9

E-banking in Barbados: Regulation and Monetary Policy

Anton Belgrave, Yvonne Parris and Warrick Ward

Introduction

The Internet has dramatically changed the cost and capabilities of the marketing and distribution of new types of products and services. This is especially true for retail financial services, where the widespread adoption of electronic interfaces, primarily the Internet, and the standardisation of the World Wide Web, have made it possible to reach customers in ways that even five years ago were too costly.

To this end, this paper explores the nature of e-banking and its likely impact on the financial system, especially its effect on the regulatory function in Barbados. The paper is organised into five parts. Section one provides a general overview of e-banking and focuses on its benefits and repercussions; Section two explores the current state of e-banking in Barbados, including a look at its adoption rate by domestic banks. In Section three there is a review of the regulatory effects of e-banking and the potential impact of e-banking on monetary policy in a networked environment is discussed in Section four. Section five concludes.

1. E-banking - *Trends, Benefits and Repercussions*

Improvements in information collection, transmission and distribution technologies have greatly enhanced and influenced all aspects of banking in most countries. Between 1995 - when the demand for e-banking exploded - and 1999, the global market is estimated to have risen by 171.25 million users (Smith, 1999). E-banking is the use of electronic processes and

products in the provision of banking services, such as the automated teller machine (ATM) and telephone wires. This paper, however, emphasises banking through the use of the Internet.

According to the Electronic Banking Group of the Basle Committee (2000), there were approximately 130 banks and thrifts in the United States (US) with web sites at the end of 1995. By March 2000, the number burgeoned to approximately 4,000, with 12 per cent having transactional sites. Large banks for the most part led the e-banking drive, reporting an 85 per cent penetration[1], with only 5 per cent penetration among small banks. Among those with web sites, 12 were considered virtual banks, which operate primarily through an Internet portal in the absence of branch structures. Interestingly, a Jupiter forecast survey predicted that by the end of 1999 there were approximately 7 million US households utilising on-line banking facilities, but these were projected to increase to between 20-30 million households by 2003. Further support for the growth capabilities of e-banking stemmed from a Datamonitor projection in 2000 that annual spending on e-banking implementation would have quadrupled from its 1999 figure to US$1.4 billion by 2004.

In Barbados, this level of sophistication is not evident, since most financial institutions do not even maintain an active web site. At the end of 2001, of the seven commercial banks, only two had functional web sites that provided informational services. However, there are signs that this new technology is beginning to permeate the banking sector. It is expected that with further promotion and initiative undertaken by both the public and the private sectors, such as the Education Enhancement Project (EDUTECH)[2] in the public sector, the benefits of greater technological absorption in commerce will be realised.

---

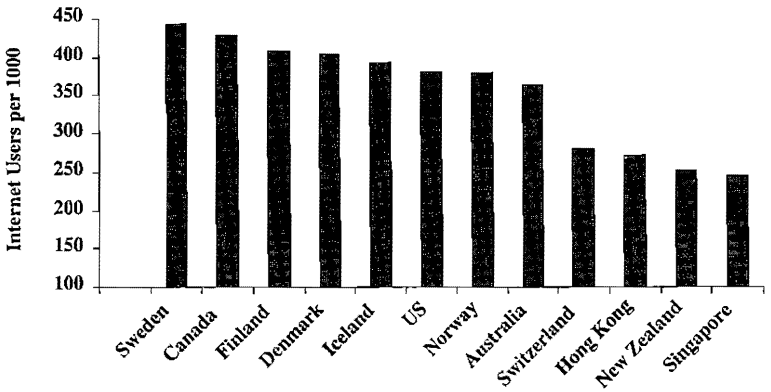
[1] Penetration, in this context, is defined as the introduction of e-commerce activity in its operations.

[2] The EDUTECH programme is designed to provide for the widespread introduction of computers in schools to prepare students for life in a technologically-advanced society.

Despite the presence of the infrastructure necessary to benefit from the possibilities that the Internet can provide, most commercial entities have not fully embraced technology-assisted commerce. Clearly the critical mass necessary to render such ventures viable has not yet been reached in Barbados (see Figure 9.1). Customers tend to be mostly concerned about security, an element that is necessary in all e-banking functions. Sufficient marketing and education may drive the adoption of e-banking, but it is the experiences that would lead to its continued use. Essentially, there should not be wide gaps between expectations and service, especially in areas of access to information, reporting services and other real-time account information.

