Finance and law: money laundering and new payment methods

Finance

Executive Summary

In recent times, new and innovative methods enabling funds transfer through electronic methods across the borders have increased. These have opened new opportunities formoneylaundering and the financing ofterrorism. As a result, this report explores the issues surrounding NPMs (New Payment Methods) and as such it has explored non-face-to-face typology as one of the most abused NPM typologies. Moreover, the vulnerabilities the NPM could expose in relation to the firm and its products such as fraud, reputational, legal and operational risks have been discussed in detail. Outstandingly, special considerations that NPM should include in their AML systems have been identified with the likes of data encryption, antispam, antiphishing and privacy policies along with limitation of the accessibility of personal data. Again, measures like setting out in the law the customer Due diligence measures, have been identified as effective tools directed towards the regulation and guidance relating to NPMs in order to better protect the firm and the customer, from the risks associated with the new payment methodologies.

Introduction

In the modern times, new and innovative methods of funds transfer through electronic methods across the borders have increased. These have opened up new opportunities for money laundering and the financing of terrorism. Following this point, the FATF (Financial Action Task Force) Typologies Report of 2006 on New Payment Methods (13th October 2006) recognized the emergence of the new payment methods as being far different from the

traditional methods of money transfer. With the emergence of the new and innovative methods of cross border money transfers, AML (Anti-Money laundering) vulnerabilities increased. Subsequently, FATF published their report “ Money Laundering Using New Payment Methods” (2010), which revealed the potential risks of money laundering and the financing of terrorism using the New Payments Methods. Furthermore, the report revealed the actual risks through an analysis of new case studies along with the particular typologies. In the light of this point, the purpose of this report is to remind the regulatory Authority department of the issues surrounding NPMs.

In connection to this point, an example of a NPM typology will be given explaining its mode of operation and its vulnerability to money laundering through a financial firm and its products. Accordingly, the report will identify and as such determine special considerations that NPM providers need to include in their AML systems in order to combat the abuse of NPMs through money launderings. Moreover, the report will reveal the measures which, if considered and implemented would improve guidance and regulation to NPMs translating to better protection of the firm and its customers.

NPM Typology 2: Non-face-to-face NPM accounts

Basically, typology two describes a model through which most NPMs rely on and as such it is a business model where minimal face to face interaction is utilized or it is absent. In the light of this point, Internet payment services (IPS) such as PayPal and moneybookers among others as such together with prepaid cards (MasterCard, Visa Electron, Maestro, etc) are utilized (Paulus,

Pohlmann & Reimer 2005). Under this typology, online banking, prepaid internet payment products and digital currencies are commonly used. Notably, the non-face-to-face nature of most NPMs can facilitate cases of money laundering through the abuse of the system by the criminals. On the other hand, typology one has to do with third party funding whereby cards can be funded through the bank, cash and person to person transfers. Additionally, there is the third typology (complicit NPM providers or their employees). There is also a high risk as portrayed in findings made in the past of IPS and prepaid card providers who were controlled by criminals and as such promoted cases of laundering

How Non-face-to-face NPM accounts can be utilized for money laundering and terrorist financing purposes

According to Financial Action Task Force (2006), several cases were brought out through which NPM products were used to launder illegitimate proceeds. This was accomplished by theft of identity together with money being stolen from bank accounts or credit and debit cards through the use of computer hacking. It was also accomplished through phishing, which describes a fraudulent e-mail designed to bring about the theft of information or identity. Owing to such abuses, the criminals managed to hack through the computers with such information and as a result, bank accounts, credit and debit cards were used as reference translating to funding of IPS or prepaid card accounts (FATF Report 2010).

In such a case, it is not easy to determine or rather detect a suspicious activity. Likewise, the non-face-to-face typology facilitated money laundering

through fake and stolen identities being used to create NPM accounts. In such cases, IPS or prepaid cards are used as transit accounts for the financing of terrorists' activities and money laundering.

Therefore, a firm wishing to offer NPM as one of its products, should critically consider the way NPMs makes AML systems vulnerable to money laundering activities. It is important to take note of the fact that most of the services offered in this typology are virtual in the sense that the customers dealt with are virtual and in such a case cross-border transfers are common. So to speak, identification, verification and monitoring systems should be implemented in such a manner that they can detect any form of money laundering. However, this may be limited by the fact that credit risk does not exist in this typology (FATF Report 2010). Therefore, the service providers may not be so concerned with the money laundering activity detection since this may not bring about credit risks to them.

