Journal of African Law, page 1 of 33 © SOAS, University of London, 2018.
doi:10.1017/S0021855318000104

Regulation for E-payment Systems: Analytical Approaches Beyond Private Ordering

[redacted]

Abstract

Technology-driven payment instruments and services are facilitating the development of e-commerce; however, security concerns beleaguer their implementation, particularly in developing countries. This article considers the limits of private ordering in the regulation of e-payment systems. It uses Nigeria to exemplify a developing country that is increasingly pushing for the adoption of a regulatory framework for e-payment systems based on private ordering. It argues that, although technical standards and self-regulation by the financial industry are important, law is an essential regulatory mechanism that is largely absent. The article proposes that law be used as a mechanism to set and compel compliance with technical and industry standards, thus building trust, catering to public interest concerns and legitimizing the regulatory process.

Keywords

E-payment, regulation, private ordering, public interest, Nigeria

INTRODUCTION

Over the past decade, a "silent revolution" in payment systems has occurred with the introduction and implementation of e-payment systems. Aided by the rapid proliferation of information and technology, it has not been without inherent problems. Although e-payment systems have enhanced interoperability, convergence and competition in the payment industry (and, from a user's perspective, efficiency and flexibility), the ensuing migration to the

[redacted]

The authors wish to thank [redacted] and anonymous referees who made helpful comments on an earlier draft of this article.

systems has aggravated the risk of cybercrime and undermined trust and confidence in payment services and their providers.[1] Likewise, banks and other providers of e-payment services have become more susceptible to large-scale data breaches, while users face the risk of financial losses from identity theft and fraud. Therefore, effective e-payment regulation is central to building trust and confidence in electronic transactions, particularly for developing countries in their bid to bridge the digital gap and leverage the benefits of the global market.

The European Central Bank aptly defines e-payments as payments made over the internet using remote payment card transactions, online banking systems or e-payment providers with which the consumer has set up an individual account.[2] Nigeria is a good example of a developing nation that is increasingly pushing for the adoption of these systems.[3] As recent government policies[4] demonstrate, objectives include developing internationally recognized payment systems and achieving global digital market integration. Thus, migration to card transactions and other electronic payments has increased. However, with that migration, Nigeria now faces significant challenges in securing payments. Because of its rather unsavoury reputation related to scams, advance fee fraud, identity theft and cybercrime in general, there is a shadow of suspicion over electronic transactions and communications originating from or terminating in the country.[5] Effective regulation of the relatively new e-payment systems could therefore represent a significant opportunity to build trust and control crimes in e-payment systems.

This article argues that, as presently constituted, regulation in Nigeria focuses exclusively on technology-based solutions and payment card industry data security standards (PCIDSS),[6] an industry private ordering not supported

1 See European Commission "Towards an integrated European market for card, internet and mobile payments" (COM 941 2011), para 2.3.

2 European Central Bank "The payment system" (2010), available at: <https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf> (last accessed 12 February 2018); see also Ofcom "Innovation in UK consumer electronic payments: A collaborative study by Ofcom and the Payment Systems Regulator" (2014), available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0014/45041/e-payments.pdf> (last accessed 12 February 2018).

3 Other countries, particularly in Africa, are also involved in this drive. For example: Kenya's M-pesa is the largest market for mobile money; South Africa has the most developed e-payment systems in Africa; and Ghana and Tanzania are pushing for wider adoption of e-payment systems. See KPMG "Payment developments in Africa" (vol 1, 2015), available at: <https://assets.kpmg.com/content/dam/kpmg/za/pdf/2016/09/Payment-Developments-in-Africa-2015.pdf> (last accessed 12 February 2018).

4 These include "National payment systems vision (NPSV) 2020" developed by the federal government; and the Central Bank of Nigeria's "Cashless Nigeria" policy.

5 D Smith "Nigerian scams as political critique: Globalization, inequality and 419" in R Grinker, S Lubkemann and C Steiner (eds) *Perspectives on Africa: A Reader in Culture, History, & Representation* (2010, Blackwell Publishers) 616 at 617–28.

6 PCIDSS is a proprietary information security standard for organizations that handle branded credit cards from the major card companies including Visa, MasterCard and

by any mandatory legal requirements. This approach is unsustainable for three reasons. First, e-payments are a multi-stakeholder environment comprising banks, as well as financial and non-financial institutions. As such, a private ordering arrangement designed for banks and other financial institutions may not be effective outside that industry unless it is recognized as applicable and binding. Secondly, the technical standards on which the system depends are inefficient because there are no laws mandating security standards or compliance with the standards. Thirdly, there are serious public interest concerns that limit the effectiveness of private ordering. In the context of e-payments, public interest concerns include controlling cybercrime and correcting market failures, as well as the need for fairness, transparency and clarity in the adjudication and administration of justice.[7]

This article argues that law is crucial to engendering the efficiency and legitimacy of e-payment regulation because of its capacity to regulate multiple players in the heterogeneous e-payment market and to enforce technical standards. Law plays a central role in ensuring that public concerns in e-payment systems are adequately addressed. However, since the choice between private ordering and state regulation cannot be binary in the complex environment of the internet, Lessig's theory of modalities of regulation in cyberspace is used to highlight how the law would regulate efficiently in the context of e-payment systems and services. Lessig's model is essential to a critical understanding of the argument that private ordering is inherently weak and subject to manipulation by the payment industry. The theory also justifies the proposition that regulation through formal rules is better at securing recognition and acceptance for regulatory mechanisms and fostering compliance.

The article starts with a brief analysis of how private ordering fits into the broader debate on regulation. It then considers the threats posed to e-payment systems and how the integration and convergence of e-payment and other services undergird the inadequacy of regulation in Nigeria. The article further evaluates the efficiency of industry-mandated technical standards and PCIDSS as a private ordering mechanism. It argues that, while private ordering can be quite efficient, it is inherently limited in heterogeneous markets and seldom caters to the public interest. Therefore, to achieve the non-efficient goals of regulation, the government needs to constrain private actors. The article concludes with a proposal for a regulatory approach that models Lessig's theory of modalities of regulation in cyberspace. It reformulates Lessig's regulatory modalities of code, market, norms and law to develop a proposal that incorporates technologies, users, industry and law. It argues that a correct synthesis of these modalities leads to efficient regulation of e-payment processes,

---

contd
American Express. For more information, see: <https://www.pcisecuritystandards.org/pci_security/> (last accessed 12 February 2018).

7 The concept of public interest is discussed in the next section.

instruments and institutions, legitimizes the regulatory process and addresses public interest concerns.

REGULATION BY PRIVATE ORDERING: LEGITIMACY AND PUBLIC INTEREST CONCERNS

The meaning and scope of regulation is varied and contested. Morgan and Yeung have argued that "regulation is a phenomenon that is notoriously difficult to define with clarity and precision, as its meaning and the scope of its inquiry are unsettled and contested".[8] However, a useful way to navigate the regulatory debate is to consider its broad and narrow meanings based on the origin or source of a regulatory framework. In a narrow sense, regulation refers to formal legal rules aimed at controlling the behaviour of entities or individuals.[9] This so-called command and control model of regulation implies regulation by law or at least by state-appointed actors with the objective of benefiting society or a section of society. In a broader sense, regulation refers to any form of behavioural control, whatever its origin.[10] This notion of regulation includes both state and non-state actors and includes all forms of social and economic influence designed to affect behaviour, whether it is state-based, from markets or comprises self-regulatory mechanisms in professions or trades.[11]

Private ordering refers to rules, regulations and codes of practice developed by private actors (such as industry, firms and sectors) to influence behaviour within the firm, sector or industry.[12] Private actors often voluntarily adopt codes and observe rules without government sanction and enforcement.[13] PCIDSS is an example of private ordering in the payment industry. PCIDSS is an established global standard for cardholder account protection across all parties in the payment chain, including acquirers, third party processors and merchants.[14] Its core framework consists of 12 requirements organized

8 B Morgan and K Yeung *An Introduction to Law and Regulation* (2007, Cambridge University Press) at 3.

9 R Baldwin, M Cave and M Lodge *Understanding Regulation Theory, Strategy and Practice* (2nd ed, 2012, Oxford University Press) at 3.

10 Ibid.

11 Ibid.

12 They have also been defined more broadly to include rules originated by the private sector but put in place by sovereign governments, as well as rules put in place by private actors following government delegation. However, a critical reading of the literature suggests that these more aptly describe self-regulation generally and could refer to other models of regulation such as co-regulation and meta-regulation. See S Schwarcz "Private ordering" (2002–03) *North West University Law Review* 319 at 324; see also C Coglianese and E Mendelson "Meta-regulation and self-regulation" (Penn Law School public law and legal theory research paper no 12-11) 1 at 6–9.