Figure 9.1

A Cross-Country Comparison of Internet Users



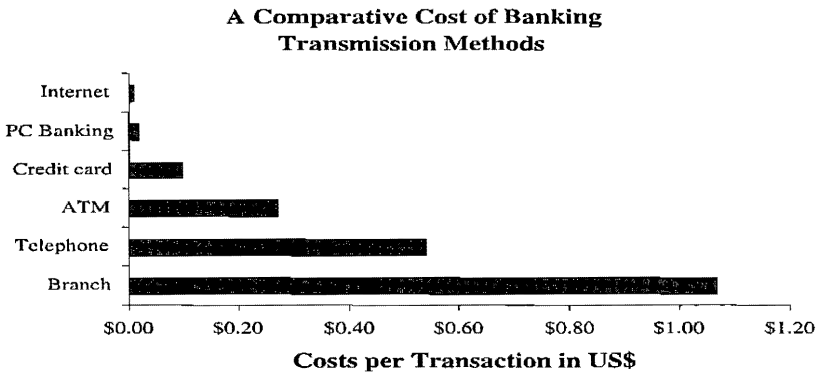
Source: Newsweek Special Report, April 1999

Potential Benefits

There are a number of benefits of e-banking, but the most prominent is its ability - through process efficiencies - to reduce operating costs. The Office of the Comptroller of the Currency (OCC) noted that the average costs per transaction in the US banking industry declined from an average of $1.07 for a branch to $0.01 with the use of the Internet (see Figure 9.2). This

shows the efficiency[3] gains in banking and payment systems and the potential economies of scale and scope in retail operations directly resulting from the use of an Internet portal[4]. These, in addition to providing enhanced levels of convenience to the customer, are expected to expand current markets beyond traditional credit and deposit-taking activities through the offer of new products and services. Any increased capacity is likely to strengthen the competitiveness of those banks with enhanced operating systems.

Figure 9.2



Source: Office of the Comptroller of the Currency (OCC) using data from Booz, Allen and Hamiltion Inc, First Manhattan (1999).

Despite the obvious benefits expected from implementing new technologies, there remains a body of evidence that does not currently support the hypothesis of "pure-play" or virtual Internet banks replacing "bricks-and-mortar" banks. Indeed, most banks that operate on the Internet use a "click-and-mortar" business strategy, where they have

[3] These efficiencies, if transferred, can potentially result in productivity gains and increases in general economic welfare.

[4] This has further implications for legislation and detection of fraud and money laundering activities, which will be discussed in subsequent sections.

maintained traditional networks of "bricks-and-mortar" branches, but have incorporated their transactional web sites within their operating systems. Comparing a sample of "pure-play" Internet banks with a traditional bank DeYoung (2001) found that Internet banks were considerably less profitable than the traditional banks. While DeYoung admits that the results are derived from a relatively small sample of "young" institutions, they are, nevertheless, intriguing since they imply that the "pure-play" Internet banks may not always be a financially viable business model, as had been projected.

DeYoung further points out that the distributive channels are not perfect substitutes. The processes involving checking on account balances, transferring funds, paying bills and applying for credit cards do not require personal contact or a large physical space, and, hence, are well suited for delivery on the Internet. However, in information-deficient societies, the setting up of new accounts, applying for a business loan, retirement planning, closing a mortgage and other complex transactions often require a secure physical space. To provide further credence to this position, within the last three years a number of virtual banks have folded as the technology sector weakened. Therefore, the repercussions, pitfalls and obstacles of operating a virtual bank must be carefully examined, so as to determine their viability. Furthermore, it is unclear whether cost savings will be the primary benefit derived from the adoption of e-banking systems, as any cost reductions achieved may not be a source of sustained competitive advantage for individual commercial banks. Cost savings using e-banking techniques are generally easily replicated by competitors. Secondly, cost savings are also accompanied by reduced entry barriers or increased market transparency leading to a further intensification of competition.

