# Journal of Internet Banking and Commerce

*An open access Internet journal (http://www.arraydev.com/commerce/jibc/)*

*Journal of Internet Banking and Commerce, December 2008, vol. 12, no. 3*
(*http://www.arraydev.com/commerce/jibc/*)


## Payments and Inclusion:

## From Branchless Banking to Bankless Banking


**Dave Birch**
*Email:* mail@dgwbirch.com
*Web:* http://www.dwgbirch.com
Dave G. W. Birch is a Director of Consult Hyperion. He chairs the Digital Money Forum and co-edits the Digital Money Reader.


For many governments, financial inclusion is an important element of policy and it is sensible for both businesspersons and technologists to focus on ways to support this policy strand and see it implemented effectively. In the U.K., there is a Financial Inclusion Taskforce to oversee progress, the Treasury has a "Payments and Inclusion Team" and while financial inclusion is not a statutory obligation on the Financial Services Authority (FSA), I am assured that it is something they do take seriously in the context of other objectives on consumer protection and public awareness. The government's 2004 report on Promoting Financial Inclusion highlighted some of the costs of exclusion [1]:

- Higher charges for basic financial transactions and credit. The lack of access to a bank account means that certain financial transactions such as money transfer and cheque cashing may be more expensive;
- No access to some products and services. Many services, such as contract mobile telephones, require a bank account for regular direct debits;
- A lack of security in holding and storing money. Operating solely on a cash budget leaves people more vulnerable to loss or theft;
- Barriers to employment, because a bank account for receipt of wages is a basic requirement for some employers; and

- Entrenching exclusion. Having no formal banking or credit history at all can be as much of a disadvantage as an impaired credit history in accessing certain financial services.

Unfortunately, life (and government policy) is rarely simple. The law of entirely predictable consequences means that there is a growing tension between the policy of financial inclusion and the policy of financial exclusion (otherwise known as anti-proceeds of crime, anti-money laundering, anti-terrorist financing and the like). This tension leads to problems that are not resolvable by technologists, but the technologists can help to inform next generation policy by highlighting them.

My son wanted to play an online game, one of those where the players are wizards and dragons and suchlike, but he needed a card to pay for it. I told him that I was happy for him to do this, but in no circumstances would I let him use his real name. I'm not comfortable with children being required to divulge their real names in online environments. (Come to that, I'm not comfortable with giving out any personal details on line.) I happen to have a U.K.-issued prepaid card that I'd been trying out in connection with a project I'm working on, so I gave it to him and told him to use it. It didn't work. When I called to find out why, I was told it was because I hadn't registered the card and my son couldn't use it online until I had done so. I went to the relevant webpage and was confronted with boxes and boxes of information to fill out, about how long I'd lived at my address, my passport number and inside leg measurement. I took one look at it all and gave up. All I wanted was a low-value, cash replacement "card" and since the European Money Laundering Regulations have an exemption for cards with an annual account throughput of less than €2,500 I didn't think it would be so much hassle to get one.

It's not like such products do not exist anywhere. NZ Post has been distributing what sounds like an excellent product, pretty similar to pre-paid Visa cards distributed by the post offices in Italy. The pre-paid card lets anyone make anonymous purchases over the web and is encouraging more people to shop online. NZ Post has marketed the card primarily as an alternative to gift vouchers or giving cash, branding it as the Prezzy Card. To buy online (about 10% of the transactions), customers key in the number and expiry date on the card and use "prezzy card holder" into the name field, if required. Yet "fears are being voiced" that the cards could aid criminals and terrorists, and the regulators are being asked to look at the product [1].

Should the full weight of the Financial Action Task Force (FATF) be applied to a prepaid card being used for a $10 per month payment to a game operator? Not only does this prevent trade (and therefore prosperity) from growing, but I strongly doubt that it catches criminals and terrorists either. And where can this line of thinking go? Any further tightening of money transfer rules is pointless as it will become impossible (as opposed to very difficult) for the vast majority of ordinary people wishing to receive money transfers to comply, particularly with the Customer Due Diligence (CDD) and Know Your Customer (KYC) requirements [2]. This achieves nothing other than to force such people to continue to use informal networks with high social costs and less of an audit trail. How is that better for either the people involved or society as a whole?

We have to find a much better balance: It's all very well to perpetuate the "if you've nothing to hide, you've nothing to fear argument" for tracking and tracing every single miniscule transactions, but the drag that this imposes on the economy may well be unacceptable (setting aside any other moral concerns). We need a risk-based approach, where regulators set reasonable thresholds and focus on the areas of major risk instead

of holding back the whole cash replacement industry, not misguided attempts to hold back nascent industries. Are the World of Warcraft and Second Life really a hotbed on "online money laundering"? The Fraud Advisory Panel, set up by the Institute of Chartered Accountants in England and Wales, has said legal loopholes are exposing virtual world users to "a growing risk of theft and deception" (although they do go on to note that the dangers are "hypothetical" [3]). They even recommend treating virtual currencies like the Linden Dollar (the currency in Second Life) as "real money", although quite what the boundary between real and virtual actually means is not clear to me at all. The Panel's report also recommended that virtual world operators like Linden Lab to report suspicious financial transactions, just as for real-world banks and financial institutions, thus adding to the vast number of Suspicious Transaction Reports (STRs) filed every day.

