NEW PAYMENT PRODUCTS & SERVICES AND ASSOCIATED CHALLENGES FOR RISK & COMPLIANCE

Bhanu Wijayaratne
Chief Compliance Officer
Hatton National Bank Plc

Introduction

In a fast growing economy banks cannot achieve their growth objectives and increase the value of shareholders, if they are not prepared to innovate. The advancement of Information & Communication Technology (ICT) throughout the globe has left Sri Lanka no alternative. The banking sector has been in the forefront among other sectors and industries, as a beneficiary of ICT advancements, which enable them to have greater reach towards their customers in a speedy manner, and of course at a relatively lesser running cost as well.

Similar to the benefits derived by the bankers, with the advancements of ICT, the banking customer too has equally benefited and is now equipped with internet facilities which could be accessed from anywhere in the world. The introduction and high usage of smart phones, Media pads, Tablets etc have turned traditional banking customers more tech savvy. As a result he is not only demanding innovative banking products but is also well equipped to research for various other banking products offered by competitor banks before visiting you, to patronise your services.

Even in the event that Bank is fortunate enough to capture a customer to its customer base, the challenge does not end there, as it becomes a herculean task to retain him. He is sure to demand from the bank, innovative products such as internet banking, telephone banking, mobile banking, E-Saver Accounts, E- Deposits Accounts, E-Cash Management Services etc. enabling him to operate from anywhere, without presenting himself in person at the banking outlet.

In addition to above products, another range of innovative products such as Prepaid Cards, Travel Cards, Mobile Payments and Internet Based Payment Systems are in high demand by the modern customer who seeks banking services whilst travelling, at work station, on holiday or may be simply whilst in the bedroom.

Associated risks & compliance concerns involving innovative products & services

The rapid development, sophisticated functionality and the increasing trends and usage of innovative financial products no doubt create challenges for banks and financial institutions in ensuring that such products and services are not misused for criminal activities, especially for Money Laundering (ML) and Financing of Terrorism (FT).

Further, such innovations and E products and delivery channels could trigger violations of Exchange Control regulations which in turn could raise risk and compliance concerns, as Exchange Control violations are predicate offences as per provisions of Prevention of Money Laundering Act No: 5 of 2006.

Risk factors associated with New Payment Products and Services (NPPS)

Among several risk factors associated with NPPS, given below are certain key issues which merits attention.

1) Non face to face relationships and anonymity.

NPPS can be used to speedily transfer / move funds across the globe and make access to cash through ATM network. The absence of a face to face contact could trigger higher ML / FT risks.

2) The absence of customer due diligence (CDD)

The absence of CDD increases the difficulty for the service provider to effectively put in place monitoring and reporting mechanisms.

3) Different ways of funding prepaid cards

The funding of prepaid cards can be done in various ways with different degrees of CDD including through Banks, Internet, at Retail Shops or at ATMs etc. This too will increase the ML / FT risks involved with NPPS.

4) Mobile Payment Services established through agents

Mobile Payment Services may establish customer relationships through agents, with limited KYC. In the given scenario, the risk of ML / FT further increases, when mobile payment service itself is used to reload the card.

5) Usage of NPPS globally

Certain prepaid cards allow users to effect payment domestically as well as internationally through global payment gateways. Such cards can be used to purchase goods and services or access cash internationally. In addition, certain prepaid cards allow cardholders to transfer funds from person to person. This feature makes the prepaid cards more attractive for ML / FT purposes.

6) Complex functionality of NPPS

The extent to which the NPPS can be used globally for making payments or transferring funds is an important factor to determine the level of risk. More the geographical reach permitted, the higher the ML / FT risks created.

7) Methods of funding NPPS

The methods of funding NPPS could impact the level of ML / FT risks posed.

a) Anonymous funding methods obscure the origin of funds
b) Allowing cash funding and at times reload-ability without limits would increase ML / FT risks.
c) Internet based payment services that allow third party funding from anonymous sources too increase ML / FT risks.

Risk factors associated with money remittance and currency exchange business

Among several risk factors associated with money remittance and currency exchange business, given below are certain key areas which merits attention.

1) Simplified processes involved in money remittances business

Several features in money remittance business have made same an attractive methodology through which illegal monies are pumped into the financial system. Among such features the simplicity and trustworthiness of the process (for the user) have been the key attractions for the criminals and money launderers to rely on the remittance business in pursuing their unlawful activities. Also the less stringent customer identification rules that apply to remittance businesses when compared to the rules applicable to opening of accounts, had made the remittance business a favourite product among criminals.