Drawbacks of an e-banking system

Clearly, there are a number of repercussions that may counter the possible benefits of e-banking systems. Globally, financial systems are becoming increasingly dependent on computerised inter-linkages, thus heightening the likelihood of

external contagion effects. This is of great concern to regulatory authorities charged with maintaining the stability of the financial system, as the failure of any bank – including e-banks - could undermine the confidence and integrity of the entire system. Notably, Internet banking presents all of the traditional banking risks, as well as a greater degree of strategic, reputation, transaction and compliance risks. In recognising the importance of these risks, a number of regulatory entities have issued specific guidelines relating to Internet security, certificate authority systems, privacy and technology risk management. These are considered areas that pose the greatest level of vulnerability and, therefore, must be properly addressed before e-banking can flourish.

With the drive towards more convenient forms of banking, it is expected that there will be a wider range of Internet-related activities, in some cases even cross-border banking. Regulatory agencies, especially in small, open economies with fixed exchange rates, must not allow unmonitored flows resulting from cross-border transactions. Some may even be forced to confine virtual banks to purely local operations, even though the virtual bank may possess the capability to extend banking services abroad. Unregulated activity could severely impact on the foreign exchange position, particularly where exchange control regimes are not officially in place[5]. In the case of Barbados, the careful monitoring of capital flows is critical, as most cross-border e-banking transactions will require settlement in foreign currencies. However, an institution that generates cash flows externally may only remit some of these flows to Barbados, seeking to circumvent established exchange control rules.

Despite the wide array of potential benefits resulting from electronic delivery, the supervisory agency – the Central Bank in the case of Barbados - must place the greatest emphasis on depositor protection and/or the stability of the financial sector. The regulatory authorities must also ensure that services

[5] Such structures are continually under threat with the commitment towards liberalised capital flows under Protocol II of the Agreement for the Caricom Single Market and Economy.

transacted through electronic means are consistent with the required standards of traditional banking methods. Notably, one possible challenge to regulators is the cost of monitoring these "new" banks. For effective monitoring, regulators need to exhibit some degree of flexibility and be prepared to adapt their thinking and methodologies to meet the challenges posed by the changing environment in which they function.

2. The Electronic Banking Experience in Barbados

The adoption rate of electronic banking in Barbados has been slow. As Table 9.1 reveals, activity in this sub-sector centred mainly around the provision of the most basic forms of e-banking - a network of automatic teller machines (ATMs), telephone banking, debit cards, and electronic funds transfers (EFT). Though much of the use of ATMs occurred as a cost-saving measure[6], many have realised savings of time and convenience. Consequently, ATM banking has become the most popular form of electronic banking in Barbados, with even some non-bank entities hosting similar services. However, the graduation to the next level of e-banking – Internet banking - has been sluggish, with very few banks even operating an informational or promotional web site (see Table 9.1).

The explanations for the lacklustre interest in the more complex forms of e-banking cannot be based solely on the behaviour of the commercial banks. Some of it is cultural and can be explained by customer preferences. There seemingly exists a divide between those who prefer traditional banking and those who prefer using the electronic methods of account access. Survey results conducted by observations in the various commercial banks in Barbados over a period of time support the hypothesis that the use of e-banking products is driven by job type and age (see Parris, 2001).

---

[6] During the late 1990s, most banks implemented charges for over-the-counter teller services, above a specified minimum number of transactions. This was conveyed to the public as an effort to entice customers to increase their use of the ATM, which is cheaper per transaction and is largely underutilised.

Table 9.1

E-banking Activities Offered by Commercial Banks

	Bank A	Bank B	Bank C	Bank D	Bank E	Bank F	Bank G
E-banking Activity	*	-	-	-	-	-	-
Web Site – Informational	*	-	*	-	-	-	-
PC Banking	-	-	-	-	-	-	-
Automated Loan Machines	-	-	-	-	-	-	-
ATMs	*	*	*	*	*	*	*
Debit Cards	*	*	*	*	*	*	*
EFT	*	*	*	*	*	*	*
Web Site-Transactional	-	-	-	-	-	-	-
Telephone banking-account balances	*	-	*	*	-	-	-