**PIGGY BANK IN THE MIDDLE**

Putting cards and the Internet to one side for a moment, another great boon to terrorists (or, at least, terrorists who have never heard of 500 euro notes) will be mobile payments. Rachel Ehrenfeld, founder of the Terror Finance Blog calls the hook-up between the GSMA and MasterCard a "terrorist dream" [4]. David Nordell, another finance terror commentator, says, "Person-to-person transfers via mobile phones will be almost anonymous, and completely uncontrollable unless the regulators intervene and block these new services until ways are devised to track the flow of funds". (Whereas in the current system, people can use utility bills they printed out themselves and trivially-forgeable documents to open bank accounts.)

The worry is that "the m-payment process can leave little to no audit trail; perhaps, two mobile-phone numbers; the amount; and short and simple instructions on transmission and reception" [4]. So law enforcement officials have only the mobile phone numbers (and therefore the locations) of the criminals? The argument that international criminals would use schemes such as these to move money illegally it is, to my mind, fairly thin. Why would they go to the trouble of using a superficially anonymous but ultimately traceable prepaid instrument (and in the case of a mobile phone in instrument whose location is known with high degree of accuracy) instead of the cheap, convenient and highly effective alternative of the €500 note itself? Which is, of course, precisely what they do. When the Mexican police made last year's biggest-ever drug bust, they found more than $50 million in cash. Similarly, when the British police broke up a major money-laundering gang, they found that "hundreds of thousands of pounds in 'dirty cash' was being ferried up the M1 on an almost daily basis" [5]. Not top-up vouchers, not frequent flier miles, not pre-paid cards, but cash.

I can understand people being concerned and, as I've said, we need to address these concerns. But that doesn't, conversely, mean that all of the concerns are equally valid or have equal weight. Somehow, public policy needs to be at once holistic (in the sense that it balances all of the stakeholders legitimate concerns) but also specific enough to frame enforceable laws that will actually do some good. The benefits to society as a whole from farmers in sub-Saharan Africa being able to open mobile payment accounts without conventional identification documents and therefore participate in the wider marketplace greatly outweigh any risks that may result from the less stringent approach to AML that this implies. In fact, assuming that the maximum balance and maximum turnover bounds for such accounts are set realistically, it is difficult to imagine what any practical risks might be: If sending the odd €20 from Darfur to Dar-es-Salam really is a terrorist modus operandi, then they ought not to prove insurmountably difficult to contain.

## SIMPLIFY AND WIN

What I'm trying to get over here is that we should not get hysterical about the arrival of mobile banking and mobile payment services. The sky is not going to fall in because of low-value pre-paid or m-payment instruments and we are not going to help law enforcement find needles in haystacks by making the haystacks even bigger. What we need to do instead is to help the policymakers to find the right place to strike the balance between financial inclusion and exclusion, between monitoring and intrusion, between "security theatre" and worthwhile activities.

Why not take the €500 note as the benchmark for this balance? Any prepaid instrument with a maximum daily transfer of €500 and should be regarded as cash and regulated globally much as the FSA regulates Electronic Money Issuers (ELMIs) in the U.K. but with higher limits on both balances and annual transfers. In Europe, there is to be an additional chapter in the Payment Services Directive (PSD) to create a framework for electronic money institutions (alongside the frameworks for credit institutions and payment institutions) to perhaps this could form the basis of reciprocal international agreement.

In other words, anyone should be able to wander into a Post Office or wherever and buy a prepaid card with €500 loaded on to it and then do what they like with it: use it on eBay or in Marks & Spencers, send it to a grandson at University or back to the old country as a remittance. The immediate benefit to the poor (who lose some 20% of their annual remittances to charges or fraud [6]) would surely outweigh any marginal convenience offered to drug dealers. And if an international terrorist were to go round Post Offices buying a pre-paid card in each one and then sending €100,000 worth of cards to their uncle up the Khyber Pass, it would cost them a lot more than sending €500 notes (and the Post Office might well lose them anyway).

More realistic limits for KYC/AML and increasing competition in the provision of mobile payment services would bring (literally) hundreds of millions of people into the financial system would deliver a significant net welfare increase and make a huge difference to the daily lives of some of the poorest people.

## REFERENCES

[1] D. Birch. *Regulation of prepaid products* in *Electronic Finance & Payments Law & Policy* (May 2008).

[2] S. Cavill. *Money transfer: why mobile operators are leading banks* in *E-Finance & Payments Law & Policy* (Jun. 2008).

[3] A. Reuters. *UK panel urges real-life treatment for virtual cash*. at (14th May 2007).

[4] R. Ehrenfeld and J. Wood. *Terrorist funding in real time*. at http://www.public-integrity.org/article/invent_index.php?id=345 (11th Apr. 2007).

[5] M. Wainwright. *Eleven jailed in £500m 'dirty cash' case* in *The Guardian* (18th Apr. 2007).

[6] *Phoney finance* in *The Economist* (29th Oct. 2006).