Terrorist Financing: The Risk of Prepaid Cards

by Carole Margolis - World-Check Terrorism & Insurgency Unit

08 July 2008: External state support for terrorist and insurgent groups has become increasingly limited, causing these illicit actors to adopt a dizzying array of funding strategies. Among these, new payment systems including prepaid cards, mobile banking and e-currencies have emerged as a particularly worrisome domain that terrorists can exploit to fund their support infrastructures and organizations.[1] This paper addresses the terrorist financing risks associated with prepaid cards. Mobile banking and e-currencies have been addressed in previous Expert Talks.[2]

In recent years, huge leaps in information and communication technologies have fueled an increased convergence between the telecommunications and banking industries. This has resulted in new types of international payment systems characterized by an increased ability to move money quickly and cheaply across jurisdictions. While these new systems hold vast potential for legitimate users, they also offer a number of opportunities for terrorists and criminals. The implications for countering the financing of terrorism (CFT) are that terrorists may increasingly by-pass conventional banking and money transfer systems, thereby making it more difficult for regulators and CFT agencies to identify and trace clandestine transactions.

In February 2008, the Financial Action Task Force (FATF) indicated that new payment methods, also known as 'e-money' or 'digital cash',[3] were a major concern because they effectively provide terrorists with additional means of raising, moving and storing money anonymously and instantaneously. Furthermore, plastic cards have become increasingly vulnerable to the proliferation of theft and fraud.

Several types of cards are particularly at risk including standard or prepaid payment cards (debit/credit) issued by a financial institution and prepaid or stored-value cards issued by retailers and telecom providers (gift card/calling card). This exposes the banking and finance industry, telecommunications providers, processing companies and consumers to a wider spectrum of threats such as fraud, money laundering and terrorist financing.

Plastic cards can be exploited to enable terrorist funding through money laundering operations and identity theft schemes, to sustain both their day-to-day operational needs and broader support activities.

A prepaid card looks like a credit or debit card, and gives users the ability to purchase products and services but with the crucial difference that only the preloaded balance can be spent. These cards are linked to an existing standard credit card or ATM/debit card account and usually carry the logo of a major card service provider such as American Express, MasterCard, or Visa.

1. See FATF's report: http://www.oecd.org/dataoecd/30/47/37627240.pdf on New Payment Systems
2. See John Solomon's three-part series on mobile banking and digital currencies for more information http://www.world-check.com/experttalk/2007/.
3. http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf

The prepaid card will 'ride the rails' of the existing account, meaning that while the opening of the existing account should necessitate stringent identification procedures by the card issuer, the application for the prepaid card will not require any information on the cardholder[4].

A thief in possession of another person's bank account information could therefore apply for several prepaid cards in all anonymity and constantly reload them with money from the feeding credit or debit account.

Prepaid gift cards represent a rapidly growing multi-billion dollars business, notably in the US where they are issued by major retailers such as Neiman Marcus, Safeway and Starbucks. Some cards are closed-system cards and can be used only at the issuing retailer while others are open-system cards. Open-system cards usually have the logos of major card service providers. They can be reloaded online or at checkout counters and provide the additional advantage of withdrawing money at ATMs worldwide. The open-system cards appear to pose the greater threat. Industry specialists have warned that prepaid cards represent a dangerous 'blending of a bank and nonbank product', since they enjoy ATM privileges but are not linked to monitored personal bank accounts[5]. Although at some point cardholders are supposed to provide basic identification to card issuers, in reality it can be hard to trace ownership.

Prepaid cards and gift cards offer a similar benefit. They can be loaded with money and then easily transported or smuggled across borders, inasmuch as they function like electronic purses. Meanwhile, these money flows will fall outside the scope of any kind of regulatory oversight or audit trail.

Identified risks include recruiting card mules (i.e. international students) to purchase prepaid cards; the mailing or shipping of prepaid cards out of a country; and the structuring and layering of numerous small deposits on various cards to hide either the origin or the destination of funds. Another technique used to transmit funds involves disposable prepaid mobile phones linked to a prepaid card or credit card account.

A terrorist financier may link the card to his phone and register with a mobile payments service provider using his mobile phone number, the stored value card and an anonymous free e-mail account. He may then use the phone to wire money via an m-service provider to a fellow cell member's own stored-value card. The recipient, who may be in another country altogether, will then be able to withdraw the funds credited to his stored-value card at any available ATM.