13 Schwarcz, ibid.

14 PCI Security Standards Council "PCI security", available at: <https://www.pcisecuritystandards.org/pci_security/> (last accessed 3 March 2018).

under six functional goals and requires a combination of physical, technical and operational measures to protect cardholder data, whether in storage or transmission.[15] The standard was developed in response to an increasing incidence of cardholder account theft and is intended to help organizations proactively protect customer account data.[16]

The purported legitimacy of private ordering comes from its ability to utilise market incentives to allocate public resources.[17] Because it can avoid the expensive rule-making and enforcement processes that accompany state regulation, the most obvious advantages of private ordering are its efficiency in cost saving and its expertise in the rule-making process.[18] Conversely, because the rule-maker ultimately expects compliance from itself and because compliance with private ordering is almost always entirely voluntary, private ordering tends to undermine the "consequences" element of regulation. Also, because private ordering mechanisms can be diffuse, in that they tend to apply to homogenous sectors and their goals can therefore be quite narrow, private ordering tends to be limited in the way it addresses broader public interest issues. In line with Ogus, if the term "regulation" is used to denote law that implements a collectivist system, then arguably it must be taken that regulation contains the idea of a superior authority, being the state. It has a directive function and compels individuals and groups to behave in particular ways, and threatens sanctions if they do not comply. As a public law, it enforces requirements that cannot be circumvented by private agreement, because the state plays a central role in its formulation. This suggests that the characteristics of sanctions are often more noticeable in state or formal regulatory regimes and that state regulation is more efficient at modifying behaviour because it carries the threat of state enforcement and sanctions. It may also explain why references to regulation in political rhetoric are seldom taken to mean non-state regulation.[19] Furthermore, as Black defines it, regulation is "the sustained and focused attempt to alter the behaviour of others to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard setting, information gathering and behaviour modification".[20] Therefore, even when non-state actors (such as social norms, technologies or markets) influence how regulatory systems operate, and while regulatory systems might harness these influences toward a regulatory end, they do not themselves

15 Ibid.
16 Ibid.
17 Schwarcz "Private ordering", above at note 12 at 319.
18 See generally, K Webb "Understanding the voluntary code phenomenon" in K Webb (ed) *Voluntary Codes: Private Governance and Public Interest and Innovation* (2004, Carleton University Press) 3.
19 A Ogus *Regulation: Legal Form and Economic Theory* (2004, Hart Publishing) at 15.
20 J Black "Critical reflections on regulation" (2002) 27 *Australian Journal of Legal Philosophy* 1 at 20.

constitute regulation.[21] Again, the suggestion here is that formal or legal rules are better at setting standards and achieving behaviour modification.

Surely, if regulation formally involves interference by a party that is not directly involved in or part of the activity involved,[22] the legitimacy of private ordering should be subject to scrutiny. However, legitimacy is arguably not necessarily tied to rules made by the legislature and also connotes recognition of the source of the rule, confidence in the rule-making process, and acceptance of the source and process through compliance with the rules, so alternative measures for any claim to legitimacy by private ordering systems must be explored.[23] Baldwin, Cave and Lodge provide a broader basis for adjudicating good regulation. According to them, although a legislative mandate (which implies that a regulatory framework derives authorization from an elected legislature) is one of the essential criteria of good regulatory regimes,[24] good regulation must also satisfy four additional criteria. These are: accountability and control, which underscores the need for regulators to be properly accountable; due process, which presupposes support for regulation because the procedures are fair, open and accessible; regulatory expertise, which denotes trusted regulator judgment based upon specialized knowledge, skills and experience; and efficiency, which implies that the legislative mandate in support of a regulatory regime is being implemented effectively.[25] In effect, while some of these criteria appear to depend on some formal monitoring or enforcement process, others (such as regulatory expertise) depend more on the industry and may arguably be attained by private ordering. Nevertheless, for a regulatory regime to be perceived as good and perhaps legitimate, it should arguably satisfy all four criteria.

More significantly, since rationalization that regulation proceeds in the "public interest" is often at the base of most regulatory instruments,[26] it is important for regulation to account for the public interest components of the regulated activity. As Mitnick argues, regulation is "the public administrative policing of a private activity with respect to a rule prescribed in the public interest".[27] Selznik sees regulation as "a sustained and focused control exercised by a public agency over activities that are valued by a community"[28] and, in Lennes's view, the deliberateness and intentionality to bring about a regulatory end, which must be seen as a deliberate supervision of private

21 Ibid.

22 BM Mitnick *The Political Economy of Regulation: Creating, Designing, and Removing Regulatory Forms* (1980, Columbia University Press) at 242.

23 See for example JR Macy "Public and private ordering and the production of legitimate and illegitimate rules" (1997) 82/5 *Cornell Law Review* 1123 at 1133.

24 Baldwin, Cave and Lodge *Understanding Regulation Theory*, above at note 9 at 25.

25 Id at 25–39.

26 Mitnick *The Political Economy*, above at note 22 at 7.

27 Id at 7.

28 P Selznick "Focusing organisational research regulation" in R Noll (ed) *Regulatory Policy and the Social Sciences* (1985, University of California Press) 363 at 363.

activity in the interest of public rights, interests and welfare, is what qualifies an activity as truly regulatory in the first place.[29] These definitions underline the public interest theory of regulation, which justifies regulation as a corrective to perceived deficiencies in the operation of the market.[30] The theory underpins regulation as a restrictive activity directed toward private entities on the basis of general rules that are conducive to the public interest.[31]

It is not the authors' intention to get into extensive argument about the meaning and scope of public interest, yet it is relevant to note that public interest is a contested and nebulous concept. Public interest has been described as a vague and indeterminable concept,[32] and a catch-all phrase for the subjective interest of lawmakers or powerful interest groups.[33] According to Feintuck, although "public interest has an air of democratic propriety, the absence of identifiable normative content renders the concept insubstantial, and hopelessly vulnerable to annexation and colonization".[34] Nevertheless, he argues, some common elements of its contents are ascertainable.[35] Further, public interest must assume or underpin the existence of some interests common to all members of society and therefore mesh with society's dominant values.[36] It underlines certain democratic values and serves to complement human rights.[37] Public interest also assumes an ideal of general welfare and the maintenance of conditions that permit an ongoing social order.[38] Therefore, the nebulous nature of public interest notwithstanding, it is certainly right to assert that, in a regulatory context, intervention into private activity is justified by reference to an economic belief in the efficacy of competitive market forces.[39] For example, if market efficiency is a public good[40] that could arguably be achieved by private ordering or self-regulation, it would still ultimately fall on government to regulate market efficiency in order to correct market failures. This is because public goods are susceptible

29 R Leenes "Framing techno-regulation: An exploration of state and non-state regulation by technology" (Legisprudence Tilburg Law School legal studies research paper series no 10/2012) 143 at 149.

30 RA Posner "Theories of economic regulation" (1974, NBER working paper no 41) at 1.

31 JG Christensen "Competing theories of regulatory governance: Reconsidering public interest theory of regulation" in D Levi-Faur (ed) *Handbook on the Politics of Regulation* (2011, Edward Elgar) 96.

32 Mitnick *The Political Economy*, above at note 22 at 91.

33 For example, Posner "Theories of economic regulation", above at note 30 at 4–5.

34 M Feintuck *The Public Interest in Regulation* (2004, Oxford University Press) at 33.

35 Id at 38.

36 Id at 11.

37 Id at 39.

38 Id at 39–41.

39 Id at 58.

40 A public good is a commodity the benefit of which is shared by the public, or by a group within it. It consists of two characteristics: that consumption by one person does not leave less for others to consume; and it is impossible or too costly for the supplier to exclude those who do not pay for the good but enjoy the benefit. See Ogus *Regulation*, above at note 19 at 33.

to free-rider problems.[41] In this sense, even if the public interest is debatable, it appears that regulation in the public interest must seek the welfare, protection and benefit of the public at large or at least of a section of society. Correspondingly, it is arguable that, if regulation ultimately controls crimes, prevents or corrects market failures and imbues transparency in adjudication, it is unequivocally in the public interest.

These definitions and characteristics of regulation suggest that there are two problems with using private ordering as a regulatory model. The first is that it raises questions about whether the private ordering is legitimate in the sense that it satisfies the criteria of good regulation. The second and more crucial problem is whether it accounts for public interest concerns in e-payment services and systems. The following sections highlight how new cybercrime threats have forced new regulations and the ways in which these create legitimacy problems.

THE THREAT LANDSCAPE: CYBERCRIME AND THE LIMITS OF BANKING AND FINANCIAL GUIDELINES

There is a profound irony at the heart of this debate. Fraud was already endemic in Nigeria, even before the widespread use of computer systems. However, it is widely acknowledged that the use of electronic systems acted as a great facilitator and made the so-called "419" or "advance-fee" e-mail frauds remarkably successful.[42] The proliferation of "419 spam" exemplifies the internet-created opportunity. By offering global accessibility,[43] the internet effectively enabled fraudsters to send spam e-mails, typically requesting assistance in transferring illegally sourced funds to bank accounts abroad.[44] Perhaps due to the limited infrastructure for electronic money transfers and the stigmatization of the Nigerian political class as highly corrupt, many perceived these e-mails as credible and the e-mails were particularly successful with victims outside the country. The scale of the problem forced PayPal, the global payment service provider, to close all Nigerian accounts in 2005.[45]

Partly because of existing cybercrime threats, government policies to promote e-payments in Nigeria were unsuccessful at first. However, in 2011, the Central Bank of Nigeria (CBN) introduced the "Cashless Nigeria" project. This project significantly improved migration to e-payments, primarily by

41 Ibid.

42 See A Smith "Nigerian scam e-mails and the charms of capital" (2009) 23/1 *Cultural Studies* 27 at 30 and 33.

43 M Zook "Your urgent assistance is requested: The intersection of 419 spam and new networks of imagination" (2007) 10/1 *Ethics, Place & Environment* 65.

44 J Oboh and Y Schoenmakers "Nigerian advance fee fraud in transnational perspective" (2010) 15 *Policing Multiple Communities* 235.

