New Payment Methods and Financial Crime Risks

by David Thomas

Statement of intent

Evolving technology continues to impact on how we do business and more specifically, how we transfer funds. New Payment Methods (NPMs), such as prepaid cards and mobile payments, present new opportunities for exploitation by criminals, a cause of concern for both potential users and providers. But what are the actual risks involved and what can NPM providers do to reduce that risk?

Risk. Revealed. Resolved.
www.world-check.com

Contents

New Payment Methods (NPMs) 2
What are the NPMs? 2
High risk and financial regulation 3
The criminal approach to money transfers 3
Significant risk to NPM providers 4
What are the risks? 4
What can NPM providers do to reduce the risks to their business? 5
Protecting your business 5

New Payment Methods (NPMs)

NPMs may no longer be new, but the term has become synonymous with financial payments transacted via mobile telephones, data storage cards, and internet connections. Naturally, variations of the methods change as technology develops. NFC or Near Field Communications technology is being embraced by the world's telecommunications giants and will fuel a massive increase in the mobile payments market – China alone estimates it will have 410 million users of NFC-enabled mobile payments as early as 2013.

Technology may be enabling this market but it is not necessarily driving it as there is an admirable global political movement for social and financial inclusion. In April 2011 the world's financial inclusion policymakers met in Kuala Lumpur, Malaysia, and discussed issues ranging from consumer protection and education to regulatory integrity. The issue of financial crime, money laundering, and terrorist financing was raised but was rightly recognised as only one aspect of these new, fast moving, and exciting financial developments.

This paper does not describe in detail how the methods work but looks at the risks involved to those businesses providing the NPM services. Interestingly, this includes businesses within the regulated financial sector (e.g. banks, money service businesses) and businesses outside of the sector (e.g. telecommunications companies).

The risks include possible abuse of services by criminals and terrorists, compliance action by regulators, prosecution by law enforcement, and reputational damage due to media exposure.

In 2006 the Financial Action Task Force (FATF) published its first typology on NPMs, acknowledging that very little was known about them and their potential misuse. A much more comprehensive and better informed FATF report was published in October 2010 and I recommend it to readers, with advance warning that it runs to 117 pages.

What are the NPMs?

Pre-Paid Cards
Typically a plastic card with magnetic strip or electronic chip pre-loaded with value that can be used to transfer value to businesses for goods/services. It can be used in country of issue or abroad, physically or via internet. Other descriptions used are stored value cards, e-money, e-purse etc.

Internet Payments
This is not online banking (i.e. mainstream account-based transactions using the internet) but rather transactions often facilitated by non-bank businesses without associated accounts. Other similar services include Digital Currency Exchangers or Providers.

Mobile Payments
As Internet Payments but via mobile telephones that can also store value, known as Mobile Money Services.

High risk and financial regulation

I have seen and heard much anguish from many in the world of anti-money laundering policy (both public and private sectors), regulation, and law enforcement about the loopholes of NPMs that allow uncontrolled, unregulated proliferation of money laundering and terrorist financing. The NPMs do not fit neatly into the existing FATF Recommendations nor do they fall neatly within the regulatory structures, nor easily within existing business structures, for example, the relationships between telecommunications companies, handset manufacturers, and banks.

New providers will either operate outside of the national regulatory regimes or will be included, thereby expanding the width, depth, and complexity of financial regulation.
I am interested in what the criminals think of NPMs, although they are probably not aware of that acronym. Let us look at the business models of crime to see where and when use of NPMs may offer an attractive service.

The criminal approach to money transfers

At all levels of crime, from street level to international organised networks, the common requirements for moving money are convenience, security, and obscurity if not anonymity. Speed and cost are less important or not important. Use of the latest technological offerings is not important.

In every country there are criminals committing acquisitive crime at street level – high volume and relatively low value crimes – and in the main the proceeds are generated in cash and spent in cash. Some examples: street level drug dealers selling to consumers, thieves selling stolen goods, smugglers selling cigarettes, extortionists selling protection to businesses.

