United Nations A/CN.9/728

General Assembly

Distr.: General
21 March 2011

Original: English

United Nations Commission on International Trade Law
Forty-fourth session
Vienna, 27 June-15 July 2011

Present and possible future work on electronic commerce

Note by the Secretariat

Contents

		Paragraphs	*Page*
I.	Introduction	1-5	2
II.	Report on the colloquium on present and possible future work on electronic commerce	6-67	3
	A. Identity management	9-28	3
	B. Use of mobile devices in electronic commerce	29-67	7

V.11-81441 (E) 230311 240311

I. Introduction

1. At its fortieth session, in 2007, the Commission requested the Secretariat to continue to follow closely legal developments in the area of electronic commerce, with a view to making appropriate suggestions in due course.[1]

2. At its forty-first session, in 2008, the Commission requested the Secretariat to engage actively, in cooperation with the World Customs Organization (WCO) and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), and with the involvement of experts, in the study of the legal aspects involved in implementing a cross-border single window facility with a view to formulating a comprehensive international reference document on the legal aspects of creating and managing a single window, and to report to the Commission on the progress of that work.[2] That request was reiterated by the Commission at its forty-second session, in 2009,[3] and again at its forty-third session, in 2010.[4]

3. Furthermore, at its forty-second session, in 2009, the Commission requested the Secretariat to prepare studies on electronic transferable records also in light of the written proposals received at that session (documents A/CN.9/681 and Add.1 and A/CN.9/682), with a view to reconsidering those matters at a future session.[5]

4. In furtherance of that request, a document on current and possible future work on electronic commerce (A/CN.9/692) was submitted to the consideration of the Commission at its forty-third session, in 2010. At that session, the Commission requested the Secretariat to organize a colloquium on the topics discussed in document A/CN.9/692, namely electronic transferable records, identity management and electronic commerce conducted with mobile devices, and to prepare a note summarizing the discussions at that colloquium and possibly identifying a road map for future work by the Commission in the area of electronic commerce.[6] It was agreed that that note should provide sufficient information for the Commission to make an informed decision and to give a clearly defined mandate to a working group, if deemed appropriate.[7]

5. In line with that request, the present note reports on the colloquium on possible future work of UNCITRAL in the field of electronic commerce, held in New York on 14-16 February 2011.[8]

---

[1] *Official Records of the General Assembly, Sixty-second Session, Supplement No. 17* (A/62/17), part I, para. 195.

[2] Ibid., *Sixty-third Session, Supplement No. 17* (A/63/17), paras. 333-338.

[3] Ibid., *Sixty-fourth Session, Supplement No. 17* (A/64/17), para. 340.

[4] Ibid., *Sixty-fifth Session, Supplement No. 17* (A/65/17), para. 244.

[5] Ibid., *Sixty-fourth Session, Supplement No. 17* (A/64/17), para. 343.

[6] Ibid., *Sixty-fifth Session, Supplement No. 17* (A/65/17), para. 250.

[7] Ibid.

[8] The preparatory documents of the colloquium are available in the form they were submitted by the speakers from the UNCITRAL website: www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010program.html.

II. Report on the colloquium on present and possible future work on electronic commerce

6. As an introduction to the colloquium, reference was made to past work of UNCITRAL in the field of electronic commerce. It was indicated that, while the Working Group on Electronic Commerce had not met since the finalization of its work on the United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 (the "Electronic Communications Convention"),[9] work in the field had continued regularly. That work included the preparation of the publication "Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods",[10] coordination of work with other organizations, and the promotion of the adoption and uniform interpretation of UNCITRAL texts in the field.

7. It was added that several legislative provisions relating to the use of electronic communications had been discussed in recent years by UNCITRAL Working Groups dealing with arbitration, maritime transport and public procurement, inter alia.

8. It was said that over the years UNCITRAL had become a leading international body and main repository of international expertise on legal issues relating to electronic commerce. However, rapid technological progress and developments in business practice occurred in the last few years had given rise to new legal challenges that needed to be addressed. It was added that, while other bodies could take up those challenges with equal competence, the universal composition of UNCITRAL represented the best guarantee of a balanced and fair approach. It was also suggested that further delay in resuming the work of the Working Group on Electronic Commerce might lead to loss of institutional expertise and, eventually, of its prominence in the field.

A. Identity management (IdM)

9. The colloquium provided an opportunity to discuss recent technical, policy and legal developments relating to identity management, which continued to attract significant interest in several fora. Reference is made also to basic information on the structure and goals of identity management systems that has already been compiled (A/CN.9/692, paras. 48-66).

10. With respect to technical standards, reference was made to the work of Study Group 17 (SG 17) of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). It was explained that business, and especially financial institutions, had expressed a need to create a safe and secure electronic environment for their customers that could be accessed in a simple, seamless and convenient manner. In short, business requested better identity assurance of electronic entities. It was added that better identity assurance could assist in addressing a number of regulatory, operational and contractual risks with

[9] United Nations publication, Sales No. E.07.V.2.
[10] United Nations publication, Sales No. E.09.V.4.

multiple legal aspects including privacy and data protection, fraud prevention and compliance with anti-money-laundering regulations.

