



Photo: Scott Morrison

By Jennifer L. Hesterman

All good investigators know the value of the money trail to an investigation. Whether tracing a petty fund in a continuing criminal enterprise or millions of dollars moved by an international terrorist group, an investigator can learn a great deal about the unique story of an operation by paying attention to the origin, path, and destination of the money. Often, this story yields evidence that allows infiltration of the group, identification of its key players, and ultimately, the eradication of the organization or one of its cells.

Although improved technology has greatly improved the quality and ease of daily life in recent years, it is not without its problems. One downside to technological advances is that terrorists and criminals are users, just like law-abiding citizens. With this new technology comes innovative means to move, store, and liquidate funds, often in ways that are not transparent or detectable. Unfortunately, as corporations continue to rush cutting-edge products to market, technology is sometimes fielded without complementary safeguards to prevent exploitation by individuals who are engaged in illegal activities. The emerging nexus between telecommunications technology and illicit financial transactions is one such area of concern.

NEW PAYMENT METHODS

The Financial Action Task Force (FATF) is an intergovernmental body that works internationally to combat money laundering and terrorist financing (ML/TF). In recent years, the FATF has become increasingly concerned over so-called “new payment methods,” or NPMs.¹ NPMs, also referred to in the finance industry as “e-money,” “digital cash,” or “e-cash,” facilitate the transfer of value between individuals and organizations by way of the Internet, cellular phones, or other electronic methods.

It is important to note that e-cash was intended to be analogous to physical cash

by design; thus, it offers unconditional anonymity and is impossible to trace because payments are not linked to a particular customer account. Other benefits associated with the use of e-cash include rapid transaction times and the ability to accumulate value. Obviously, these characteristics make NPMs appealing to those engaged in nefarious activity.

Common examples of NPMs include the following:

- **Internet payment services.**

Through privately held companies labeled by the FATF as “nonbanks,” Internet payment services allow users to pay bills online, make purchases at participating websites, buy and sell items from auction sites, and contribute to charities. Niche companies have also emerged that serve markets not engaged by larger providers, such as Internet gambling sites. Setting up an account with a nonbank is simple and requires little personal data, most of which can easily be fabricated. Money may be accumulated in a nonbank account; then, when the account’s owner is ready, the balance can be liquidated in several ways, including through untraceable debit cards that can be used to withdraw cash from ATMs worldwide.

Notably, a few nonbanks operate globally, and their transactions can cross borders. Such companies need only follow licensing and regulatory guidance in the countries in which they are based. Therefore, the regulations that apply to

The ease of obtaining and using open system cards opens the door for “smurfing,” a money-laundering activity in which criminals spread a great deal of cash across many sources, concealed from regulators and law enforcement.

individual nonbanks vary and directly correlate to the strength of the rule of law in each nonbank's host nation, as well as whether ML/TF is an area of concern or focus in that country. Of further concern are offshore nonbanks, which offer even more anonymity to customers and fewer restrictions on transaction limits.

- **Stored value cards.** This popular category of NPM includes phone, retail, and credit cards that can be purchased with cash at many grocery and drug stores. The owners of these cards remain anonymous, an unlimited number of cards may be purchased and held by one person, and any subsequent use is virtually untraceable. Stored value cards can be divided into two types:

- **Limited-purpose or closed-system cards.** This category consists of merchant-issued gift cards and calling cards. Such cards can only be used for specific purposes, may have an expiration date, and usually cannot be reloaded. However, there is still a ML/TF risk associated with these cards. In particular, an unlimited amount of cards can be purchased anonymously with cash and then sold through online auction sites, with the value transferred to a nonbank for subsequent liquidation through an untraceable ATM card.



- **Multipurpose or open-system cards.** Of much greater ML/TF risk are multipurpose or open-system

stored value cards, which bear the name of a major credit card company and may also be purchased with cash in unlimited quantities. Value can be added to these cards through an online nonbank or with cash at a participating retailer. Then, when the cardholder is ready to cash out, money can be withdrawn from most ATMs, or these cards can be sold online with payments being laundered through the nonbank. As long as the amount doesn't exceed the \$10,000-per-day threshold that necessitates generation of a currency transaction report (CTR), such transactions will occur off the radar screen, with no documentation.