In all cases the front line criminal is face to face with his customer and collects cash. Cash has many benefits but also presents some problems of security (the criminal is a potential target for robbery or police seizure), volume (a busy criminal can generate a hold-all, if not, suitcase full of cash per day), and a logistical problem of storing it or transferring it. Despite these inconveniences the system works. Yes, the police prosecute some criminals in possession of large unexplained amounts of cash; yes, some cash is discovered and seized crossing international borders; and yes, some Suspicious Activity Reports are submitted by regulated sector firms receiving large amounts of cash. To the criminals these are acceptable business risks.

On-the-street transfers by internet or mobile telephone from the customer to the front line criminal removes the problem of robbery, seizure , storage, and transport. Any anti-money laundering value restrictions imposed by the NPM provider are not likely to present too many barriers at this level of low value crime. So far it seems an ideal alternative. The major challenge for the street criminal is the volume of customers. NPM providers that set limits on frequency of transactions will significantly hamper the street criminal's business objectives. If a product allows sufficient value and unlimited frequency then the criminal's remaining problem is to promote significant business change amongst his diverse customers. NPMs may make the criminal's life easier but why should the 'customers' change? This change becomes easier in countries or regions where the NPM services are taking hold amongst the general population for legitimate purposes e.g. in the absence of accessible main stream banking facilities. Already a risk profile emerges of the type of criminal, the geographic location, and the most vulnerable product.

Significant risk to NPM providers

In my view the FATF NPM October 2010 report misses this point when it suggests, in paragraph 114, that restrictive value limits are one of the main reasons why so few money laundering cases have involved mobile payments. If one takes the view that money laundering consists of organised, sophisticated, multi-million currency operations then a few simple restrictions of usage do reduce, or even remove, the risk. But criminal money laundering happens prolifically every day at much lower value levels, and the risks to NPM providers of being seen to provide services to every day criminals are significant.

It should be obvious that terrorist financing often involves small value, infrequent transactions - commonly raised, collected, and moved in cash and/or transmitted via money service businesses. The requirements for convenience, security, and obscurity are well met by a variety of NPM services. The risks to NPM providers of being seen to provide services to any terrorist connection are significant.

Let's return to the criminal business models, this time looking at the national and international criminal. Their requirements for moving money remain the same: convenience, security, and obscurity. Any chosen method needs to accommodate high values – commonly this involves bulk cash smuggling and placement, use of all main-stream methods of transferring value, investment in and transfer of fixed and moveable assets. There is no shortage of methods that work and so there is little or no attraction for this level of criminal to launder their criminal proceeds or move their working capital via NPM services. This may be of some comfort to NPM providers.

This category of criminal has a particularly financial service requirement, that which enables him to lead a life with minimal audit trail – i.e. obscurity. Currently this is achieved by the use of cash – e.g. for accommodation rental, vehicle leasing, travel, cash withdrawals via ATMs without accounts etc.

Similarly, these are the sort of everyday lifestyle transactions required to support terrorist networks. In most jurisdictions terrorist financing is not restricted to the more obvious and infrequent purchase of explosive and other attack materials. The risks to NPM providers of being seen to provide everyday lifestyle services to serious, organised criminals and to terrorists are significant.

What are the risks?

There is regulatory, law enforcement, and public attention on these new payment methods – there will be those who wish to expose the dangers and make examples of those businesses who are :

- being seen to be the financial services provider of choice for street level criminals,
- being seen to be providing financial services to any terrorist connection,
- being seen to be the financial services provider of choice for everyday lifestyle services to serious, organised criminals and to terrorists.

These risks will manifest themselves through three external forces, all of which have a realistic potential to be high impact. I place them in order of highest likelihood:

1. **Media exposure** – affecting reputation, market reach and market share.
2. **Regulatory action** – financial penalties, management time costs, reputational damage
3. **Law enforcement prosecution** – criminal action against company and individuals, financial penalties, reputational damage

What can NPM providers do to reduce the risks to their business?