45 See "Countries and regions supported by PayPal", available at: <https://developer.paypal.com/docs/classic/api/country_codes/> (last accessed 12 February 2018).

penalizing cash transactions.[46] With the increasing adoption of e-payments, the threat of cybercrime changed significantly. Targets became more domestic and schemes evolved to match the increasing online population.[47] As the CBN admitted, fraud migrated to card-not-present transactions and other web-based payment applications.[48] Due to the ubiquity of the internet and increasing payment mobility (Nigeria has about 60 million internet users), it is reasonable to assume that data breaches, identity theft and fraud will increase. Hence, the CBN has made a significant effort not only to increase awareness of cybercriminals' tactics and how users of e-payment services can avoid victimization, but also to recommend increased resilience of the payment systems' infrastructure and work-streams to encourage the use of e-payment systems.[49]

The CBN regulates e-payment services and transactions by issuing guidelines specific to different transactions. For example, its 2001 Guidelines on Point of Sale Card Acceptance Services (POS Guidelines) deal with card systems, mobile regulations deal with mobile payments and mobile moneys, and so on.[50] The problem is not that there are different regulations but whether the regulations are applicable across the broad spectrum of e-payment services and providers. To illustrate this, the POS Guidelines stipulate that computer networks used to transmit financial data over the internet must meet the required standards specified for data confidentiality and integrity. The precise standards specified by the regulations are that all payment service providers comply with PCIDSS, as a minimum use the 3DES encryption standard, and apply a minimum of two-factor authentication to verify user access to systems and services.[51] The use of public key infrastructure (PKI) is optional, as the e-banking guidelines provide that banks may need to consider the use of PKI to authenticate users.[52]

---

46 For example, the CBN had directed Nigerian banks to charge processing fees on all cash transactions but not for e-payments; see CBN letter titled "Industry policy on retail cash collection and lodgement" (IITP/C/01 circular BPS/DIR/GEN/CIR/01/003, 16 March 2012) (copy on file with the authors).

47 For example, ATM fraud constituted the leading consumer complaint to the CBN between 2010 and 2012, as a result of which the CBN directed the system to migrate from basic "chip and PIN" to EMV cards (cards using the global standard for chip-based debit and credit card transactions, developed by Europay, MasterCard and Visa). See Nigeria Deposit Insurance Corporation "Annual report and statement of account" (2010, 2011 and 2012), available at: <http://ndic.gov.ng/publications/> (last accessed 12 February 2018).

48 Nigeria Electronic Fraud Forum (NeFF) "Annual report 2012" (copy on file with authors). It is not clear whether the report was subsequently published or otherwise made publicly available.

49 See CBN "Payments system vision 2020" (release 2.0, September 2013).

50 See generally Electronic Banking Regulations 2003; Revised Guidelines on Stored Value / Pre-Paid Card Issuance and Operation 2012; Standards and Guidelines on Automated Teller Machines (ATM) Operations in Nigeria 2010; Regulatory Framework on Mobile Payment Services in Nigeria 2014; and the Electronic Banking Regulations 2003.

51 POS Guidelines, item 3.1.

52 E-banking Guidelines, item 1.5.2 (emphasis added).

Apart from the fact that Nigerian banks are affiliated with global card service providers and are therefore obliged to comply with PCIDSS by contractual agreements with relevant card networks, the CBN mandates compliance with PCIDSS by providing that, "[a]ll industry stakeholders who process and / or store cardholder information shall ensure that their terminals, applications and processing systems comply with the minimum requirements of the following [PCIDSS] Standards and Best Practices … In addition, all terminals, applications and processing systems should also comply with the standards specified by the various card schemes".[53]

The primary concern here is whether guidelines issued by the CBN will be accepted as generally binding by non-banks and non-financial institutions within the payment chain. The national electronic identity card clearly illustrates the problem. The e-identity card is expected to offer PIN and fingerprint authentication, digital signature and payment functionalities, and it has been proposed that all Nigerians be issued a national identity number, to be used for identification and account establishment purposes.[54] The card is designed to serve as both an identity card and a bankcard. This suggests that, although banks may be leading providers of e-payment services, non-banks and non-financial institutions, including the identity management authority, are now industry stakeholders who could potentially process and / or store cardholder information. If we assume that unregulated access could compromise consumer data on the Nigerian Identity Management Commission (NIMC) database, we begin to see how the adoption of technical security standards prescribed by the CBN could become problematic. Stated differently, although the POS Guidelines mention *industry stakeholders*, it must be presumed that these are stakeholders within the banking industry to which banking regulations apply; institutions like NIMC may not consider themselves bound to implement 3DES encryption or apply two-factor authentication or even comply with PCIDSS. The same argument applies to mobile network providers, which are regarded as providers of infrastructure or platforms on which mobile payments may be initiated and completed, or mobile money stored.[55]

Although these factors can raise questions of legitimacy in the sense that the CBN rules and standards are not generally accepted or recognized as binding, they could also suggest that the guidelines are inherently limiting. The following sections analyse the limits of technical standards mandated by the CBN and PCIDSS even within the banking and financial industry where they must apply. They also assess the constraints of PCIDSS as a specific form of private ordering. The analysis highlights areas where formal laws would produce better regulation.

53 POS Guidelines, item 3.1.

54 See Nigerian Identity Management Commission Act 2007, secs 27, 28 and 29.

55 See Revised Guidelines on Stored Value / Pre-Paid Card Issuance and Operation 2012.

THE LIMITS OF TECHNICAL STANDARDS

It was noted above that the CBN prescribes compliance with PCIDSS, the use of a 3DES encryption standard and a minimum of two-factor authentication, as well as the optional deployment of PKI. In a sense, therefore, the industry relies on technology to regulate e-payment services and systems. Although technology-based security systems are of immense importance to users because technology regulates behaviour without requiring users to change their behaviour,[56] there are constraints on technology and three clear areas that may inhibit efficient regulation in Nigeria. These are cost, the industry-centred character of technology application and the fact that no security is completely impervious to threats.

Technology is expensive

The cost of implementing mandatory technologies, particularly PCIDSS, affects the willingness of industry stakeholders to deploy them. For example, although all parties (including acquirers, third-party processors and merchants, as well as all entities that store, process or transmit cardholder data) are expected to comply with PCIDSS, the level of compliance in Nigeria is questionable.

According to one estimate, the cost of fully implementing PCIDSS for a merchant in Nigeria is about USD 20,000, which is considerably more than the total operating capital of an average merchant.[57] Thereafter, the business needs an additional USD 1,000 per year for software updates to electronic points of sale.[58] Merchants must also bear the additional cost of periodic system vulnerability and compliance scans from third-party firms appointed by PCIDSS operators to ensure full and ongoing compliance. Arguably, this prohibitive cost can only be borne by the major players in the industry, such as banks and switching companies.[59] Invariably, cost is a barrier to entry into e-payment services and may also lead to compromises in security standards. As noted in PCIDSS's own guidelines, the prohibitive cost of compliance invariably leads to compromises in consumer information, such that businesses that are unable to encrypt data because of technical constraints or business limitations adopt compensating controls designed to mitigate associated risks.[60]

---

56 See further at note 65 and sections on "Private ordering and the index for strong regulation" and "How law regulates: Lessig's modalities of regulation in cyberspace and the regulation of e-payments" below.

57 FC Obodoeze et al "Enhanced modified security framework for Nigeria cashless e-payment system" (2012) 3/11 *International Journal of Computer and Science Applications* 189 at 189.

58 Ibid.

59 Id at 189–90.

60 See Security Standards Council "Securing the future of payments together", available at: <https://www.pcisecuritystandards.org/> (last accessed 12 February 2018).

However, beyond identifying the likely impacts of the prohibitive cost of PCIDSS, the payment industry has offered no viable solution. In fact, the possibility that service provider organizations will not deploy PCIDSS is heightened by the lax oversight. As an example, although the PCIDSS requirements are couched in mandatory terms, compliance is primarily determined through self-assessment. Additionally, while the Security Standards Council sets PCIDSS, it has no obligation to validate or enforce any organization's compliance with the standards or impose penalties for non-compliance. Enforcement and penalties are governed by card brands and their partners, who may impose financial penalties or withdraw card acceptance services.[61] There is therefore a lack of uniformity in the implementation of the standards, because each card brand has different programmes for compliance, validation and enforcement.[62]

Whether or not these drawbacks indicate a need to re-evaluate PCIDSS, the authors argue firmly in favour of the establishment of an independent legal authority to enforce the standards, on behalf of either the Security Standards Council or the card brands.[63] Alternatively and more efficiently, legislation may set legal standards for securing card transactions and other e-payment services. Indeed, with developing countries such as Nigeria, the failure to legislate the regulation of payment card transactions translates to governments effectively ceding consumer protection to private law-making by card associations and banks.[64]

Technology in industry regulation: Misuse in evidential matters

Another important aspect of regulation by technology is its near-total dependence on industry for implementation. Because of its highly technical nature, the deployment of technology is better understood by industry, and this may lead to discriminatory and even abusive use. Lessig noted that, because of the self-executing and independent nature of technology (or code) regulation, the application of law or legal constraints in cyberspace is inherently limited.[65] However, the most persuasive argument made is that, because code or technology can control better and more effectively than law, it may be misused, particularly by the market. As such, code may not strike a proper balance or protect the various values prescribed by law and may become quite arbitrary in its application. In other words, technology is not always a positive regulator and does not always constrain in a manner that promotes the law.

61 Ibid.

62 EA Morse and V Raval "PCI DSS: Payment card industry data security standards in context" (2008) 24 *Computer Law and Security Report* 540 at 553.

63 Id at 551.

64 AS Rosenberg "Better than cash? Global proliferation of debit and prepaid cards and consumer protection policy" (2005, Berkeley University Press (Bepress) Legal Series paper 766).