Source: Parris, 2001

Note: * denotes that the activity is offered

More specifically, the survey highlighted that non-clerical workers prefer traditional teller or over-the-counter transactions to ATM machines by an 80 to 20 ratio. Eighty per cent of students, professional and clerical staff, use ATM transactions instead of teller services. The results also reinforced the assumption that the adoption of e-banking and related electronic products is likely to be a function of age. Additionally, consumers' preference for the ATM network has implications for the efficient utilisation of the banks' plant. Parris (2001) observed (Table 9.2) that during peak periods customer

transactions through the ATM system were in the worst case 3.6 times greater than the traditional teller system, and in the best case they were 12 times as fast. Still, these services relate to the most basic form of electronic banking and the offer of the next level of e-banking - Internet/PC banking - requires a certain number of prerequisites for efficiency and safety.

Table 9.2

Observation of Traditional and ATM banking: A Busy Day (No. of Customers per 30 Minute Intervals)

Bank	ATM	Traditional (Teller)
A	45	8
B	36	10
C	90	8
D	90	15

Source: Parris (2001)

Whatever services are offered, in addition to providing a secure platform, banks will need to make software applications and solutions that are seamlessly integrated into existing systems and provided without additional burden to the customer. Importantly, retail customers are not motivated to transact on-line on cost alone; it is a combination of cost, quality of service and security that encourages e-banking.

3. Regulatory Issues of E-banking

Although the basic types of risks involved are not new, e-banks provide new forms and speeds of "delivery", and consequently, a number of interrelated policy and regulatory issues, such as consumer protection, competition, access and standards need to be highlighted (Basle, 1998). Since the adoption of premature, conflicting or inappropriate regulation can stifle the

use of technology in financial transactions, and consequently forego any efficiency gains, the timing and form of necessary regulatory adjustments are essential.

Further challenges to the supervisory authorities in Barbados lie in determining the net impact on the financial system of the increased use of e-banking, and then devising necessary policies that address any potential weaknesses. Of greater importance is the expanded provision of services to foreign entities under e-banking, thus requiring more cross-border co-ordination among regulatory agencies. Such transactions can also potentially expose local depositors to a wider range of credit risks. Furthermore, policy responses to regulatory, legal, and monetary issues may vary across jurisdictions, thus necessitating further co-ordination of regulatory efforts.

Still, there are many aspects of risk that are neither fully discernible nor measurable (Basle, 1998). Hence, there is a need for a framework that allows a banking entity to operate with sufficient levels of safety and soundness, which require proper certification and authorisation processes. Policy-makers and regulators need to ensure that requirements, including the licensing and registration of, not only banks, but also certification authorities (CAs), are met. Most e-commerce transactions are largely dependent on these third parties, who confirm the authenticity of the digital message or signature[7].

Since the legitimacy of the digital signature infrastructure largely depends on the procedures set out by the CA, rigorous investigations of these are warranted before any widescale adoption in Barbados. To allow for such, there may be a need for further modification of the Financial Institutions Act, and the establishment of licensing procedures and standards for CAs. Clearly, there remains some preparatory work to be done, but in the final analysis, banks must be encouraged to follow a rigorous risk management process, one with the capacity to deal with the known material risks, including those posed by outsourced

[7] Electronic signatures relate to the use of electronic or similar means with the intention of authenticating a written document. A digital signature, a narrower term, is a string of alpha-numeric characters which can serve the same function as a hand-written signature.

products. In this regard, banks should be able to properly monitor and control third-party risk, while supervisors must have the capability to examine the parties and related products to which business is outsourced.

With the integration of e-banking into the domestic financial system, the traditional financial legal framework will no longer be suited and it will be necessary to formulate and revise financial laws and administrative procedures. However, in most instances the current regulatory framework based on "bricks-and-mortar" entities could be amended to account for the risks posed by "new" products and processes, leading to modifications to supervisory, policy and legal norms. In Barbados, a necessary legal prerequisite for e-commerce activity stemmed from the allowance of digital signatures. For widescale e-commerce activity to be conducted in Barbados, e-banking included, legal updates were needed to allow digital signatures to be legally binding[8]. Likewise, guidelines to regulate CAs also need to be implemented. These entities ensure the uniqueness of individual signatures and data and operate under a framework where data are linked to a signature, which if altered, invalidates the transaction.