Vulnerabilities the NPM could expose in relation to the firm and its products

A firm offering NPM products and services should be careful of misuse and abuse by criminals and terrorists since the typology deals with virtual customers. In actuality, a firm offering such a service or product should understand the risk of exploitation of the non-face to-face nature of NPM accounts whereby criminals may use fake identities, documents or stolen identities and documents (FATF Report 2010). The firms should understand the exposure of the firm and its products to money laundering activities carried out by hacking and phishing of account information and identities (Bidgoli 2006, p. 399). In reality, the firm venturing in such a business should

ensure that it has functional identification, verification and monitoring systems in order to avoid the risks associated with such dealings. Such risks involve the reputational implications if customer's accounts are hacked. In the same manner, the firm should be careful of operational risks which refer to the loss incurred as a result of failed or inadequate processes, systems, external events and people involved (Bidgoli 2006, p. 399).

In addition, there is also a legal risk if the identification, verification and monitoring systems are not implemented with tight surveillance to detect illicit activities by terrorists. In particular, a legal risk has to do with the potential for law suits once involved in a money laundering case. Again, it may result in sanctions, unenforceable contracts, penalties and fines which may translate to significant financial costs (Steiner & Marini 2008). Furthermore, the institution's licences may be revoked and this may lead to the closure of the institution and as such, may be expensive for the institution since the losses involved may be costly (Fagan & Munck 2009).

Special considerations that NPM providers need to include in their AML system

Following the increased use of NPMs, service providers should reform and as such restructure their AML systems from the traditional way of operation to a more modern one. In this sense, NPM providers need to involve verification, identification and monitoring systems to track records even in the real time. In line with this point, NPM providers should install anti-phishing mechanisms during login and as such, personalized images next to password prompts should be implemented (Moore 2010, p. 145). As a security measure, TLS

Encryption and authentication should be applied by NPM service providers. In the same line of thought, NPM providers should also employ antispam policies and as such, employees should be restricted from interfering or rather exposing personal information of the accounts of the customers (Moore 2010, p. 145).

In essence, controls to combat the abuse of the NPMs and counteract any potential risk to the firm should begin with customer due diligence (CDD). In line with this point, use of ATMs, prepaid cards, mobile and internet banking has presented a great opportunity for money launderers. However, there are some countermeasures that can prove viable. For instance, one countermeasure may be the implementation of robust identification and verification procedures (FATF Report 2010). In spite of the challenges associated with the use of NPMs, it is important to note that the electronic records produced in this case can help with law enforcement (Marks et al. 2012).

Essentially, NPM providers should include a robust identification system and as such, should not allow a double holding on accounts by one user. This is to suggest that they should ensure that there is no confusion of identities. This is given to the reason that some individuals may hold several accounts under the same identity. At the same time, NPM providers should place limits on the transaction amounts and frequency and as such should include strict systems of monitoring on these aspects. Along with this point, Simplified due diligence, digital currency, and suspicious transaction reporting in cross border cases, and law enforcement against foreign providers with

identification of secondary card holders should be applied (FATF Report 2010).

As earlier on mentioned, CDD should be carried on the customers even if they are not in face to face contact. This can be accomplished by ensuring that the names of the customers are known, the location, country of origin, web data sources verified and as such customer contacts taken into consideration (Demetis 2010, p. 64). One should also consider using financial transaction records of the particular customers from wherever the place in the world.

For instance, moneybookers (Skrill) in its verification of identity, will ask for the name of the customer, verification of the identity through a scanned national identity card, address and location and they also ask for a utility bill, bank statement, passport or driving license, with which it is meant to verify one’s identification (Janczewski 2008). Obtaining such information may not be easy but it can be made possible by employing various agencies and expertise from around the world. This is due to the fact that customer base is worldwide and as such, national cultural understanding would be of paramount importance.

Specific considerations NPM providers need to include in their AML system

Therefore, the following considerations should be included in AML systems for a firm wishing to work as a NPM provider:

The AML system should contain effective policies, procedures and processes while carrying out the identification and verification of the customers.

It should as well contain protective measures such as personalized images next to password prompts in the case of internet based payment methods along with data encryption, antispam and antiphishing policies.

Protective measures should as well be put in place within the web system and the computers themselves which contain personalized details and information in order to counter the hacking of computers.