65 See L Lessig *Code Version 2.0* (2nd ed, 2006, Basic Books) 120 at 127.

Wu makes this point more forcibly by asserting that code could be used as a mechanism of avoidance rather than protection.[66]

Although there have been no cases on this point in Nigeria, some cases in England demonstrate how abusive uses of technology by the financial and payment industry can undermine the judicial process and result in injustice.[67] The claim in *Job v Halifax PLC* (*Job*)[68] was for the sum of GBP 2,100 (with interest), which the claimant argued had been wrongfully debited from his account with Halifax Bank through the fraudulent use of his debit card. The bank admitted the debit but argued that it was justified because the money was withdrawn from the claimant's account using his card and correct PIN. However, in providing evidence, the bank declined to disclose card authentication keys because they were derived from a batch and would compromise other cards in issue. It was argued on behalf of the bank that key management procedures were commercially sensitive information and an outside expert witness could not verify the authentication codes in the logs. However, the claimant argued that these pieces of evidence were essential to the bank's claim that the transactions occurred. They were also necessary to prove that the protocols were flawless and tamper-proof, and particularly that the bank maintained appropriate security controls related to key management. Notwithstanding the bank's failure to produce the evidence, the claimant failed, and judgment was entered in favour of the bank.[69]

Similarly, the claimant in *Rahman v Barclays Bank* (*Rahman*)[70] sought reimbursement from his bank for money debited from his account because of the fraudulent use of his debit card by a third party. Without requiring the defendant bank to provide strict proof, the court accepted its explanation that the fraud was committed because the claimant was negligent in that he gave the thief his card and other authenticating information. Also, without proof, the court accepted the defendant's assertions about the security of its authentication process and its electronic banking system. As the court itself observed, "[t]he bank did not put before the court any detailed evidence about the security information it sought from the fraudster. It had no record of the transaction, save in general terms".[71] An important factor in this case is that the claimant might have prejudiced his case by his alleged untruthfulness regarding the circumstances surrounding the fraud. Nevertheless, when banks

66 T Wu "When code isn't law" (2003) 89 *Virginia Law Review* 101 at 106.

67 Cases from England are particularly relevant here because they constitute persuasive authorities in Nigerian courts, as Nigeria was a British colony and operates a common law system.

68 Case no 7BQ00307 (30 April 2009) in A Kelman "Case judgement: England and Wales" (2009) 6 *Digital Evidence and Electronic Signature Law Review* 235.

69 Id at 238.

70 Clerkenwell and Shoreditch County Court case no 1YE003643 (24 October 2012) in S Mason and N Bohm "Commentary on case on appeal: England and Wales" (2013) 10 *Digital Evidence and Electronic Signature Law Review* 175.

71 Id at 185.

can succeed in defending claims by their customers without producing crucial evidence, there is a disincentive to retain such evidence and produce it when required. Conversely, if the law rendered the production of such evidence mandatory, banks would have no choice but to retain the evidence. As Mason and Bohm argue, "[i]f [the banks'] defence fails for lack of relevant evidence, they will soon enough learn to make sure to retain and produce it. Soft cases make bad law".[72]

These cases demonstrate how technology can serve as a shield and can also be used to manipulate legal and judicial processes. Such manipulations may lead to doubt as to whether justice was served in cases involving disputed transactions between banks and their customers. The provisions of the Nigerian Evidence Act give some indication that Nigerian courts may arrive at conclusions similar to those in *Job* and *Rahman*. The Evidence Act admits electronic signatures generally.[73] Section 93(2) provides that, "[w]here a rule of evidence requires a signature or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences". However, regarding the nature of e-signatures or the evidential weight or standard and burden of proof, the provisions of the law are quite vague. For example, section 93(3) provides that "[a]ll electronic signatures may be proved in *any* manner, including by showing that a procedure existed by which it is necessary for a person, to proceed further with a transaction, to have executed a symbol or security procedure for verifying that an electronic record is that of the person".[74]

It is not clear whether the act is referring to the mere generation of an e-signature or whether it incorporates the means of verifying the correctness of the procedure for creating the signature. For evidential purposes, the fact that a signature exists is not terribly important. It is more important to be able to verify the signer and to ensure that correct security protocols were implemented in creating the signature. Therefore, the manner of proving a signature depends largely on the type of signature in question. To illustrate, in contrast to simple e-signatures, advanced e-signatures (often referred to as digital signatures) use a combination of a mathematical algorithm and a key system to create a unique digital fingerprint associated with a person or entity. Moreover, digital signatures are supported by PKI, which enables third-party certification authorities to verify the authenticity of the signer. It is therefore logical to assume that a digital signature may be proved by reference to the protocols used to create the signature and the authority verifying its authenticity. However, because the act provides that a signature can be authenticated in any manner, regarding some symbols or procedures this vagueness may allow banks and other service providers to make arguments like those in *Job* and *Rahman* cited above. Stated differently, a bank may simply have to prove

72 Id at 187.
73 See Evidence Act (Nigeria) 2011, secs 93–97.
74 Emphasis added.

that certain security protocols exist without also having to prove that such protocols were, in fact, applied or correctly implemented. It is therefore arguable that the vagueness in the Evidence Act derives from the fact that Nigeria has no digital signature law. Digital signature laws often define different forms of e-signatures and delineate procedures for the creation and verification of the signatures; courts could routinely refer to such laws to determine the type of e-signature at issue, how it is created and who bears the burden of proof, as well as the weight or evidential value to ascribe to the signature.[75]

Security is never "absolute"

Secured payments often depend on authenticating technologies. However, authenticators have different degrees of reliability. PINs, passwords, tokens and access codes that are based on authentication protocols of what a person knows or has are susceptible to criminal attacks and can be forged or stolen by hackers and phishers. Additionally, encryption combined with stronger authentication technologies such as digital signatures is still susceptible to criminal attacks, such as man-in-the-middle, unless PKI is fully deployed to minimize the risks.[76]

In addressing the limits of technical security measures, it is pertinent to discuss biometrics, which are now touted as the "silver bullet" in combating identity-related cybercrime in Nigeria. The CBN introduced the use of biometrics for account holder verification in February 2014. Under the tagged biometric verification number (BVN) initiative, banks are required to register their customers' biometric information, including their fingerprints and facial image. The objective of BVN is to use biometrics for the identification and authentication of account holders across the financial industry, thereby reducing customers' exposure to identity theft and fraud.[77] However, while it is true that, unlike PINs, passwords and tokens, biometrics are permanently linked to a person, it is also correct that biometric characteristics, whether biological or behavioural, carry the risk of false performance. That is, biometrics can generate false positives and false negatives. False negatives deny access to otherwise authentic users, while false positives grant access to fraudulent users or impostors.[78] Fingerprint readers used during the Nigerian general elections sometimes failed to identify authentic voters, highlighting the

75 See, for example, Regulations on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (910/2014/EU), in particular regs 3, 13, 25, 26 and 32.

76 See SG Kanade, D Petrovska-Delacretaz and B Dorizzi *Enhancing Information Security and Privacy by Combining Biometrics with Cryptography* (2012, Morgan and Claypool).

77 See CBN "Letter to all other financial institutions (OFIs): Bank verification number (BVN) enrolment for customers" (ref OFI/DIR/CIR/GEN/17/139, 21 April 2017), available at <https://www.cbn.gov.ng/Out/2017/OFISD/CIRCULARONBVNOFOFIs0001(3).pdf> (last accessed 4 March 2018).

78 AD Meadows "Spoof and vulnerability of biometric systems" in EY Du (ed) *Biometrics from Fiction to Practice* (2013, Pan Stanford Publishing) 188 at 195.

problems associated with false negatives. In e-payment transactions, e-commerce and e-banking, false negatives and false positives may have further implications for financial loss. False negatives may cause payment systems to decline otherwise authentic transactions, while false positives may grant fraudsters access to victims' financial information or even to the databases of organizations.

More crucially, identity databases, particularly those storing biometric information, are prone to identity theft attacks because of the inherent value of the stored information. In the case of BVN, the stakes are even higher, as a compromise to the database of any bank in Nigeria could potentially endanger biometric information stored by all banks in the country. For example, if legitimate user data is replaced with false data or stored biometric templates are deleted to facilitate re-enrolment, the same information will be compromised across all payment institutions and chains because the unique biometric is identical on all systems. This susceptibility suggests the need for another law: a data protection law that would set standards of protection for personal data collected and stored in proprietary databases.[79]

PCIDSS AND MARKET CONSTRAINTS: INFORMATION ASYMMETRY AND EXTERNALITIES

Although industry standard-setting is a rule-making process and has a regulatory effect, the authors maintain that, even if the industry were willing, it would be unable to regulate e-payment systems to prevent cybercrimes such as identity theft and fraud without the coercive force of law. Market economy considerations create inefficiencies that limit the effects of industry's initiatives and discourage its investment in technological solutions.