Supervisory agencies, in order to be guided by updated regulatory procedures or concepts, must be equipped, particularly in the area of risk assessment procedures related to information technology (IT). So far the level of e-banking could be sufficiently safeguarded by log-ins and passwords, but this is insufficient to properly secure an Internet-based system. The Central Bank of Barbados is adopting active measures and promoting guidelines to support the development of e-banking in Barbados. These specific guidelines must focus on the importance of internal controls to the proper management of technology-related risks. The development of these measures involves a collaborative process with commercial banks, all in an aim to encourage innovation and to avoid producing restrictive policies.

[8] This was addressed by the Electronic Transactions Act (2001). Some documents, such as deeds, wills and affidavits still require hand-written signatures because their signing involves the presence of witnesses and the taking of oaths.

Regulators are the "'gatekeepers" of the financial system and possess the ability to determine the severity of the risks posed by e-banking. They hold power over jurisdiction, which is enforced through a variety of licensing options. Even though e-banks - as some might suggest - are not bound by jurisdictional laws, in practice they must be treated in a similar fashion to other deposit-taking or financial entities. Importantly, resources must be placed on public awareness and education, and unbiased views of e-banking and their operations should be solicited. Overall, the major concerns to the regulator encompass infrastructural security, protection against infiltration by criminal elements, transparency of legal and regulatory arrangements and effects on monetary policy.

Infrastructural Security

System security requires special attention because of the increased risks from the amplification of the effects of security intrusions and the potential impact posed by lax technical standards. Losses resulting from a breach of security are likely to be borne by the owners, lender of last resort, or in the extreme case, the depositors.

As a counterfoil, effective security mechanisms are necessary in order to detect and control fraud, vandalism and sabotage in a timely manner, while ensuring the integrity of the system. There must be effective security on all levels, the client, server and the operating system[9], as well as its data movement[10] for an e-banking system to operate optimally. The major security requirements are a trusted means of authentication over open networks, confidentiality of transactions, means to ensure integrity of data in transit and ways to allow non-repudiation of payment or receipt.

[9] This provides the platform for the software that runs the computer. Therefore, if it is vulnerable, all other security measures can be considered useless.

[10] The Internet, being a public portal, is inherently an insecure medium for the sending of messages or data. It lacks a fixed path for the transmission of data and, without adequate security, data could be intercepted and altered before they reach their intended recipient. This is sometimes termed as "web spoofing".

Adequate controls, as Rowe (1998) highlighted, must be in place in order to deal with the major banking risks. Although, it is still possible for security breaches to occur external to the bank's operating framework, the risks posed by the flows in the bank's system and storage facilities are greater, and therefore require more attention. However, this does not always occur, and there have been a number of high-profile breaches. One such was reported in the *Economist* magazine in 1999, where it was revealed that Egg's system, the on-line bank operated by Britain's biggest life insurer, Prudential, allowed a breach in the account-holders' personal information. A similar occurrence had also affected Halifax's on-line shareholding service and the reaction by clients was immediate, leading to closed accounts and volatility in share prices on the financial markets. This clearly highlights the need for banking systems to possess the capacity to immediately detect security breaches and operational "glitches" as soon as they occur. These attacks and "glitches" are not only confined to the initial loss, but can also extend far beyond this.

In summary, the impact of a breach in a bank's technical security is not confined to a specific bank, but also to other banks and to the supervisory authority, as a result of its effects on the financial system. A breach can spill over, leading to a loss of public confidence in the entire financial system, and if pervasive enough, can spread to the real economy. It cannot be stressed enough that reputable forms of authentication must be applied. It must, however, be emphasised that no single set of security measures is sufficient for e-banking, and banks should ensure the use of best practices. As highlighted by the European Central Bank (1999), "it is the combination of measures together with the rigour with which they are implemented that will serve to reduce risk most effectively."