All businesses need to manage their risk effectively as no business can operate in an entirely risk-free environment. Although each will have different appetites for risk, all need to understand the risks and to make decisions about appropriate avoidance or mitigating action. It is important, particularly in new and innovative sectors, to demonstrate to all interested parties (including customers, shareholders, the public, regulators, and law enforcement) a commitment to good governance and public interest whether or not the business activities lie within any formal financial regulation and law.

The first step in protecting your business is to understand what threat you need to be protected from, then it's vital to implement a system that recognises the threat and minimises the chance of it occurring.

1. **The threats** –used by criminals and terrorists to support their illegal activities and/or support their everyday lifestyle. This threat becomes a risk to business when discovered and exposed, whether by an investigative journalist, a regulator, a whistle-blower, or a criminal investigation. This exposure can start many, many steps away from the NPM services but the provider can find itself embroiled as a facilitator.
   There is also a threat to those within the financial sector of the regulator penalising those with inadequate systems, regardless of the actual exposure to criminal or terrorist money. During 2010 and 2011 we have seen large multi-million fines on large banks and insurance companies based on inadequate screening and monitoring systems even when no financial crime has been identified.

2. **The systems** – the nature of the product and the customer demographic frequently means that not all NPM providers can readily obtain the same degree of customer identification and verification as mainstream financial institutions that offer fixed account services.

However NPM providers should do what they reasonably can – and there are many additional identifiers that can be taken on the grounds of security questions to gain access to the services such as places of birth, mother's maiden names, aliases etc. Technical identifiers such as IP addresses and geographic locators can also be collected and retained. All such information contributes to building a profile of the people with whom you are doing business.

Identifying details should be obtained for first line customers, any third party users of the facility (e.g. pre-paid card users); recipients of transfers; and agents.

There are many regulatory compliance challenges with agents, and sub-agents, but at the very least NPM providers should know who the people are within those agencies, and their beneficial owners, and screen those for any adverse links to criminal or terrorist organisations.

Protecting your business

Introducing a screening service from a business intelligence provider allows credible verification and on-going monitoring of high risk relationships with suspect clients and associated parties. Having such a system in place immediately reduces the risk of regulatory action for 'inadequate controls and systems'; and reduces the range of risks of supplying services to criminals and terrorists.

The implementation of business intelligence screening delivers an extra level of assurance that great care has been taken to ensure there are no links to organised crime or terrorism. That knowledge assures the Board of the NPM provider, its shareholders, its regulator, any investigating law enforcement agency, and the public that it could not have been expected to do any more to conduct appropriate due diligence.

About the author

David Thomas is an internationally recognised expert in developing aligned anti-money laundering strategies. His deep understanding of suspicious activity reporting (SAR), money laundering threats, terrorist financiers and wider financial crime has seen him called upon by numerous governments and their Financial Intelligence Units who trust in his expertise and counsel.

In 2005 David was appointed by Sir Stephen Lander (Chair Designate of SOCA and former Director-General of MI5) to be the financial crime expert in his team to review the UK Suspicious Activity Reporting (SAR) Regime. From 2006 until his retirement in 2010 David was the Head of the UK FIU within SOCA. In this role David was responsible for providing strategic leadership for the FIU, and also played a crucial role in liaising with national and international stakeholders. David was Project Leader and Chair for the Financial Action Task Force's (FATF's) project to design, research, and author the first Money Laundering and Terrorist Financing Global Threat Assessment published in July 2010.

From 2006 to 2007 David served on the Egmont Group Committee and subsequently to 2010 he participated in each annual Plenary, and the Operational and Training Working Groups – frequently presenting the UK experience.

WORLD-CHECK ™
A THOMSON REUTERS BUSINESS

Risk. Revealed. Resolved.
www.world-check.com