2) Placement (Currency Exchange) – stage

Currency exchange is an important link in the money laundering chain, particularly during the "placement stage". When the placed monies are exchanged and converted into a different currency, it is an extremely difficult task to get to its true origin.

3) Smurfing

In economies where there are many money remittances and currency exchange services exists, it is a difficult task to track "smurfing". Smurfing has been frequently reported as a more popular money laundering method identified with regard to money remittance and currency exchange Business.

4) Money mules

Another danger commonly associated with remittance business is the use of "straw men" also known as "money mules". A money mule is a natural person whose account has been misused by criminals, may be with or without his knowledge or could be for some form of a remuneration in return. A "money mule" is often contacted via a telephone call or through other form of communications to accept and transfer money received from a victim or from a criminal organisation which he is instructed to transfer to an account of another designated person which is known as "layering" in AML terminology.

5) Third party transfers

Another commonly reported method is the involvement of a third party to transfer funds. Transfers performed by the customers through multiple branches by using third parties on behalf of a criminal are often aimed at concealing the true beneficiary of the transaction.

6) Drug trafficking & human trafficking

Another reported activity in money remittance business is the involvement in human trafficking and drug trafficking. Its reported that in certain trafficking cases money remittance providers have been used to pay living expenses of parties concerned and also for purposes such as payments for air tickets etc.

7) Use of forged identification documents

The use of forged identification documents is another method commonly identified for misuse of money remittance business for ML / FT purposes.

The number of investigations carried out has revealed that money remittances services are frequently used as a vehicle for money laundering. The laundered proceeds in most of such

cases have been identified as coming primarily from drug trafficking, human trafficking, frauds (say from card skimming and committing phissing attacks etc), economic crimes (through forgery of documents, tax evasions etc) and smuggling (arms, liquor, tobacco etc).

How to mitigate risks that may arise from NPPS

The overall degree of risk of a particular NPPS is the cumulative effect of each of the risk factors described above.

However, it is important to note that the procedure to mitigate risks should be proportionate to the level of risk posed by a NPPS. One has to be mindful of the fact that overdoing risk mitigation or overrating the risk could compromise and negate the functionality of the product (NPPS), which is aimed at customer convenience and ease of use. On the other hand ignoring or under-estimating the risks can lead to a disastrous situation as the increased risk of ML / FT can be detrimental to the bank or the service provider.

Given below are certain risk mitigating measures that can be put into practice.

1) Effective customer due diligence (CDD)

Effective customer due diligence (CDD) is a proactive measure that could be taken to mitigate ML / FT risks associated with NPPS.

Such CDD to be carried out by banks should be proportionate to the risks posed by NPPS. If the risk posed is lower, simplified CDD would be sufficient. However, simplified CDD does not mean that a complete waiver or an exemption is possible. Greater the functionality of the NPPS, the higher the need for enhanced CDD.

Prepaid cards and specially, mobile payment services are commonly operated through wide range of agents, merchants or distributors. As a result, service providers and banks may not have a face to face contact with the customer or the card wallet holder. In such situations, CDD obligations are carried out by agents or distributors on behalf of the principal. This necessitates the service provider or the bank to monitor the effectiveness of KYC / CDD done by the agent or the distributor.

2) Limits on loading, determining value and geographical location of usage of NPPS

Having limits on value of NPPS, its loading capacity and the usage in different jurisdictions (geographical locations) can be treated as an effective mechanism to mitigate ML / FT risks, provided the operation of NPPS are in conformity with other AML / CFT measures such as

- Account opening,
- Transaction monitoring and
- Filing of suspicious transaction reports etc.

As regards mobile payment services, limits could be placed on-

- maximum amount that could be held in an account or a wallet,
- maximum value of transactions allowed done per day
- maximum amount permitted on a single transaction etc, which actions would keep a close tab on its operations and reduce the vulnerability for ML / FT risks.

Also limitations or prohibitions could be placed on NPPS, based on the geographical locations in which same are to be used. This control will facilitate curbing of unlawful fund transfers beyond jurisdictions.

3) Source of funds

Establishment of source of funding is a critical area which merits the attention of service providers and banks, as anonymous source of funding such as cash deposits would certainly increase the ML / FT risk involving NPPS. If cash is paid by a person, to add value to NPPS, the service provider should consider requiring such person to be identified specially if the sum involved is exceeding predetermined thresholds or if they (service providers, specially banks) are of the opinion that the sum involved is beyond the known / declared level of transactions or beyond, when compared with a peer group customer or a card holder.

