of defining them as banks preferable?

International regulatory frameworks (i.e., the United Nations) are stymied by the notorious problems in regard to crafting a universally accepted definition of terrorism. Without being drawn into the futile and stale freedom fighter v. terrorist debate, this report identifies a relevant precedent that may offer some hope for overcoming not only definitional disputes but also jurisdictional ones also.

International maritime law provides an interesting and potentially useful precedent. Maritime laws dealing with piracy extend back at least 2,000 years when Roman statesman Marcus Cicero defined pirates in Roman law as *hostis humanis generis* (enemies of the human race).[1]

[1] For more information see: Douglas R. Burgess Jr., "The Dread Pirate Bin Laden," *Legal Affairs*, July/August 2005.

Nearly a millennium and a half after the fall of Rome at the 1856 Declaration of Paris, European states – who used pirates as proxy non-state saboteurs against other states – agreed to extirpate the scourge of piracy.

The states involved established a legal precedent determining that pirates were to be considered enemies of the human race and even created a distinct legal category separate from individuals and states whereby they could be captured wherever they were found by anyone who found them; in essence, providing universal jurisdiction for arrest and prosecution. The 1952 and 1982 UN Conventions on the Law of the Sea echoed the Paris Declaration and defined piracy as "any illegal acts of violence or detention, or any act of depredation, committed for private ends." Pirates are the only type of criminal subject to this definition and special jurisdiction.

Private wars for private means could in a broad sense also apply to the wars that terrorists wage against states and civilians. In the interest of resolving the definitional and possibly jurisdictional disputes that hinder cooperation on counterterrorism and CFT in particular, perhaps a similar definition and legal framework could apply to the fight against terrorists and their financial backers.

Conclusion: the way forward

On a macro level, there are many factors contributing to an ambiguous regulatory environment regarding e-payment systems and CFT. Jurisdictional and definitional issues will continue to constitute key obstacles in regulating e-payment systems.

E-payment services intersect with global information technologies and, like the Internet, raise difficult questions about whose responsibility and national right it is to interdict criminals when the jurisdiction is not clear.

On the definitional front, reaching a consensus on the type of financial service that e-payments constitute is at its core a technical, objective question.

However, reaching a consensus on the definition of terrorism requires the reconciliation of fiercely held normative values that can seem contradictory if not incompatible. Therefore, greater progress in the near-term may be had by concentrating on technical definitions of e-payment systems and adopting suitable regulatory measures while recognizing that resolving the terrorism definition debate is a longer-term goal.

On a micro level, the volume of potential transfers via e-payment systems is likely to become staggering. If traditional banks still struggle with AML/CFT requirements and good KYC procedures, then adequate regulation of these new forms of payment could be more difficult not only by degrees of difference but potentially by orders of magnitude.

"The nebulous regulatory framework for e-payment systems therefore necessitates that service providers take the initiative to implement sound KYC policies – the bedrock of any successful CFT regime."

The nebulous regulatory framework for e-payment systems therefore necessitates that service providers take the initiative to implement sound KYC policies – the bedrock of any successful CFT regime. Integrating a KYC screening solution is the first step.

It is clear that the costs of not taking the appropriate steps may sully the reputation of a burgeoning industry and could thus erode the future financial success of individual organizations and stakeholders engaged in this high-growth space.

Regulatory bodies and financial institutions alike hold the front lines in the fight against terrorist finance, the lifeblood of terrorist organizations and attacks.

If the institutions that constitute the financial community fail to take strong, effective measures to mitigate the terrorist financing risks inherent in emerging e-payment systems, the hard won progress in combating terrorist finance post-9/11 could be severely weakened.

Join us next year for many more compelling and thought-provoking articles about the threat of terrorism, and the latest on counter terrorism financing initiatives.