Criminal transactions

A further concern stems from the risk of contamination by criminal elements, such as money launderers. Money laundering relies on anonymity of, and the inability to trace, large and complex transactions. Both of these factors are likely

to be greater in e-banks. With this in mind, it is clear that measures aimed at detecting and eliminating these factors must be developed. This is a major point, since an institution whose main activity is based entirely on market forces to attract customers may be more likely to run the risk of integrating funds into systems derived from illegal operations.

A safeguard which is gaining increasing prominence in e-commerce transactions is the use of encryption technology. This, and other security processes, which involve the use of firewalls, digital signatures, and a hierarchy of certificates, are used to validate users. At the moment, the most secure method of transmission is public key infrastructure (PKI) technology or asymmetric encryption. Under PKI, each user is issued with a private and public key. According to *Financial World* (1999), "the public key can be broken, but the private key cannot be intercepted [since] the trusted certificate authority guarantees security by protecting the private key from insecure access." This method ensures the information content of the data, its authenticity, preventing any undetected modification, repudiation and unauthorised use.

Such technology is even more vital for transactions involving the exchange of electronic contracts and the movement of funds or sensitive information, as occurs with e-banking. In this vein, the supervisory agency must ensure that the e-bank provides a comprehensive security policy, backed by adequate contingency measures. Practitioners view strong encryption as essential, if only for boosting consumer confidence; but opposing views suggest that strong cryptography might conceal criminal activities. Though valid in theory, the positives of using encryption outweigh the negatives.

However, the benefits of encryption do not imply that the use of electronic signatures be totally applied, since some documents must still be signed in the traditional fashion. Users must recognise that an encrypted electronic signature provides some assurance of the content, whereas the digital signature in itself cannot guarantee the identity of the sender, but serves only to identify the computer from which the message is sent. Note, it is possible for personal identification numbers (PINs), and cryptographic keys to be compromised. Clearly, as a result of its

importance, in devising any regulation of certificate providers, a system should be in place for their licensing. This is expected to further enhance the level of trust in e-banking transactions. Furthermore, such a structure would serve to reassure users that all confidentiality and other requirements are stringently adhered to.

An added defence in breaches or affiliated criminal activities is that banks should adhere to the commonly cited "know-your-customer" guidelines. If properly implemented, within an effective operational and regulatory framework, such guidelines should prove pivotal in this regard. In the final analysis it is essential that the operators of an e-bank provide sound management of all risks on an on-going basis, comply with the relevant number of initial requirements aimed at ensuring financial soundness, and subject the entity to on-going supervision by a competent authority, such as the Central Bank of Barbados.

Transparent legal and administrative arrangements

Apart from changes to the institutional and technical infrastructure, legal issues have been, and will need to be further, addressed in anticipation of e-banking activities. One such piece of legislation is the Electronic Transactions Act (2001), which accounts for - among other things - the validity of electronic signatures. However, to maintain technology neutrality, an e-bank should be required, in addition to having access to electronic signatures, to receive signed agreements and documents in hard-copy form. Furthermore, customers should be given the option of using e-signatures, while being accorded the opportunity to view the full text of the relevant document, with appropriate risk warnings on the web site before a contract is agreed upon. After this, there should be at least one verification check, such as an e-mail return receipt facility that announces execution.

Clearly, within the sphere of e-commerce, consumer and data protection issues cannot be overlooked, since such rights do exist in the laws of many of Barbados' larger trading partners. Moreover, consumers all over the world have been so sensitised

to the concept of privacy on the Internet, that it has become an over-riding and pervasive concern. This has also spread to Barbados, where interestingly, there is no recognition of any right to privacy on the statute books. Despite this, if many local users are concerned about their privacy – as well they should - then it is expected that users will only conduct business on-line if they are confident that their privacy will be protected.

In banking, privacy[11] is seen as one of the pillars on which customer relationships are built. The more businesses respect privacy, the greater the expected level of confidence customers will have in electronic banking. The difficulty arises with respect to the appropriateness of imposing on electronic commerce higher standards of privacy than for other media. It seems appropriate to do so, given the reach of the information that a consumer may provide and the absence of control over access to that information. E-banking will not only impact on regulation and supervision, but also on monetary policy formulation, a topic which will be discussed in the following section.