4) Record keeping, transaction monitoring and reporting

Transaction monitoring and record keeping are key to AML / CFT initiatives which are complementary and supportive, towards law enforcement investigations.

Accordingly, details such as

- Information required to identify the parties to the transaction,
- Details of accounts or wallets involved,
- Nature and the date of the transaction
- Amount of the transaction should be captured.

As the size or volume of the transaction is immaterial to determine the need to have records, details of all transactions must be captured and retained, irrespective of the value of such transactions.

Additional measures to be considered at national and international level

In addition to the risk mitigating measures detailed above which are pitched more at an operational level, following additional measures could be considered at national and international level.

1) Lack of knowledge of sector, services offered and transaction channels

Researches have revealed that authorities in many countries are lacking in clear insight into the subject area. The sector being very heterogeneous, the service providers are keen in developing and introducing innovative products and delivery channels, which necessitate the regulators / authorities to engage in continuous dialogue with such service providers, of course with banks as well. This involvement by the competent authorities and regulators are extremely important as they need to ensure that sufficient measures are taken by "Business" with regard to control of their agents, of audit plans, how often agents are to be visited, the turnover levels of operators etc.

2) Guidance and training

Lack of capacity, knowledge, experience and resources to implement AML / CFT regulatory requirements are common among service providers. It is therefore the responsibility of regulators and supervisors to play a key role in providing appropriate guidance and training to banks and service providers. This area merits the special attention of regulators and supervisors.

3) Implementation of CDD measures

Weakness in implementing necessary controls and safeguards relating to customer due diligence processes are commonly observed, specially in countries with relatively weak AML / CFT regimes. Due to the absence of healthy relationships with customers and not having sufficient knowledge of the nature of transactions banks and money remittance agencies find it challenging to perform on-going monitoring of activities, with a view to detect suspicious transactions and anomalies in processes.

4) Licensing & Registration

Lack of procedure and implementation in licensing and registration of service providers, agents, distributors etc merits a special attention of the competent authorities. This is due to most countries not having clearly designated regulatory authority to cover this area of work.

5) Supervision

The level of vulnerability of banks and service providers towards ML / FT risks were found rather high in countries where there are weak supervision by regulators.

6) Fit &Proper

It has been found that in certain instances money remittance and currency exchange operator or agencies are owned by criminals and those who do not possess clean track records. Therefore it is necessary to carry out adequate "Fit and Proper" tests before registering

/ licensing in such service providers. The best way to meet this challenge is to impose regular registration renewal obligations.

7) Agents

Monitoring of agents and sub agents of money remittance and currency exchange service providers appears having deficiencies in certain instances / jurisdictions. Such weaknesses provide for a potential loophole whereby the "Fit & Proper" requirement of agents is not given due attention. It is important that regulators do not under-estimate even the role of smaller players.

8) Reporting System

The importance of putting in place effective reporting requirements, enriched with threshold based reporting, should not be compromised if the regulators are to ensure effective AML / CFT controls.

9) Law enforcement action

The level of law enforcement appears to differ greatly from one jurisdiction to another. The researches reveal that the law enforcement under certain jurisdictions is unable to gather sufficient information enabling them to act to enforce law against criminals. Further analysis confirm that such inabilities are due to incomplete or insufficient information and in some cases falsified documents.

Conclusion

The traditional financial services such as banking services are increasingly offered through new and innovative products by banks throughout the globe. Innovation has therefore become an integral part of banking, if the banks are to win. However, greater the functionality and the complexity of new products that are innovated and offered to customers, the higher the risks faced by banks and financial institutions. In other words the dynamic and evolving nature of such new products and innovations present enormous challenges to banks, especially from a risk and compliance stand point, which need to be duly identified, captured, evaluated, monitored by banks, in order to manage and mitigate such risks. It is therefore the prime responsibility of both the banks and regulators to ensure that adequate risk mitigating processes and mechanisms are put in place, if the banks are to be real winners of innovation, as the failure to do so would certainly be detrimental not only to banks but also to the financial industry, as a whole.

References

- FATF Report on Money Remittances & Currency Exchange Providers
- FATF Recommendations
- Protecting Mobile Money against Financial Crimes – Global policy changes & solutions published by the World Bank
- Risk Management in Electronic Banking – Concepts & Best Practices by Jayaram Kondabagil