The AML system should as well ensure compliance with the legislative laws where applicable since some of the NPMs do not have clear provisions as far as compliance with the law is concerned

Representatives from various parts of the world should be involved in the AML system in order to help in carrying out of CDD. This has the advantage of ensuring the right data sources are provided along with the verification of their authenticity (Rosenbloom 2002).

AML system should involve a group of experts in human resource, IT (informationtechnology) and experts with good knowledge of nationalculturejust to mention a few (Rosenbloom 2002). This has the advantage of ensuring that the NPM provider operates competitively.

The AML system should as well put flexible procedures in order to cope with the changing environmental factors since the legal framework for the operation of NPM providers is not well established.

Risks involved in NPM business

From a broader point of view, considerations that NPM providers need to include in their AML system range from law, human resources and various technologies among others as such. In thisrespect, it should be clear to NPM providers that engaging in NPM products calls for tight surveillance owing to

its vulnerability to money laundering and the financing of terrorist activities. Again in this context, NPM providers should be careful with regards to how they carry out their CDD along with the whole operation of their AML systems. This is given to the reason that there are various risks associated withfailureto carry out an effective Customer Due Diligence (Steiner & Marini 2008).

In particular, NPM providers, if caught in money laundering and/or financing of terrorist scandal, are faced with a considerable reputational risk. Following theglobalizationof businesses, global financial systems operate with clients from all over the world. In this context, it is important to note that if CDD measures are not appropriately applied, then, this gives an opportunity for various losses. As such, failure to conduct CDD can lead to a reputational risk which translates to adverse publicity as far as the practices of the business are concerned. Inaccurate application of CDD measures may in this case lead to a loss of public confidence and as a result, may jeopardise the integrity of the institution. Subsequently, borrowers, investors, depositors and other stakeholders may cease business with that institution should scandals arise (Booth et al. 2011).

Apart from this point, AML system failure may lead to law suits whereby the particular NPM provider may be sued for facilitating money laundering. This is due to the fact that the institution has the obligation to conduct CDD and thus should be able to prove to any third party proof that every effort has been made to ensure CDD is carried out (Steiner & Marini 2008). Similarly, if CDD were to fail, in such a case it would be advisable for the AML to close

the account of that particular customer and as such to decline establishing a business relationship whilst ensuring that a suspicious transaction report is made.

In view of that, any AML systems implemented should be in line with the law. At the same time, it should not leave gaps while carrying out Customer Due Diligence since this may result into operational risks (Booth et al. 2011). This has subsequent consequences of the suit by law and financial costs. A continued monitoring of the customers should be ensured and as such, this will help NPM providers to avoid cases of computer hacking, multiple accounts by the same Identity, fake identities, stolen identities and in the larger perspective this would prevent phishing of the customer accounts and information altogether.

NPMs and the Law

Notably, with an institution intending to make the use of NPMs, money laundering may be inevitable. NPMs are well known for their vulnerability to money laundering and terrorist financing. Use of ATMs, prepaid cards and mobile and internet banking has given a great opportunity for money launderers although there are some countermeasures that can prove viable. In this connection, one countermeasure may be the implementation of a robust identification and verification procedure (FATF Report 2010). Especially with the non-face-to-face typology, robust identification and verification would be of a supreme importance.

In line with this point, limits on the transaction amounts and frequency should be monitored with strict systems ofobservation. In fact, not all NPMs are subject to law in all authority and as such, they take in the use of internet and mobile payment. Most of the NPM providers provide their products or services through both internet and mobile (i. e. virtual world) systems and the FATF recommendations do not specify the specific risks involved and as such, NPM providers may not apply the CDD measures (FATF Report 2010). In spite of the challenges associated with the use of NPMs, it is important to note that the electronic records produced while carrying out transactions can help to carry out law enforcement.

Importantly, a firm seeking to provide NPM as one of their services should consider the fact that there are three typologies depending on which one chooses to use. As such, the first typology has to do with the third party funding whereby cards can be funded through the bank, cash and person to person transfers (FATF Report 2010, p. 36). Furthermore, there is the second typology which takes in the exploitation of the virtual nature (non- face-to-face) of the NPM accounts (FATF Report 2010, p. 40). This typology has the highest potential by its ability to facilitate criminals in money launderings. On the other hand, if the firm chooses the third typology (complicit NPM providers or their employees) there is also a high risk as portrayed in findings made in the past of IPS and prepaid card providers who were controlled by criminals and as such promoting cases of laundering (FATF Report 2010, p. 33).

