

# AML Services International, LLC

## ***Mobile Phone Laundering: Fact or Fiction?***

By Saskia Rietbroek, CAMS

March 2008

In Europe and Asia, and to a lesser extent, the United States, you can pay for groceries using their cell phones. You can make payments wirelessly with your cell phone. You can also transfer funds to another telecom subscriber using SMS text messages. Authorization typically occurs by keying in a PIN (personal identification number) associated with the person or the mobile device. The customer receives a text (SMS) confirmation after the transaction is conducted. Sounds easy, right?

Does this mean that a money launderer can use his cell phone to launder money? And if so, what can be done by telecom providers to control the risk? Some argue that even if mobile payments could theoretically be used for money laundering, the service is typically used for micro-payments and involves amounts too paltry to be of interest to a money launderer. Before answering these questions, let's take a look at how mobile payments work.

### *Linked to bank account or not?*

The most basic form of mobile payment is when the customer uses the cellular phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards. Because of the involvement of a bank account at a regulated institution, the customer has been identified when the underlying bank or credit card account was opened.

But the mobile payment can also function as a stand-alone facility without a direct underlying bank or payment card account. In this case, the telecom operator acts as a payment intermediary to authorize and settle the payment in its own system. In the stand-alone facility, there are prepaid and postpaid payment services: In a postpaid system, the telecom operator allows the phone owner to charge certain payments to the phone bill. In a prepaid system, the telecom operator lets the phone owner fund an "account" (this is not a bank account) held by the telecom operator for the purposes of making prepaid payments. In this stand-alone option, telecom companies engaged in these activities may not be overseen by a country's central bank or other banking regulator in regard to money laundering purposes.

### *How to abuse the system*

Here is how the launderer can abuse the mobile payment system: The launderer buys a prepaid card for any amount and loads it with ill-gotten money. He then registers online with a mobile payment provider using a free anonymous e-mail account, the prepaid mobile phone number, and the money on the stored-value card. Of course, he provides a false identification number and a false address. Using the cell phone, the launderer then logs on to the payment service provider website and gives them the number of the mobile phone to which he wishes to transfer the funds from his prepaid card. The telecom company then sends a message to the receiver's phone number asking where to transfer the money. If there is a partnership with a bank, the recipient can request the

2008 © AML Services International, LLC

Tel. +1-305-608-7888

[www.nomoneylaundering.com](http://www.nomoneylaundering.com)

[saskia@nomoneylaundering.com](mailto:saskia@nomoneylaundering.com)

# AML Services International, LLC

transfer be made to his stored-value card and then withdraw the funds from any ATM, anywhere. The transaction leaves a minimal audit trail: two mobile phone numbers, the amount of the transaction, perhaps short instructions on the transmission, and reception.

This could create a situation where we have a minimal audit trail and anonymity, combined with functional similarity to a credit or debit card or remittance services. And all of this is virtually unregulated.

## *Risk mitigation*

**Amounts.** Money laundering and fraud issues can arise when the maximum transaction and loading amounts are high. When mobile phones are access devices to underlying bank and credit card accounts, limits may not be necessary. If the mobile payments are *not* linked to underlying bank accounts, the telecom provider often imposes a maximum per transaction per day to a few hundred dollars or euros, which limits the vulnerability to money laundering.

**Identification.** If the mobile phone service is prepaid and the funds used to facilitate mobile payments are also prepaid, the service provider may not be motivated to fully identify customers because of the absence of credit risk and legal requirements. It would be prudent to identify the customer and to verify the information provided in the registration process. Otherwise, there is no way for the telecom provider to know if the information provided is real or has been stolen from another person.

**Method of funding.** Mobile payments that draw on a prepaid account can be funded by adding money from a bank account, or from a debit/credit/prepaid card. Payment sources which have independently verified the identity of the phone owner and which maintain a record of the funds transferred to the mobile payment account are low risk. The use of cash to fund a mobile payment account, independent of other risk factors, may present some limited money laundering/terrorist financing risk. By limiting funding options, the risk can be mitigated.

**Usage limits.** Typically, payments can only be received for POS (point of sale) transactions by participating merchants or fellow service subscribers. Subscribers can also withdraw money from their mobile payment account directly from their bank account, or as cash from an ATM with a prepaid card. Limited transaction value and limited cross-border functionality can help reduce the risk.

## *Detecting the cell phone launderer*

The telecom firm may not be legally required to do so, but their internal policies and procedures or partnerships with banks may require them to report suspicious activity. In order to do this, they need not only to identify the customer, but also to keep records for every transaction (including tiny micro payments) in order to create patterns of transactions and to monitor for suspicious transactions. With pattern recognition technology, the mobile payment firm can determine if the activity is commensurate with what was expected from the customer. This is done using algorithms that predict and link data, and that generate alerts for investigations and further analysis. This way, the

# AML Services International, LLC

right software can help the firm distinguish suspicious from normal activity, and mitigate the risks presented by ingenious launderers trying to launder money with their cell phones.

## Detection scenarios

- A mobile payment account that is used in an ATM to access cash from a prepaid account operates in a similar way to a debit card accessing a bank account via an ATM. Software can use detection scenarios that are also used in a bank account setting, such as transactions above certain amounts, foreign withdrawals combined with up-front cash loading within a certain period, and transactions in certain high risk countries.
- If a certain threshold for number of transactions is reached for a particular account holder, an alert can be generated by an automated monitoring solution for further investigation. Different thresholds can be set for mobile payment account holders with different risk classifications
- A detection scenario can be created for limits on the acceptable range of transfers for certain cards. An alert is generated when the limit is reached.
- With a network or link analysis feature, automated monitoring solutions can identify, investigate, and trace links between mobile account holders. This can help uncover a money laundering trail. It allows the firm to build an overview of account holder relationships: Who is transmitting funds to which other account holder?
- Automated monitoring solutions can import an initial risk score that is assigned by the firm to its customers in order to –on an ongoing basis - monitor the activity. This way the firm can see if the initial risk score still applies, or must be changed.
- Automated monitoring solutions can compare the activity of a particular customer with the historical profile of that customer. It can compare patterns within peer groups such as customers living in the same zip code or with a similar age.

Risk is the likelihood of a given threat attacking a particular vulnerability and the resulting impact. The likelihood of cell phones being used for money laundering is not that big if appropriate safeguards are being used. On the other hand, if a firm is mentioned on the front page of the newspapers as being involved in a money laundering or terrorist financing case, the impact is tremendous. A telecom firm's reputation can be permanently damaged if caught up in a financial crime scandal. Only with appropriate risk management, a firm can isolate the risks and identify potential mitigation options to stay out of trouble, and out of the newspapers.

*From 2001 – 2005, Saskia Rietbroek, CAMS, served as the original Executive Director of the Association of Certified Anti-Money Laundering Specialists (ACAMS). She serves on the Advisory Board of ACAMS. In 2005, she founded AML Services International LLC and conducts money laundering audits and training for financial institutions in the US, Caribbean, and Latin America. She is also Financial Crime Advisor to NetEconomy, a leading company in financial crime detection. She is based in Miami, FL.*  
[saskia.rietbroek@gmail.com](mailto:saskia.rietbroek@gmail.com).