Market systems and asymmetric information

Information asymmetry exists in markets where information about goods and services is unilaterally known to one party. This may be the seller or the buyer. In any case, markets in which information asymmetry exists are characterized by low quality products and high prices, because products cannot be distinguished by their characteristics. Where, for example, sellers hold exclusive information buyers are deprived of making informed decisions about price and quality. In other words, because information about quality is known only to the sellers, prices fail to signify quality to buyers and sellers of low quality products can sell at prices comparative to those of high quality products. This information deficit has additional consequences. First, it drives

79 This would be a general or omnibus data protection law modelled on EU data protection law. Although detailed discussion of the problems with the EU law is beyond the scope of this article, it is important to note that a proposal to adopt the EU approach does not suggest that a Nigerian law on data protection should replicate the exact provisions of EU law, particularly because of its broad and rather nebulous definition of personal data.

the sellers of high quality products out of the market because they cannot increase the prices of their products because of buyer ignorance regarding quality. The second consequence is the proliferation of poor quality products in the marketplace, which leads to buyers' withdrawal from the market and ultimately market failure.[80] In financial and payment services terms, asymmetric information comes into play when providers of payment services promote or disclose the strong qualities of their products, such as efficiency, while withholding the negative features, such as weak security.[81]

Concerns about information asymmetry are particularly useful in assessing the risk of identity theft in e-payment systems. Since non-cash transactions involve the transfer of personal information from the consumer to the seller, the seller's standard of safeguarding information is material to the customer's evaluation of the risk of the transaction. Where there is laxity, the cost of the product should be reduced to reflect the risk of misuse. That is, less secure products should sell for less, and more secure products should sell for more. However, because information asymmetry exists, this is not the case. Both secure and insecure products and services sell at relative prices. Providers of less secure products and services "free ride" on the market and will not lower their prices because consumers associate high price with high quality, and sellers of more secure products are unable to attract customers desiring such products because of the lack of price differentials. Overall, sellers of better security products operate at a loss, while providers of less secure products are profitable. Nevertheless, because payment systems' integrity and efficiency are public goods[82] (in the sense that the market as a whole suffers the consequences of identity theft), sellers with less security have no incentive to provide better security. In other words, if bad security precipitates data breaches and increased incidence of identity theft, consumers associate losses with the entire market and may therefore migrate from e-payment systems, causing market failure or total collapse.[83]

This discussion can be placed in the context of the Nigerian financial market, which has been described as a market where fraud information is kept top secret.[84] This lack of transparency, which is characteristic of virtually all aspects of banking and financial transactions, includes information about conditions related to the use of financial products, transaction costs, and so on. Recognizing the need to review transparency practices in the financial market, the CBN noted:

---

80 See generally G Akerlof "The market for 'lemons': Quality uncertainty and the market mechanism" (1970) 84/3 *The Quarterly Journal of Economics* 488. See also SL Schreft "Risks of identity theft: Can the market protect the payment system?" (2007) *Fourth Quarterly Federal Reserve Bank of Kansas City Economic Review* 5.

81 Schreft, id at 23.

82 See the definition of public goods, above at note 40.

83 Schreft "Risks of identity theft", above at note 80 at 22–28.

84 NeFF "Annual report 2012", above at note 48.

> "An important component of the review exercise was the development of a minimum disclosure requirement that stipulates the information banks are required to disclose to all customers prior to the consummation of every credit transaction. … The overreaching goal … is to produce a Guide that … will accommodate the freedom of operators to charge competitive prices, while protecting consumers from arbitrary and excess charges."[85]

These observations imply that service charges in the financial industry are seldom reflective of value and may be arbitrary regardless of quality. Banking applications and implementation standards for EMV cards (cards using the global standard for chip-based debit and credit card transactions, developed by Europay, MasterCard and Visa) exemplify how asymmetric information works in e-payment systems. According to Murdoch and Anderson, not only does the security of banking apps vary across platforms and suppliers, but, because most apps are proprietary, their vulnerabilities are known only to service providers. Additionally, while acknowledging the security of the EMV protocol, they argue that the protocol has numerous vulnerabilities, which are the inevitable result of implementation choices. Banks can choose, for example, to issue relatively inexpensive cards that use public key cryptography in the card authentication step or opt for cheaper cards that merely present a certificate signed by the issuing bank. These cheaper cards, which do not use PKI, are easier to clone.[86]

It is possible to argue that consumers may be completely unaware of banks and other payment service providers with lax security systems. Consequently, products, services and charges are not comparatively and competitively priced. The CBN itself recognizes the effects of asymmetric information on the financial market and has concluded that it invariably leads to distrust and market collapse. The CBN has stated that, "customers do not perceive fraud as an issue with a specific bank, but with electronic payments overall, which eventually affects the entire industry and not just the institutions that have been impacted by fraud".[87]

It is important to note that, as information asymmetry is invariably a part of traditional markets, this position is unlikely to change. Organizations expect to protect their brands and withhold adverse information from customers unless they are legally compelled to disclose it. Therefore, it is the role of government to correct transactional imbalances and impose transparency rules through legislation.[88]

---

85 Letter dated 6 July 2012 from CBN to all deposit money banks, ref CFP/DIR/GDL/01/018 (copy on file with the authors).

86 SJ Mudorch and R Anderson "Security protocols and evidence: Where many payment systems fail" (pre-proceeding draft for the Conference on Financial Cryptography and Data Security, Barbados, 3–7 March 2014), available at: <http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf> (last accessed 12 February 2018).

87 CBN "About Nigerian Electronic Fraud Forum", available at: <http://www.cenbank.org/neff/about.asp> (last accessed 12 February 2018).

88 See for example, Payment Services Regulations 2009 SI 2009/209 (UK), part 5.

Market systems and negative externalities

Externalities operate to confer costs or benefits on entities other than those who should bear them. They can be positive or negative. Positive factors confer benefits on those who cannot be charged for the benefits, while negative ones confer costs on those who should not bear the cost. In markets where the externalities are negative, entities most often engage in activities that impose costs on others and less often in activities that benefit others.[89] In the context of e-payments, if the risks of weak security, data breaches, identity theft and fraud are borne by individuals, society or other organizations, rather than by the payment service providers, there is less incentive for organizations to provide better security and therefore prevent the proliferation of negative externalities.[90] Two activities in the Nigerian payment industry demonstrate how externalities operate to displace the cost of fraud. First, the liability allocation regime already places the burden of fraud on the consumer or user. Second, through law enforcement, society appears to have assumed the cost of preventing fraud on e-payment platforms, thus providing a further disincentive to the industry.

How unclear rules about liability allocation promote the operation of externalities

The transaction alert system introduced by banks in Nigeria is a good example of how unclear policies promote externalities. Under the system, card or account holders receive alerts or notifications immediately when a transaction occurs on their account or payment card. The effect is to alert the card or account holder instantly to fraudulent transactions and forestall further fraud. Customers who receive notifications of unauthorized transactions are expected to notify the service provider immediately, which then "blocks" the account or card to prevent further use by the fraudster. Invariably, because it allows at least one fraudulent transaction even if it prevents others, the system amounts to "closing the stable door after the horse has bolted." More importantly, bank customers may still be liable for losses that occur before the transaction alert, as, even if a transaction is fraudulent, it is not certain that the customer will be reimbursed or indemnified for the loss, and the bank does not guarantee that it will even investigate the loss.

This practice is correct since the regulatory framework allows parties the flexibility to determine where fraud liability falls. Under e-banking guidelines, "agreements reached between providers and users of e-banking products and services should clearly state the responsibilities and liabilities of all parties involved in the transactions".[91] However, the guidelines fail to provide any meaningful guidance on the allocation of liability and offer little, if any,

89 See R Cornes and T Sandler *The Theory of Externalities, Public Goods and Club Goods* (2nd ed, 1996, Cambridge University Press) at 39.

90 Schreft "Risks of identity theft", above at note 80 at 5.

91 CBN Guidelines on Electronic Banking 2003, item 3.0(g).

protection for users of electronic banking and payment systems. It is arguable, for example, that, while contracts constitute important evidence of an agreement between parties, contracts envisaged by the guidelines will usually be standard form contracts containing extensive exemption of liability clauses. Information asymmetry suggests that the parties' respective bargaining powers are likely to be unequal because of the superior knowledge of service providers about product functionalities and security defects. Ultimately, however, if consumers bear their own losses, providers of e-payment services such as banks can externalize the cost of fraud.

Perhaps in recognition of the inefficiency (and even unfairness) of the existing liability allocation structure, the CBN proposed a card arbitration framework called the E-payment Dispute Arbitration Framework. The objectives of the framework include providing speedy redress for e-payment disputes without involving the courts. The framework is also intended to facilitate the identification of the entity at fault in disputed claims and shift liability toward that entity.[92] Again however, apart from the fact that the framework has yet to become operable, some of its provisions already suggest that it would be equally problematic and is unlikely to have much effect on the status quo. For example, item 5(d) of the framework provides that, "*where a Cardholder uses an EMV Payment Card on an EMV Terminal and fraud occurs, liability is on the Cardholder*. However, it is the responsibility of the issuer to prove to the arbitration panel that the Payment Card issued was the Payment Card used and the Payment Card was not reported stolen" (emphasis added).

Based on their literal construction, these provisions already carry a presumption that the cardholder is liable, without requiring the production of evidence regarding the security of the service provider's systems. Contrary to the arguments demonstrating that EMV cards can be compromised, especially when issuers influence the security design, the provisions appear to suggest that the cards are completely impregnable. Some provisions of the UK's Payment Services Regulations help to highlight the point here. Regulation 60(3) provides that, "[w]here a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that - (a) the payment transaction was authorised by the payer; or (b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 57."

Regulation 57 addresses the obligations of the payer / user to provide notification to the service provider of theft, misappropriation or unauthorized use of the payment instrument in the agreed manner without undue delay after becoming aware of the fact.[93] The cumulative effect of regulations 57(2) and 60

92 CBN "E-payment dispute arbitration framework" (proposed, 2013), item 3, available at: <https://www.cbn.gov.ng/out/2013/ccd/e-payment%20dispute%20arbitration%20framework.pdf> (last accessed 12 February 2018).

93 Payment Services Regs, above at note 88, regs 60(3) and 57(2).

(3) is to displace the presumption of negligence and collusion, which often follows a consumer's allegation of the unauthorized use of a payment instrument. The payment service provider is required to provide strict proof, even when it appears that the actual payment instrument issued has been used to authorize a disputed transaction.