In order to better protect the firm and the customer, from the risks associated with the new payment methodologies, new laws and regulations should be implemented in order to regulate the NPMs operations. Again in this context, measures such as the implementation of anti-phishing measures should be put in place. As such, it should be provided by the law that if they are not implemented, law suits should be applied. Besides this point, antispam policies (softwares, hardware and processes) directed towards combating proliferation of spam or keeping spam from entering the system should be implemented (Moore 2010). Equally important, measures to protect computers with personal details should be protected from hacking. Accordingly, for non-face-to-face NPM accounts, there should be provisions in the law to ensure that firms comply and as such put in place measures to prevent the cases of hacking, phishing just to mention a few.

In the same line of thought, if implemented, tight surveillance within the various websites present in the internet should be carried out and as such, it should be a provision of the law for every NPM provider to carry out such surveillance. This can be possible in a virtual world through representatives in various countries with expertise in both identification and verification of data sources (Rosenbloom 2002). Technologies such as firewall, encryption of data, limiting accessibility to customer data and the development and implementation of privacy policy are of paramount importance as measures for combating activities of money laundering and financing of terrorist activities (Rosenbloom 2002). With such measures in place, both the firm and the customer can be protected from the risks associated with the new payment methodologies.

Currently, where the regulation of NPM service providers is active, law enforcement agencies, supervisors, and legislators, among others as such, are faced by various challenges some of which include simplified due diligence, digital currency, and suspicious transaction reporting in cross border cases and law enforcement against foreign providers with the identification of secondary card holders among others as such. Therefore, the most important thing to do is to ensure that the requirement for implementation of AML systems for each NPM provider is set out in the law. At the same time, firms providing NPMs and the customers can be better protected if the regulatory authorities would set it out in the law that all NPM providers apply data encryption, anti-phishing, privacy and antispam policies and limitation of data accessibility.

Conclusion

The report has identified several considerations NPM providers need to include in their AML system in order to combat the abuse of the NPMs and counteract any potential risk to the firm. Non-face-to-face typology has been identified as one of the examples that is mostly utilized and as such the most vulnerable to abuse by money launderers and criminals. As such technologies such as data encryption, establishment of antispam, antiphishing and privacy policies have been identified as effective tools for combat. Limited data accessibility should be incorporated in order to ensure the protection of customer information and private details.

In order to improve on regulation and guidance relating to NPMs and to better protect the firm and the customer from the risks associated with the

new payment methodologies, measures directed to this effect should be set out in law. Again, identification and verification of data sources through representatives in various countries across the world in order to ensure the authenticity of various documents is an important tool and a consideration that NPM providers need to include in their AML system in order to combat the inherent money laundering vulnerabilities of the system.

References

Bidgoli, H 2006, Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management, John Wiley & Sons, New Jersey

Booth et al. 2011, Money Laundering Law and Regulation: A Practical Guide, Oxford University Press, New York.

Demetis, DS 2010, Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach, Edward Elgar Publishing, Massachusetts

Fagan, GH & Munck, R 2009, Globalization and Security: Social and cultural aspects. Introduction to volume 2, ABC-CLIO, California

FATF Report 2010, Money Laundering Using New Payment Methods, Retrieved on 20th April, 2012 from http://www. fatf-gafi. org/dataoecd/4/56/46705859. pdf.

Financial Action Task Force 2006, Report on new payment methods, Retrieved on 24th April, 2012 from http://www. fatfgafi.

org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods. pdf

Janczewski, L 2008, Cyber Warfare and Cyber Terrorism, Idea Group Inc (IGI), Hersbey, PA.

Marks et al. 2012, Middle Market M & a: Handbook for Investment Banking and Business Consulting, John Wiley & Sons, New Jersey

Moore, T 2010 Economics of Information Security and Privacy, Springer, New York.

Paulus, S, Pohlmann, N & Reimer, H 2005, ISSE 2005: Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2005 Conference, Springer, New York.

Rosenbloom, AH 2002, Due Diligence for Global Deal Making: The Definitive Guide to Cross-Border Mergers and Acquisitions, Joint Ventures, Financings, and Strategic Alliances, John Wiley & Sons, New Jersey.

Steiner, H & Marini, SL 2008, Independent Review for Banks – The Complete BSA/AML Audit Workbook, Lulu. com, North Carolina. Tabb, WK 2004 Economic Governance in the Age of Globalization, Columbia University Press, New York.