The ease of obtaining and using open system cards opens the door for "smurfing," a money-laundering activity in which criminals spread a great deal of cash across many sources, concealed from regulators and law enforcement. Indeed, the multipurpose card industry is booming; in fact, the National Drug Intelligence Center's 2006 threat assessment indicates there are already more than 7 million MasterCard and Visa prepaid debit cards in circulation.²

- **E-purse.** Unlike a stored value card, which has a magnetic strip, an e-purse stores value directly on a card itself using a microchip. Currently, the most popular e-purses are the so-called "smart cards" used for public transportation, tollbooths, parking garages, and vending machines. These cards can be reloaded with cash at specialized vending machines and are also sold through online auctions.

In addition, many cell phones will soon be transformed into e-purses through new technology that imbeds debit or credit card information into the phones' SIM cards. This method,

dubbed "mobile ticketing," will allow users to simply tap their phone against a terminal to complete a sales transaction.³

- **Mobile payments.** The State Department recently issued its latest International Narcotics Control Strategy Report,⁴ which includes a new section entitled "Mobile Payments—A Growing Threat."⁵ This document sounds the alarm on a new type of remittance method with an extremely high ML/TF risk.

Mobile payments, also known as "m-payments," "proximity payments," or "micropayments," are point-of-sale cash transactions made through a mobile device such as cell phone or personal data assistant. The sender takes the cash to a remittance center, which charges a modest service fee. The center then "sends" the amount to the recipient's mobile account, also known as an e-wallet. The recipient gets a text message on his or her mobile device indicating that the sum has been placed in the account. The cash can then be collected at any participating remittance center, retail store, or, if business evolves as predicted, fast-food outlet. Although the entire transaction takes mere minutes, the ML/TF implications are tremendous and inevitable.

One of the world's leading information technology research and advisory companies, Gartner, Inc., predicts that mobile payment services are just beginning to take hold, with today's projected 32.9 million users worldwide swelling to 103.9 million users by 2011.⁶ These services are heavily marketed to segments of the world population that are unbanked or underbanked due to the cost of maintaining accounts or a lack of access to banking facilities. Consider the fact that over 3 billion people in the



Similarly, e-dinar, an offshoot and former partner of e-gold, provides a unique, niche service. Since 1992, the company has minted its own gold Islamic dinar to provide its customers a means of exchange in line with the religious specifications found in the Koran.

world have mobile phones, but only 1 billion people have bank accounts;⁷ given these statistics, the market for mobile payment services is vast.

The recent intersection of two popular NPMs has also led to emerging ML/TF concerns. Specifically, a partnership between a major Internet payment service and a global cellular phone company now allows the instantaneous transfer of funds directly between nonbank accounts. Use of a “throw-away” cell phone, anonymously purchased with cash, will make any of type of m-payment transaction even more obscure and difficult to trace.

- **Digital precious metals.** Finally, another NPM worth watching is the emerging practice of using digital precious metals as a way to store and move large amounts of currency. Through this service, users create an account and then secure cash deposits against gold, silver, and platinum. The major companies engaging in this NPM

actually hold vaulted precious metal in the name of the investor, employing major companies such as Brinks for security. Gold is the most popular product on the market, with over \$1 billion worth of transfers through the e-gold Ltd., corporation in 2007 alone.⁸ Notably, Brinks stores over 48,000 fine troy ounces of gold purchased online in their vaults located around the world.⁹

Similarly, e-dinar, an offshoot and former partner of e-gold, provides a unique, niche service. Since 1992, the company has minted its own gold Islamic dinar to provide its customers a means of exchange in line with the religious specifications found in the Koran. Therefore, the Islamic dinar retains a unique fungibility and can be directly used to pay zakat and dowry as required by Islamic law.¹⁰

The FATF reports that some companies in this international business allow investors to remain anonymous.¹¹ Indeed, a quick Internet query yields

several sites that indicate metals may be purchased using a nonbank account and possibly even with untraceable stored value credit cards.

CRIMINALS AND TERRORISTS ARE TURNING TO NPMs

Evidence shows that those individuals and groups engaged in criminal or terrorist-related activities are already turning to NPMs as a way to move and store money. In fact, the number of suspicious wire transfers in previously heavy markets is down, perhaps as a result of an increase in the use of NPMs to move money.