Unlike the proposed card arbitration framework, the Payment Services Regulations place the burden of proving a disputed payment on the service provider and negate presumptions of negligence and fraud on the part of the user.[94] Therefore, since it merely promotes the presumption of negligence or collusion on the part of the cardholder, Nigeria's proposed card arbitration framework may produce results similar to those in *Job* and *Rahman*. As Mason rightly contends, any resulting decisions would be "incorrect decisions based on a misunderstanding of the burden of proof, a failure to properly test the evidence, and an acceptance of unwarranted assumptions".[95]

Society's assumption of the cost of fraud as an externality

An example of how society bears the cost of fraud in Nigeria is evident from the efforts of law enforcement agents aimed at combating cybercrime. Although Nigeria only recently passed a cybercrime law,[96] law enforcement agents already appear to have developed a typology of cybercriminals. The typology characterizes cybercriminals as male, between the ages of 18 and 33, typically well-educated (in the Nigerian context this means the person has been educated up to university level), unemployed and technology savvy.[97] To confirm their classification in any of the categories, suspected cybercriminals will also usually possess laptop computers or smartphones with the ability to connect to the internet almost 24 hours a day.[98] Such "suspects" may be classified as "Yahoo! Yahoo! Boys" (named after the search engine Yahoo!), or "419ners" (named after the section of the Nigerian criminal code that criminalizes impersonation). They may also be classified as engaged in a new form of electronic payment fraud called "cashless Lagos" in mimicry of the CBN's cashless policy. Classifying a person as a cybercriminal is often accompanied by indiscriminate searches of them or of their properties or premises.

Although indiscriminate searches clearly infringe on certain fundamental human rights,[99] the more pressing question is how law enforcement activities

94 Id, regs 60(1)–(3).

95 S Mason "Electronic banking and how courts approach the evidence" (2013) 29/2 *Computer Law and Security Review* 144 at 144.

96 See Cybercrimes (Prohibition, Prevention etc) Act 2015.

97 This prototype was given to the authors by law enforcement agents and forms part of the data used by one of the authors in broader research into the challenges of implementing cybersecurity in Nigeria.

98 Ibid.

99 For example, rights to privacy and to freedom from discrimination, harassment and intimidation are guaranteed under the Constitution of the Federal Republic of Nigeria 1999 (as amended), chap IV, sec 28(1)(a)–(h).

operate to externalize the cost of fraud. On the one hand, such activity is wasteful if not futile, because, before 2015, Nigeria had no cybercrime law under which "suspects" could be prosecuted and convicted. Yet society pays for the time and resources expended in conducting searches and investigating arguably non-prosecutable crimes. On the other hand, because the activities raise the presumption that cybercrime is being controlled, whether deliberately or inadvertently, service providers may fail to consider all the costs and benefits of their actions or inactions for other parties. In other words, providers may under-invest in security on the basis that cybercrime is being addressed or that its challenges are only marginal. To ensure that service providers continue to invest in up-to-date security, the law must set minimum security standards below which providers must not fall.

PRIVATE ORDERING AND THE INDEX FOR STRONG REGULATION

This article has argued that private ordering must meet the index of strong regulation identified as legitimacy, accountability, due process, expertise and efficiency. The establishment of the Nigerian Electronic Fraud Forum (NeFF) is a telling illustration of the inefficiency of a legislative mandate. NeFF is an all-stakeholder fraud forum established to monitor electronic fraud and encourage fraud reporting, information dissemination and information sharing among stakeholders. As stated in NeFF's annual returns, the forum was born out of the need for "a holistic approach to combat the menace of fraud and restore confidence in all e-payment mechanisms in the country".[100] The rationale for establishing the body includes recognizing that electronic fraud attempts will increase significantly as Nigeria migrates to electronic payments, and the fact that the incidence of e-fraud is negatively impacting the entire financial industry. NeFF is mandated to form cohesive and effective fraud risk management practices through information and knowledge sharing with key industry stakeholders. NeFF, in conjunction with the CBN and Nigeria Interbank Settlement Systems, has also developed a dedicated portal for fraud reporting in the e-payment industry.[101] NeFF's establishment is therefore based on the overall assumption that cybercrime control will be more effective if payment institutions share fraud information and articulate a common requirement to law enforcement agents.[102]

However, while NeFF is innovative in promoting collaboration, some of its objectives underscore existing inefficiencies and overall failures on the part of financial regulators. First, the fact that NeFF is projected as an alternative forum for fraud reporting is indicative of the failure of primary fraud reporting systems. It therefore impairs the regulators' execution of their regulatory

100 NeFF "Annual report 2012", above at note 48.

101 See CBN "Submission of fraud report on e-channels using a common portal for the payment industry" (CBN circular BPS/DIR/CIR/GEN/02/103, 2 July 2013).

102 See generally CBN "About Nigerian Electronic Fraud Forum", above at note 87.

mandate and amounts to a reinvention of the wheel. Secondly, and consequential to the first reason, NeFF's effectiveness is questionable because it is likely to be perceived merely as a regulatory watchdog. For instance, if organizations will not report fraud to the CBN as a regulator, why would they exchange fraud information with NeFF, which is an initiative of the CBN and a convergence of competitors, regulators and law enforcement? In essence, it is reasonable to expect that fraud information disclosed at the forum will eventually be passed to regulators, with possible regulatory reprisals. This would inhibit the free dissemination of fraud information, which is NeFF's primary objective. From this perspective, NeFF may invariably represent a classic example of the failure of a legislative mandate. That is, NeFF is indicative of the failure of the CBN's legislative mandate to protect e-payment systems.

Furthermore, although regulatory guidelines provide that there must be a regular and ongoing assessment of compliance with PCIDSS, there are no fully functional monitoring processes in place in Nigeria. For example, the e-banking guidelines provide that "each vendor must provide valid certificates showing compliance with these standards, and must regularly review the status of all its terminals to ensure they are still compliant as standards change. [And] there will be a continuous review and recertification on compliance with these and other global industry standards from time to time".[103] In contrast to this requirement, organizations are only subject to an initial inspection to determine whether they meet the compliance threshold (for which they receive a certificate). Thereafter, there is no framework to ensure that organizational practices are upgraded.[104] This invariably promotes the argument that existing private ordering lacks accountability and fails to comply with due process, and that PCIDSS itself is largely ineffective.[105]

It therefore appears that, applying the index of measuring strong regulation, industry expertise will be the only strength of regulation by the e-payment industry in Nigeria. However, it has been previously argued that industry can manipulate its technological expertise to serve its own purposes. As such, industry may need to be regulated even in terms of how it applies this expertise. The concluding section of this article charts the way forward. The analysis justifies the interplay between different regulatory mechanisms and explicates the overall role of law in the regulatory schema.

---

103 POS Guidelines, item 3.1.

104 For example, statistics are disputed regarding PCIDSS compliance levels. As at 2011, only two of the potential target organizations were reported to be PCIDSS compliant. Contested reports also put the level of compliance at 2% in 2012 and up to 50% in 2013, although there are no reports on ongoing compliance checks or the present state of PCIDSS compliance in Nigeria.

105 Morse and Raval "PCI DSS", above at note 62 at 551.

HOW LAW REGULATES: LESSIG'S MODALITIES OF REGULATION IN CYBERSPACE AND THE REGULATION OF E-PAYMENTS

Perhaps because there is much debate about the regulation of the internet itself, governments have been sceptical about the best approach to regulate the activities it mediates or facilitates. For example, it has been argued that, to facilitate internet growth and ensure the protection of fundamental rights, government intervention and formal rules are both unwarranted and unwanted.[106] However, it has also been argued that an unfettered internet is not an automatic guarantor of human rights and there is a need to regulate self-evolving rules and the institutions that administer them.[107] Although the latter argument is correct in that it justifies the need for law, much of the argument in this area fails to identify how the law would operate in the complex cyberspace environment.[108] Lessig addresses this gap by proposing that legal and policy solutions to the regulatory dilemma in cyberspace are found in the interplay between different regulatory modalities.

Lessig identifies four modalities of regulation, or "things that regulate".[109] These are law, architecture, norms and the market. These modalities, as constraints to behaviour in real space, are transposable to cyberspace. According to Lessig, law constrains objectively because it provides a set of commands and threatens punishment for disobedience. As in real space, the constraints of law in cyberspace include the threat of sanctions for violations of certain rights or punishment for certain behaviours.[110] Social norms also limit, although in a manner that differs from legal constraints. The theory is that members of a community impose normative constraints through slight and sometimes forceful sanctions rather than centralized action of the state.[111] As the third modality of regulation, the market constrains through differential pricing. This is based on the fact that prices signal the point at which a resource can be transferred from one person to another.[112] The fourth, and perhaps most important modality of regulation, is the architecture of an environment, which encompasses the way things are or the way they are made or built.[113] In the context of regulation, architecture can either enable or limit interaction with the environment but, unlike the other three

106 See for example DR Johnson and D Post "Law and borders: The rise of law in cyberspace" (1996) 48 *Stanford Law Review* 1367; see also JP Barlow "A declaration of the independence of cyberspace", available at: <https://projects.eff.org/~barlow/Declaration-Final.html> (last accessed 12 February 2018).

107 See for example, JL Goldsmith "Against cyberanarchy" (1998) 65/4 *The University of Chicago Law Review* 1199; see also T Wu "Cyberspace sovereignty? The internet and the international system" (1997) 10/3 *Harvard Journal of Law and Technology* 647.

108 Goldsmith, id at 1201.

109 Lessig *Code Version 2.0*, above at note 65.

110 Id at 123–25.

111 Id at 340–41.

112 Ibid.

113 Id at 342.

constraining modalities, architecture is independent of direct human imposition and is often automatically deployed or self-executing.[114] Therefore, code constrains without subjectivity and operates regardless of whether the party being constrained is aware of it.[115] To this extent, code has regulatory potential analogous to regulation by law and, indirectly or metaphorically, "code is law".[116] However, as an overriding regulatory modality, law can modify, alter or enforce the code of cyberspace in a way that promotes the demands of commerce, society, policy and justice.[117]

Lessig's theory compels the inference that, although individually the modalities of norms, market and technology do work, whether they are effective depends on the extent to which they are regulated by law. For example, as the "most obvious self-conscious agent of regulation",[118] law will affect the other modalities in a manner that aids their roles as tools for legal regulation.[119] The following analysis reformulates and synthesizes Lessig's four modalities to propose a workable regulatory agenda for e-payment systems and underline the primary role of formal rules.