4. Monetary Policy Effects

From a central banking perspective, e-banking will perhaps have its most interesting impact on monetary policy. One such effect results from the changes that e-banking is likely to exert on the structure of the real economy. Information technology-induced changes to payment and settlement systems will also influence the effectiveness of monetary policy, in addition to the day-to-day functioning of the Central Bank. Financial innovation is nothing new. However, the development of privately-issued e-money, which could accompany the evolution of a sophisticated international e-banking infrastructure, does raise questions about the ability of central

[11] On-line privacy can be defined as a user's expectation that their on-line activities, transactions and preferences will be kept private, and will not be altered or misrepresented.

banks to manage the domestic financial system. Some observers (Friedman, 2001) argue that monetary policy could be doomed to irrelevance as official currency becomes marginalised. The widespread adoption of privately-issued e-money appears unlikely given the likely difficulty e-money issuers would face in displacing cash, credit cards and cheques from the current dominance in the payments system. However, even in the unlikely event of privately-issued e-money successfully reducing the demand for traditional money, the primary concern for Caribbean governments is not likely to be in the area of monetary policy, but in the area of exchange controls.

Indeed, the key challenge for Caribbean policy-makers is that the widespread adoption of e-money would negate their current attempts at capital controls. In the event of the widespread adoption of e-money, such regimes are likely to be hardest hit. Since the Internet recognises no political boundaries, the cost of transferring e-money within a country is equal to the cost of transfer between different countries. The ability to seamlessly transfer money across borders is likely to render traditional exchange control methods untenable, and could well force central banks to abandon exchange controls as an instrument of policy.

There stands another concern with the advent of e-money. In the absence of or a reduction in seigniorage income, central banks' profitability could be adversely impacted. However, the central banks possess a number of options which could maintain their role within the financial system, even if private network money or software value cards displace conventional central bank money. The options exercised would depend on the practicality of market-based solutions versus the effectiveness of legislative fiat.

Non-market solutions are likely to be both more prevalent and practical for regional central bankers. For instance, with the proliferation of e-money issuers, central banks could issue their own network money or smart-cards that would directly compete with those of the private sector. Issuance of successful e-money by central banks themselves would ensure a continuing demand for central bank liabilities. The object would be to allow electronic payments with the finality of paper

currency, but with the divisibility, security, and ease of transportation associated with the new electronic devices. Under normal circumstances "officially"- issued e-money would possess a number of advantages.

As Good (1997) highlighted "If the issuer of the stored-value instrument is a central bank or another official body, credit risk would not be considered an issue, since the electronic value of money would have a status similar to that of cash - a risk-free liability of the state." Although there may remain a technical risk, a central bank would be able to support its electronic money scheme without undermining public confidence in the payment media. She further notes that stored-value instruments issued by a private institution might not have equivalent financial integrity. For private e-money to gain such credence, its value would most likely be required to be collateralised by short-term government securities, thus making its credit risk to that of central bank's obligations. If the stored-value instrument was backed by investments in riskier or less liquid assets, its holders and acceptors would be exposed to a greater level of credit and liquidity risk.

Lerner (1947) argued that, "At the present time in a normally well-working economy, money is a creature of the state. Its general acceptability, which is its all-important attribute, stands or falls by its acceptability by the state." Furthermore, tax payments in most modern economies are non-trivial and range from around 20 per cent to over 40 per cent of GDP. Requiring them to be made in conventional money would go a long way toward keeping the demand for conventional "money"- and hence for central bank liabilities - coupled to the expansion or contraction of economic activity.

A second option stems from the possibility of widening the regulatory net. The European Central Bank (ECB) acknowledges that the definition of "credit institution" as currently laid out may need to be broadened to include all issuers, including those of electronic money. The proposed objective is to provide a level playing field, so as to ensure that all issuers of electronic money be subjected to an appropriate form of prudential supervision. The ECB report also advocated that the issuance of electronic money should be limited to credit

institutions "as defined in Article 1 of the First Banking Co-ordination Directive"- that is, conventional banks. While not a purely competitive outcome, the ECB's approach has some merit. The information technology revolution is unlikely to completely eliminate the fundamental informational asymmetries, which make the business of banking viable. Thus, reserve requirements whether of the traditional kind or that expanded to include the "e-money", are likely to remain a useful lever in monetary policy-making, if e-money issuers are constrained to banks.