- **Ample evidence of exploitation.**

Several high-profile cases confirm that NPMs are attractive to criminals and terrorists. Examples include the following:

- In 2008, Indonesian police reported that radical Islamic terrorists were observed selling phone cards, generating upwards of \$500 per day to fund operations.¹²
- A Mexican criminal caught at the U.S. border in 2005 was using stolen credit cards to transfer value to prepaid cards.¹³
- In 2001, a suspicious activity report (SAR) filed in the United States detailed the acquisition of more than 300 prepaid cards by a single individual who used them to transfer almost \$2 million to Colombia.¹⁴
- In 2004, German tax investigators discovered a case of ML through prepaid cards. Two participants of a criminal fraud/embezzlement scheme had transferred parts of their shares of the criminal proceeds onto several prepaid cards. In this case, more

than €350,000 were hidden and laundered.¹⁵

- Members of the criminal networking site “Shadowcrew” used e-gold to send and receive payments for illicit goods and services.¹⁶
- **Cards as a form of payment for illicit activity.** In lieu of traceable currency, stored value cards are becoming the preferred form of payment for illegal services rendered. Some examples in which these cards were used are as follows:
 - A joint Immigration and Customs Enforcement/Internal Revenue Service investigation uncovered a relationship between a U.S. criminal organization and a Mexican co-conspirator who was creating fake credit cards. The co-conspirator was paid for his assistance with retail gift cards. He then sold the gift cards and moved the cash back across the U.S. border to buy phone cards, which were then smuggled into Mexico in a separate operation.¹⁷
 - The U.S. Drug Enforcement Agency uncovered an operation in which drug dealers were loading cash onto prepaid cards and then sending the cards to suppliers outside of the country, who in turn liquidated the funds using ATMs.¹⁸
 - In 2005, U.S. Immigration and Customs Enforcement officials initiated an investigation into a state employee in Ohio who was selling fraudulent drivers’ licenses and identification cards in exchange for prepaid telephone cards.¹⁹
- **Stored value cards are a smuggling risk.** The smuggling of bulk currency out of the United States is on the rise, and according to officials, it is “the largest and most significant drug money laundering threat facing law enforcement.”²⁰ Many

experts believe that prepaid stored value cards are now an attractive alternative to bulk cash smuggling.²¹ Cards are not subject to the same rules as cash at the border. For instance, cards cannot be seized if the amount carried exceeds the \$10,000 threshold and is not properly declared.

Cards can easily be smuggled without detection onboard a commercial aircraft, train, bus, or ship. They are lighter in weight and more compact than a bundle of equivalent-value paper bills. These physical properties, along with easy, anonymous acquisition and lack of regulatory guidance, make cards the ideal smuggling mechanism.

THE BATTLE AHEAD

The potential exploitation of NPMs by criminals and terrorists is a global problem; thus, it must be addressed with a comprehensive set of regulatory guidelines that are adhered to by all parties. Until this massive undertaking is realized, self-regulation within the industry would be a positive step forward. Most importantly, there must be ongoing dialogue between counter-terrorism experts who research emerging ML/TF risks and operators on the front lines, as each group has information the other needs to ensure a united, relevant, and uncompromising strategy in the War on Terror.

Traditional money laundering makes “dirty” money “clean” after a crime has been committed; today, however, terrorists are increasingly laundering “clean” money by moving and storing it for the purposes of financing training and future operations. No matter which type of laundering a criminal organization conducts, that group stands to benefit from the nexus between telecommunications, for-profit

**HONOR YOUR
FINEST AND
BRAVEST WITH
QUALITY**

LIBERTY ART WORKS, INC.
HONORING YOUR BRAVEST AND FINEST
ST. LOUIS, MISSOURI

WWW.LIBERTYARTWORKS.COM
888-411-7744
Proudly Made in the U.S.A

Circle 195 on Reader Service Card

CellAntenna
SOLVING CELLULAR COMMUNICATION PROBLEMS WORLDWIDE

**RAPID DEPLOYED REPEATER FOR
EMERGENCIES**

CALL NOW!
(954) 340-7053

CAE750-RDCRS

DUAL BAND PORTABLE CELLULAR REPEATER COVERS UP TO 15,000 SQ. FT. CAE750 OFFERS THE PORTABILITY AND POWER FLEXIBILITY NEEDED FOR DISASTER RECOVERY AND EMERGENCY OPERATIONS DUE TO NATURAL OR TERROR-RELATED DISASTERS BOTH INDOORS AND OUTDOORS.

GET A SIGNAL IN AN EMERGENCY!

DESIGNED SPECIFICALLY FOR EMERGENCY OPERATION CENTERS AND RESPONSE VEHICLES TO ENSURE RELIABLE, CLEAR CELLULAR SIGNALS. INCLUDES A BATTERY BACKUP SYSTEM PROVIDING THE UNIT WITH UP TO 8 HOURS OF RECHARGEABLE BACKUP POWER.