Regulating with law, industry, technology and users

Based on the analysis, it is arguable that only two of the modalities (technology and market) are currently represented in the regulatory arrangement for e-payment systems.[120] However, this article has argued that technology (or code) can be manipulated, and market systems are self-serving in the sense that they allow industry (or the market) to pursue its own goals and therefore promote the primacy of sector interests.[121] The article has also suggested that the public interests at stake include the prevention of crimes and correction of market failures, as well as certainty and transparency in the administration of justice. Thus, the authors propose to include two additional modalities of law and "users" in the regulatory framework.

Users are proposed as the fourth modality, not only because the lines of social norms are often ill-defined but also because it is difficult to develop an agenda for an enforceable norm. For example, Lessig's proposal of regulation by norms would beg the question of how generally acceptable norms will develop in the first place. This is particularly so as the cultural specificity of norms and the relativity of individual choice, as well as the fluidity and mobility of the internet, negate the permanence of engagements needed to sustain

114 Ibid.
115 Id at 341.
116 Id at 5.
117 L Lessig "The law of the horse: What cyberlaw might teach" (1999) 113/2 *Harvard Law Review* 501 at 514.
118 Id at 511.
119 Id at 502.
120 See previous arguments at notes 9–18 above.
121 The use of the terms "technology" and "industry" is for consistency as they essentially align with Lessig's concept of code and market.

the development of generally acceptable norms. The idea of a global norm would therefore often be unattractive, as billions of people using the internet would not agree on regulatory norms.[122] Notably, beyond proposing that "norms could be used to respond to [the] threats … [and] Norms - among commercial entities, for example - may help build trust around certain privacy-protective practices",[123] even Lessig was unable to provide clues as to how such normative frameworks would develop.[124] Rather, he concedes that, "how people who need never meet can establish and enforce a rich set of social norms is a question that will push the theories of social norm development far".[125] Furthermore, because the effectiveness of norms depends largely on voluntary compliance, norms are analogous to the private ordering system and give rise to the same problems. Therefore, it would be correct to assert that the threat of enforcement is still necessary to cause people to conform to norms, and state enforcement is more certain and more secure than private efforts to coerce behaviour because the state can utilize its monopoly on the official use of force.[126]

As an alternative to the contested notion of a collective norm, "users" is a more specific term, which underscores the fact that the problem surrounds a group of people more likely to make individual rather than collective decisions. In the context of e-payment systems, it addresses the ability or inability of respective users to articulate their choices in view of the payment instruments, processes and providers they select. Additionally, because of their susceptibilities to social engineering, users are invariably part of the problem. Humans, unlike technology, can demonstrate extreme levels of variation in skill and do not always follow logical rules in conduct. They can be emotional actors, inevitably partial, driven by perception and emotion as much as by objective reality.[127] Indeed, users are considered the weakest link in the security chain. The Verizon data breach report noted that humans are the "the carbon layer" of information assets and are therefore notoriously susceptible to social tactics, including deception, manipulation and intimidation. Therefore, as the report concludes, while humans are the most complex creatures on earth, savvy threat agents or criminals have consistently outwitted

122 J Goldsmith and T Wu *Who Controls the Internet? Illusions of a Borderless World* (2006, Oxford University Press) at 152.

123 Lessig *Code Version 2.0*, above at note 65 at 223.

124 Id "The zones of cyberspace" (1996) 48/5 *Stanford Law Review* 1403 at 1407.

125 Ibid.

126 See RD Cooter "Law from order" in J Mancur Olson and S Kahkoneh (eds) *A Not-So-Dismal Science: Broader Brighter Approach to Economies and Societies*, cited in JR Macey "Public and private ordering and the production of legitimate and illegitimate rules" (1997) 82/5 *Cornell Law Review* 1123 at 1133.

127 AM Matwyshyn (ed) *Harbouring Data: Information Security, Law, and the Corporation* (2009, Stanford University Press) at 229.

them or otherwise leveraged them to steal data.[128] Since users are invariably part of the problem, the authors propose to make them part of the solution. Murray's observations that users are not to be considered passive recipients of regulatory initiatives support this point.[129] Again however, like technology and the market, users only operate effectively if the law intervenes and sets certain standards.

Scepticism regarding the ability of users to protect themselves ranges from the complexity of technical security to ignorance or lack of awareness. To illustrate, while certificate-based authentication may help users to verify an entity by linking its public and private keys, it is debatable whether lay users can understand why the authentication protocol is necessary or what to look for, such as the security padlock, or even how to check certificates. In Nigeria, three further reasons account for why users cannot regulate themselves or prevent cybercrime. The first is the proliferation of pirated and unlicensed software. In 2011, a global piracy study put the rate of PC software piracy in Nigeria at 82 per cent, which is almost twice the global piracy rate. The same report put the rate of unlicensed software installations at 81 per cent in 2013.[130] Since the links between cyber-security and pirated software are well documented, it is safe to assume that, if the Nigerian market is saturated with pirated software, most end-user products, including anti-virus programmes, will also be defective and unreliable. The second reason that casts doubts on users' ability to regulate without laws is the volatile threat landscape for e-payments. In other words, cybercrime remains a challenge because the threat landscape is evolving, and it is unlikely that providers and users can keep up with criminal tactics. To illustrate, since mobile devices are increasingly used for banking and payments, criminals are bound to migrate from computers and e-mails to mobile platforms to leverage attacks. In this event, user education serves a limited purpose and may have no effect at all on the rate of victimization.

The third, perhaps most important, reason is that technology is now being developed in Nigeria to address user volatility and unpredictability in the regulatory environment. Therefore, users are more likely to be regulated by technologies embedded into payment processes, services and instruments, rather than their own choices. This approach is not particularly complex, but is controversial. Some technologies described as having lock-in effects exemplify the potential problems. Lock-in technologies modify or alter the behaviour of actors in ways that ensure compliance with law or regulation

128 Verizon "2012 Data breach investigation report" at 33, available at: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf> (last accessed 12 February 2018).

129 AD Murray *The Regulation of Cyberspace Control in the Online Environment* (2007, Routledge Cavendish) at 51.

130 See BSA "The compliance gap: BSA global software survey, June 2014", available at: <http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf> (last accessed 12 February 2018).

or with industry standards for protecting privacy and security. Built-in security processes embedded in privacy by design and privacy-enhancing technologies serve as good examples. Privacy by design processes embed privacy features into design specification, implementation and networked infrastructures from the outset. This entails built-in privacy requirements from the onset of a system's development and throughout its life cycle.[131]

Consistent with this approach, and with the notion that technology is self-executing when it comes to constraining human behaviour, the CBN introduced the BVN into the Nigerian banking industry. This article has already discussed the features of the BVN and the implications for regulating users are significant. Although it is not entirely clear how the BVN will work, the presumption is that enrolment of individual biometrics would ensure that users are unable to access their accounts unless they are physically present at the point of sale. The BVN system therefore has the potential to create a lock-in effect, by employing technology to bypass certain user behaviours, such as the ability to share one's PIN with other people. However, precisely because of their capacity to compel obedience, "lock-in technologies" are controversial. They raise questions about legitimacy, choice and legal regulation that are fundamental to the user's role in regulation and fraud prevention in e-payment systems.

Beyond private ordering: Legitimacy, accountability and due process

Lock-in technologies, also referred to as "techno-regulation",[132] are defined as the deliberate employment of technology to regulate human behaviour.[133] Jaap-Koops characterizes them more aptly as "technology with intentionally built-in mechanisms to influence people's behaviour".[134] Perhaps significantly in his analysis of techno-regulation, Brownsword argues that there are moral and ethical implications of design-based technologies aimed at controlling harm-generating behaviour and technologies when they function in ways that override human choice, free will and dignity. Such a view allows for little controversy when arguing that human dignity implies that people should be able to choose not only right actions, but also wrong ones. Accordingly, because design-based technologies impose behavioural constraints on their

131 A Cavoukian "Privacy by design: The 7 foundational principles: Implementation and mapping of fair information practices" (2011), available at: <https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> (last accessed 12 February 2018).

132 See R Brownsword "Code, control, and choice: Why east is east and west is west" (2005) 25/1 *Legal Studies* 1 at 3–21.

133 R Leenes "Framing techno-regulation: An exploration of state and non-state regulation by technology" (series no 10/2012 Tilburg Law School Legal Studies Research Paper 149).

134 B Jaap-Koops "Criteria for normative technology: The acceptability of 'code as law' in the light of democratic and constitutional values" in R Brownsword and K Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (2008, Hart) 157 at 158.

subjects, they deprive those subjects of the opportunity to choose between right and wrong.[135]

Although a distinction may be made between design-based technologies that operate directly on individuals' decision-making processes and those that seek to restrict the exercise of individual judgment without overriding that judgment altogether, there are legitimate concerns that the technologies may generally jeopardize constitutional values. For example, they may limit the opportunity to appeal to the discretion and judgment of enforcement officials against the inappropriate or unfair application of regulatory standards.[136] Certainly, design-based technologies raise these concerns even when they are incorporated to enforce legal norms. Jaap-Koops indicated that, if technology's only use is to enforce prevailing legal norms, its acceptability should be called into question, since the transformation of "ought" or "ought not" to "can" or "cannot" threatens our human interpretation of norms that represent bedrock elements of law in practice.[137]

These arguments would be correct to the extent that they identify the corrosive effects of design-based technologies on legitimacy and accountability. However, if the arguments tend to suggest that lock-in technologies reduce users to robotic recipients of industry's inventions, they would be incorrect. To support this point, it is important to note that progressive technological modifications have been used to respond to user problems in payment systems. As an example, by design, mere possession authenticated the use of credit cards, but this also created an incentive to steal the card, as any holder could use it. To correct this, subsequent ATM cards were designed with a required PIN. This means that the user must not only have the card but must also know the PIN. There is less incentive to steal this card unless the thief has access to the PIN. However, the technology also proved susceptible because users wrote PINs on their cards or kept them with the cards. To increase confidence further that the holder of the card is the authorized user, biometric technologies such as fingerprints and retinal scans were introduced. Technology is also now being advanced to integrate behavioural biometrics, including typing speed, touch pad dwell time, key selection and angle of mouse movements into mobile devices and web applications to build further confidence in authentication processes.