The disposal of the incriminating mobile phones on both ends will effectively ensure a speedy and anonymous transaction that will look like only a small detail on a credit card statement[6]. While card fraud seems to be a well known funding method in criminal circles, few reported cases have yet to involve terrorists. Most terrorism experts contend, however, that this image is deceptive and that prepaid cards might well represent a great unseen danger. A well documented case is that of the Mughal network, a cyberterrorist cell that operated in the United Kingdom. In December 2005, Tariq al-Daour, Younis Tsouli (aka Irhabi007) and Waseem Mughal were arrested in London for allegedly generating some £1.8m (US$3.5m) from identity theft and credit card fraud. The network reportedly stole over 37,000 credit card numbers using a variety of techniques.

4. http://www.nbpca.com/docs/NBPCA-AML-Recommended-Practices-080220.pdf
5. http://moneycentral.msn.com/content/banking/p137668.asp
6. http://www.creditcards.com/credit-card-news/credit-cards-terrorism-1282.php

These included phishing, whereby fake e-mails were sent to solicit personal information and trick Internet users into giving up credit card numbers and other personal information; running counterfeit websites such as a fake eBay site for US customers; and sending fake e-mails with Trojan horses, computer programs embedded in innocent-looking e-mail messages that give criminals control over infected computers[7].Records show that cell members purchased hundreds of prepaid cell phones, and over 250 airline tickets using 110 different credit cards at 46 airlines and travel agencies, in addition to other equipment earmarked for various jihadi groups[8]. Money was also laundered using online gambling sites such as AbsolutePoker.com, BetFair.com, BetonBet.com, Canbet.com, Eurobet.com, NoblePoker.com and ParadisePoker.com[9].

Al-Daour and his accomplices used accounts set up with stolen credit card numbers and stolen identities of Internet gambling site members. The accounts were then used to rack up winnings to help raise funds. In total, 350 transactions were conducted at 43 different online wagering sites, using more than 130 compromised credit card accounts. Winnings were later withdrawn and transferred to online bank accounts controlled by cell members.

At least two other cells affiliated with the Liberation Tigers of Tamil Ealam (LTTE) have been identified in recent years. In October 2007, four members of an LTTE credit card fraud ring – Ibrahim Abdifatah, Sivapalasri Velayuthampillai, Usman Mahmood, and Krishantha Rasanayagan – were arrested in New York for plotting to withdraw US$250,000 in cash with cloned credit cards from ATMs throughout the city.

They were found to be in possession of over 250 blank credit cards, a coding machine, lists of financial accounting information and a laptop. It was discovered that the credit card information used to commit the fraud originated from two filling stations in the UK[10]. More recently, in January 2008, three suspected members of a UK-based LTTE cell – Kirubakaran Selvanayagam Pillai, Sethukavalar Saravanabavan, and Lojanand Srianandan – were detained in Toronto, Canada on charges of credit and debit card fraud for possessing 41 gift cards containing bank account and debit information from individuals in the UK[11].

Recent uses of credit cards by terrorists underscore the extreme vulnerability of plastic cards to misuse for both criminal activities and terrorist financing purposes. The scale of the card fraud will presumably vary by type of terrorist organisation. Most recent cases in Western countries involve occurrences of small scale petty crime perpetrated by either decentralised self-sustaining cells or networks infiltrated with the express purpose of raising and remitting money to the parent organisation. Quasi-state-like terrorist organisations such as the LTTE, however, are suspected of actively cooperating with criminal gangs worldwide in a crime-terror nexus designed to generate ever increasing amounts of funding. It is possible that future card fraud schemes will become more organised and substantial, thereby eliciting the need for firmer financial and regulatory controls.

Carole Margolis is a senior analyst in World-Check's Terrorism and Insurgency Research Unit. She is an expert on the funding strategies of terrorist and insurgent movements in the Middle East, North Africa and Western Europe. A graduate of Science Po in Paris, Margolis holds a Master's degree in International Security Studies from the University of St Andrews in Scotland. She formerly worked as a military strategy analyst for the French Army General Staff.

7. http://redtape.msnbc.com/2007/07/cyber-terror-an.html
8. http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945_pf.html
9. http://www.gambling911.com/online-poker-rooms-072007.html
10. http://www.defence.lk/new.asp?fname=20071016_08
11. http://toronto.ctv.ca/servlet/an/local/CTVNews/20080130/gift_card_fraud_080130/20080130/?hub=TorontoHome