THIS IS A PROFESSIONAL UNIT, PLEASE CALL FOR PRICING

CellAntenna.com

CellAntenna Corporation | 12453 NW 44th Street | Coral Springs, FL 33065
Tel. 954-340-7053 | FAX 954-340-9086 | Email: sales@cellantenna.com

Circle 197 on Reader Service Card
40 *The Counter Terrorist* ~ September/October 2008

“nonbanks,” and the banking industry. The lack of physical evidence in mobile transactions, compounded by the ease of moving and storing money through various NPMs, should be of great concern to policy makers and the law enforcement community alike. ●

ABOUT THE AUTHOR

Jennifer Hesterman is a retired Air Force colonel. She is currently a senior analyst for The MASY Group, a global intelligence and risk Management firm, as well as a professor at American Military University, teaching courses in homeland security and intelligence studies. Her book, Transnational Crime and the Criminal-Terrorist Nexus was published in 2005.

NOTES:

1 Financial Action Task Force, *Report on New Payment Methods* (Paris: Author, 2006), <http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf> (accessed July 22, 2008).

2 U.S. Department of Justice National Drug Intelligence Center, “Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods” (Johnstown, PA: Author, 2006), <http://www.usdoj.gov/ndic/pubs11/20777/20777p.pdf> (accessed July 22, 2008).

3 George Smith Alexander, “It’s Time to Shop through Cell Phones,” *Rediff.com*, December 22, 2003, <http://in.rediff.com/money/2003/dec/22betterlife.htm?zcc=ar> (accessed July 22, 2008).

4 United States Department of State, *International Narcotics Control Strategy Report* (Washington, DC: Author, 2008), <http://www.state.gov/p/inl/rls/nrcrpt/2008> (accessed July 22, 2008).

5 United States Department of State, “Mobile Payments—A Growing Threat,” in *International Narcotics Control Strategy Report*, vol. 2 (Washington, DC: Author, 2008), <http://www.state.gov/p/inl/rls/nrcrpt/2008/vol2/html/101346.htm> (accessed July 22, 2008).

6 Gartner, Inc., “Gartner Says Worldwide Mobile Payment Users to Total 33 Million in 2008,” press release, April 21, 2008, <http://www.gartner.com/it/page.jsp?id=652308>

(accessed July 22, 2008).

7 “Mobile Phones to Send Money Home,” *BBC News*, February 12, 2007, <http://news.bbc.co.uk/2/hi/business/6353797.stm> (accessed July 22, 2008).

8 e-gold Ltd., “e-gold Benefits,” <http://www.e-gold.com/benefits.html> (accessed July 22, 2008).

9 e-gold Ltd., “Gold Held by the e-gold Bullion Special Purpose Trust Stored at Brinks,” http://www.e-gold.com/examiner_blowup.asp?id=400&metal=1 (accessed July 22, 2008).

10 e-dinar, “What Is the Dinar?” http://www.e-dinar.com/html/1_2.html (accessed July 22, 2008).

11 Financial Action Task Force, *Report on New Payment Methods*.

12 Eva C. Komandjaja, “Indonesia: Terrorists ‘Selling Phone Cards,’” *Jakarta Post*, November 22, 2005, <http://www.asiamedia.ucla.edu/article-southeastasia.asp?parentid=34173> (accessed July 22, 2008).

13 Chester Dawson, “Prepaid Cards: Candy for Criminals?” *BusinessWeek.com*, December 12, 2005, http://www.businessweek.com/magazine/content/05_50/b3963115.htm (accessed July 22, 2008).

14 Financial Action Task Force, *Report on New Payment Methods*.

15 *Ibid.*

16 Brian Grow, “Gold Rush,” *BusinessWeek.com*, January 9, 2006, http://www.businessweek.com/magazine/content/06_02/b3966094.htm (accessed July 22, 2008).

17 U.S. Immigration and Customs Enforcement, “Prepaid Cards an Emerging Threat,” *Cornerstone Report*, December 2006, <http://www.ice.gov/doclib/pi/cornerstone/pdf/CS1206.pdf> (accessed July 22, 2008).

18 <http://www.ice.gov/doclib/pi/cornerstone/pdf/CS1206.pdf>

19 Financial Action Task Force, *Report on New Payment Methods*.

20 U.S. Department of the Treasury, et al., 2007 *National Money Laundering Strategy* (Washington DC: Author, 2007), <http://www.treas.gov/press/releases/docs/nmls.pdf> (accessed July 22, 2008).

21 U.S. Department of Justice National Drug Intelligence Center, “Prepaid Stored Value Cards.”