To summarize, the application of behaviour-modifying technology is neither new nor novel. Such technologies have evolved progressively, particularly in response to the criminal exploitation of payment instruments and user-associated problems. This position is correct even if regulatory motivations are unclear or when regulatory intentions are not clearly spelt out. It would be sensible to argue that the nature of complex regulatory environments

135 Brownsword "Code, control, and choice", above at note 132 at 15–17.

136 K Yeung "Towards an understanding of regulation by design" in Brownsword and Yeung (eds) *Regulating Technologies*, above at note 134 at 79–107.

137 Jaap-Koops "Criteria for normative technology", above at note 134 at 159.

often means that regulation has varying degrees of transparency. Whether noticeable or not, regulation is justified by the need to protect the regulated entity and others.[138] Therefore, one may view technologies that lock in or restrict user choices and preferences as a means of protecting users even from themselves, while at the same time achieving the interests of government and industry in regulating behaviour. In effect, enrolling user biometrics for account authentication, as in the case of the BVN, will not in and of itself be illegitimate. However, to ensure the effectiveness of users in the regulatory framework, the law must also ensure that providers are transparent and accountable.

As examples, while it would be quite arbitrary for the law to impose limitations on how consumers transfer their personal information, the law can set fundamental standards of behaviour sought to be locked in. Therefore, the law could define what constitutes personal information in order to identify the information that providers are obliged to protect. Additionally, legal requirements that the most effective or up-to-date technical safeguard be used may form the basis for integrating biometric technologies into payment instruments and processes, and for securing access to the biometric databases. Without such laws, the risk of fraud arising from data breaches or organizational misuse of data corresponds to the benefits provided by the lock-in technologies. In other words, consumers of the services could be locked into a false sense of security if criminals gain access to identity databases. Arguably, in such circumstances, criminals would have less need of the information that technology protects.

Furthermore, laws would be needed to set out evidential requirements to establish that correct security protocols have been implemented into payment instruments or processes that have lock-in effects. *Job* and *Rahman* highlight the need for transparent rules on evidence when security protocols are in question. The proposed Nigerian electronic identity card mentioned above also clarifies the point here. It was noted that the identity card would be embedded with payment functionalities. Conversely, one of the proposed security features of the card is the deployment of firewall technology to separate and protect the financial information on the card.[139] It is therefore possible to argue that, unless the protocols used to implement such a separation are ascertainable and verifiable, allegations of unauthorized access may be difficult to resolve.

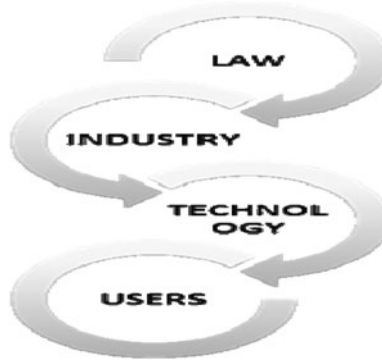
Based on this analysis, the security for e-payments depicted in Figure 1 below shows how regulation should be framed to enable the law to affect each modality within the regulatory schema.

---

138 AD Murray *The Regulation of Cyberspace Control in the Online Environment* (2007, Routledge Cavendish) at 23.

139 See NIMC "Facts about the national electronic (e-ID) card", available at: <https://www.nimc.gov.ng/facts-about-the-national-electronic-identity-e-id-card/> (last accessed 12 February 2018).

Figure 1. E-payment regulation based on the theory of modalities of control.



As shown in Figure 1, the law is at the apex of the regulatory schema. Industry follows because it can readily modify technology. Therefore, direct regulation of industry by the law would promote the development of high technical standards for security. Having derived its legitimacy from legal rules, technology can be used to constrain user behaviour. To cite a few of many possible examples, data protection law may provide that organizations use the most up-to-date, if not state-of-the-art, technology to protect personal information. Additionally, laws regulating electronic payment services may impose liability on providers in certain circumstances where authentication or authorization is contested. Digital signature laws may allocate evidential value to electronic signatures and identity management laws would ensure that all organizations, irrespective of sector, implement strong identity management standards.

There are two reasons why the regulatory modalities must operate in the order proposed above. First, the order is important to address the peculiar nature of technology and cyberspace and the inability of the law to affect users and technology directly as modalities of regulation. For example, the law has no direct impact on user behaviour, but technology does. Although technology standards may be translated into legal rules, laws cannot directly regulate technology because technology is evolving, and the volatility of technology means that security mechanisms quickly become elementary and outdated. However, since industry can readily modify technology, direct regulation of industry by legislation would promote the development of high technical standards for data security. The order therefore allows the development of specific rules that may be modified as technology evolves. Secondly, the order ensures that, in any case, the rule-making process starts with explicit efforts by the state rather than industry. Thus, while not effectively displacing private ordering such as PCIDSS, it does not also require the codification of the standards to achieve desirable security standards. In effect, while involving the state in the regulatory arrangement, the regulatory framework dispenses with the assumption that industry will ultimately write the same rules as the regulator; rather, it promotes legal standards in favour of

considerable discretion of the target over internal systems. This point distinguishes the proposed framework in this article from intermediate regulation such as meta-regulation. Meta-regulation, also often referred to as "mandated self-regulation" or "enforced self-regulation", involves efforts by governmental authorities to promote and oversee self-regulation. As demonstrated in this article, the public interests at stake undermine an assumption that industry will develop rules congruent to the state. Therefore, the main problem with meta-regulation, also demonstrated in the analysis of PCIDSS, is that, even if businesses have better information to find solutions to public interest problems, they do not necessarily have better incentives to do so.[140] The authors also argue that discretion is undermined by the industry's inability (regardless of willingness) to protect public goods or develop legal principles relating to standards of proof, fairness and transparency.

CONCLUSION

The question of whether regulation is legitimate or effective must be answered in the context of the principal characteristics of good regulation and how it meets public interest requirements underpinning regulatory activities. This article has argued that, although non-state actors now function as regulatory agents for e-payment systems, their effectiveness is limited because e-payment represents a heterogeneous market. Therefore, unless banking rules requiring compliance with industry private ordering are generally accepted and recognized, private ordering in e-payments may grapple with questions of legitimacy. Furthermore, because market constraints (such as information asymmetry and externalities) can undermine even the most effective self-regulatory regimes, it is necessary for the law to intervene in the regulatory process. The analysis of technical standards for security highlights the fact that, given the self-executing nature of technology (or code) and the industry's expertise in developing and implementing technical standards, technology could be quite effective as a regulatory mechanism. However, the effectiveness of technical standards is also limited because the standards themselves may not apply across the broad spectrum of e-payment services. What becomes clearer from a consideration of Lessig's theory of modalities of control in cyberspace are the perils of technology-based solutions. While conceding that technology plays a fundamental role in regulating activities online and admitting that "code is law", Lessig underlines the malleability of technology to abuses and underscores the need for legal regulation of technology and the industry that produces the technology.

Therefore, because the industry has the tendency to manipulate technology and abusive use can distort perceptions of fairness and justice, laws must be developed not only to set general standards of technical security but also to

140 See C Coglianese and E Mendelson "Meta-regulation and self-regulation" (Penn Law School public law and legal theory research paper no 12–11) at 16.

build accountability, due process and even legitimacy into the regulatory process. As the article further suggests, preventing crime and correcting market failures as well as building trust and confidence in electronic transactions through transparent rules and the fair adjudication of contentious cases are public policy issues that override private ordering in e-payment systems. The government must intervene with rules, setting liability standards so that industry does not use technology either to displace the burden of proof or to avoid liability altogether. Because market efficiency is a public good, formal laws are required to correct market failures and displace externalities as broader public interest concerns, which are not necessarily the focus of private ordering systems. This article has demonstrated that legal regulation is justified, not only because the law is the most obvious self-conscious agent of regulation, but also because it infuses accountability, due process and legitimacy, as well as efficiency, into the regulatory process.

Significantly, the analyses and findings in this article suggest that the proposed regulatory framework has a wider application beyond Nigeria. For example, Kenya with its widespread adoption of M-pesa,[141] Ghana and Tanzania, which are currently developing electronic means of payment, and South Africa, which has the most developed e-payment systems on the African continent, all share similarities in demographics, security and regulatory challenges. These countries all have an increasing population migrating to e-payments with the subsequent global threat posed by cybercrime. They also have similar regulatory systems based largely on narrow finance industry-driven initiatives. The proposals in this article could therefore be applied to e-payment processes, instruments and institutions in other countries facing similar challenges. For regulatory arrangements more generally, the authors suggest that, while private ordering is not inherently inefficient, its efficiency must be examined in the context of respective activities subject to regulation. Also, when intervening in the regulation of a largely heterogeneous activity, the government needs to develop uniform rules in the form of general principles rather than specific rules. In the technology environment such principles must address the malleable and evolving nature of technology and the unpredictability of the regulatory environment.

141 See above at note 3.