Still, based on current estimates, it does not seem as though in the near future that e-money will become pervasive enough to make serious inroads into the note-issuing function of the Central Bank. If e-money issuers do not engage in fractional reserve lending they are likely to evolve into simply another means of payment. Furthermore, the barriers faced by private issuers of e-money are pervasive and are likely to include low profitability, market inertia and the threat of regulatory restrictions by the states. In the improbable event of the widespread adoption of privately issued e-money, the major threat central banks would face would be to their exchange control arrangements and their profitability. Caribbean central banks still possess a number of key options derived from their intrinsic advantage of being the state's bank. These advantages are likely to undermine the accuracy of Jordan and Stevens' (1996) assertion that neither government regulation of private issuers nor direct government issuance of electronic forms of currency seems likely to ensure significant demand for central bank money over the next century.

Conclusion

E-banking and the advances in technology and their use are expected to usher in widespread changes in the domestic banking system, and will necessitate regulatory and legal changes congenial to technological change, thus forcing the adoption - in some cases – of radical reforms of current systems and structures. These potential changes range from the erosion

of the effectiveness of monetary policy to the challenges resulting from the formulation of policies necessary to deal with the increased risks emanating from electronic banking. One widely mooted area of change has been that of policy formulation in the financial system, but in the final analysis, money, and monetary policy, cannot be defined without reference to the power of the state. As Goodhart (2000) pointedly states, "What the ability of the central bank ultimately depends upon is the fact that it is the government's bank, and has the power to intervene in financial markets without concern for profitability (let alone profit maximisation)". Still, what is required is greater interaction between the private sector and regulators in formulating safety measures that are responsive to the needs of market participants.

References

Adderly, J.L. and J. Justilier; The Government Securities Market and its Role in Supplementing Monetary Policy in the Bahamas, *Social and Economic Studies,* Vols. 48, Nos. 1 & 2, 1999, pp. 43-68.

Bank for International Settlements; Implications for Central Banks of the Development of Electronic Money, Basle, Working Papers, October 1996.

Basle Committee on Banking Supervision, Risk Management for Electronic Banking and Electronic Money Activities, Basle, Working Paper, March 1998.

DeYoung, R.; The Financial Performance of Pure Play Internet Bank, *Economic Perspectives, Federal Reserve of Chicago,* First Quarter, 2001, pp. 60-75.

Electronic Banking Group of the Basle Committee; Electronic Banking Developments and Supervisory Issues, Basle, April 2000.

European Central Bank; The Effects of Technology on EU Banking Systems, Working Papers, July 1999.

Financial World; Special Report: Electronic Delivery, *Financial World,* October 1999.

Friedman, B.M.; The Future of Monetary Policy: The Central Bank as an Army with Only a Signal Corps, *International Finance,* Vol. 2, 2001, pp. 321-338.

Good, B.A.; Electronic Money, Federal Reserve Bank of Cleveland, Working Papers, No. 9716, 1997.

Goodhart, C.A.E.; Can Central Banking Survive an IT Revolution?, mimeo, London School of Economics, June 2000.

Jordan, J.L. and E.J. Stevens; Money in the Twenty-first Century, Financial Services Working Paper, Financial Services Research Group, Federal Reserve Bank of Cleveland, Series No. 2, 1996.

Lerner, P.; Money as a Creature of the State, *American Economic Review*, Vol. 37, May 1947, pp. 1–16.

Parris, Y.; The Impact of Electronic Banking on the Banking Community of Barbados, presented at the 12th Annual Conference of Regional Central Banks' Information Systems Specialists, Barbados, 2001.

Rowe, H.; Financial Services Regulation and the Internet, *Journal of Financial Regulation and Compliance*, Vol. 6, No. 2, 1998, pp.135-149.

Smith, R. G.; Internet Payment Systems and Their Security Risks, *Journal of Financial Crime*, Vol. 7, No. 2, 1999, pp. 155-160.

The Economist; Online Banking, *The Economist*, December 4th, 1999.