11. In this context, the work of SG 17 pursued the standardization of four levels of assurance corresponding to varying degrees of confidence in the asserted identity, with a view to promoting trust, improving interoperability, and facilitating the portability of identity information across organizations and borders. The resulting standard, referred to as "X.eaa" (entity authentication assurance), could be used to define the requirements that an identity service provider had to meet in order to satisfy a given level of assurance. It was further explained that such approach could facilitate the acceptance of third parties as identity providers not only by commercial and non-commercial private entities but also by governmental agencies. It was specified that the standard would be applicable to identification of both human and non-human entities.

12. Potential benefits arising from the adoption of such a standard included the provision of a consistent basis for trust and the possibility to re-use credentials in different contexts. Moreover, this approach could promote efficiency, reduce costs and provide the foundation for the uniform treatment of liability and other legal aspects. It was further explained that the work of SG 17 built on previous and ongoing similar initiatives promoted by governments and the private sector.

13. In conclusion, it was stated that better identity assurance was of fundamental importance to establish trust in electronic transactions and to fight cybercrime. It was added that better understanding of policy and legal matters at the national and international levels was necessary in order to improve identity assurance. In this respect, future work of UNCITRAL aiming at identifying legal issues in the field, for instance, of parties' liability, privacy and cross-border enforcement, would be particularly welcome.

14. From the policy perspective, it was recalled that the Organization for Economic Cooperation and Development (OECD) had prepared a first reference document[11] highlighting the benefits associated with adopting an interoperable approach in identity management systems (see also A/CN.9/692, para. 59).

15. It was explained that, building on previous work, OECD had conducted in 2010 a survey of identity management strategies at the national level.[12] A report[13] as well as a document containing the policy messages gathered from data analysis and the lessons learned would be made available to the public later in the year 2011.

16. It was illustrated that three main trends could be identified at the top level of analysis of the results of the survey (defined as a "vision"): most governments set the establishment and development of e-government systems as overarching objectives of national identity management strategy; several governments added to that goal the desire to foster innovation in the broader Internet economy; other

---

[11] OECD Working Party on Information Security and Privacy, *The Role of Digital Identity Management in the Internet Economy: a Primer for Policy Makers*, DSTI/ICCP/REG(2008)10/FINAL (11 June 2009).

[12] The survey did not deal with cross-border aspects of identity management.

[13] OECD, *Report on National Strategies and Policies for Digital Identity Management in OECD Countries*, 2011.

governments indicated as their priority the achievement of a higher level of cybersecurity. However, it was also said that, while the primary focus of each national strategy might vary, reference to each goal was present in all of them.

17. Another relevant difference among country strategies emerging from the survey was the adoption of an "universal approach" to credentials, i.e. an approach that allowed for the cross-use of credentials between private and public sector, as opposed to one that envisaged the extension to the private sector of credentials established for the public sector or, at least, of their framework.

18. Specific benefits for governments, citizens and businesses were expected from the adoption of identity management systems, and included the possibility of introducing new services, especially of higher value, due to enhanced security. Reduction of costs and enhancement in usability, including by reducing the number of credentials and pooling authentication systems (for instance, through single sign-on) were also foreseen, as well as a general increase in productivity and efficiency.

19. It was recalled that an obstacle to the development of more secure electronic environments was often identified in the insufficient number of users willing to pay for the development of such applications that made identity providers reluctant to investing in stronger identity assurance systems. In turn, secure applications using stronger identity assurance systems were not available in a number and at a cost sufficient to raise the interest of users. National identity management strategies aimed at overcoming this stalemate by providing a number of e-government applications sufficient to justify the development and deployment of a trusted national identity management system offering stronger identity assurance.

20. It was indicated that an analysis of existing policies and practices indicated a significant trend towards the migration into the electronic environment of existing off-line identity practices. Country-specific approaches would usually be maintained and influence the choice of strategy. This was, for instance, the case with national systems of registration and identification of persons, whose mandatory nature was reflected in the policy for adoption of credentials.[14] Moreover, it was said that, while varying degrees of centralization could be found, systems tended to be designed in a more "technology-neutral" manner under decentralized approaches, and to be more "technology-prescriptive" in centralized ones.

21. It was added that the retention of country-specific approaches did not favour addressing challenges related to cross-border identity management. On the contrary, it seemed that under that approach issues existing in the traditional world would remain and add to those arising from the adoption of electronic means. It was further mentioned that current experiments in the cross-border field seemed to focus on interoperability.[15]

22. In this respect, it was further indicated that, while migration of services online could offer the possibility to re-engineer and streamline existing processes, thus

---

[14] For a definition of credential, see UNCITRAL, *Promoting confidence in electronic commerce*, cit., p. 69, footnote 189.

[15] For instance, see the Secure idenTity acrOss boRders linKed (STORK) project in the European Union: https://www.eid-stork.eu.

offering additional benefits, that stage had not been reached yet by any participant in the survey.

23. It was explained that challenges posed by identity management systems might be regrouped under three general categories: technological, economic and legal. The discussion on legal topics focused on identity management systems based on a three-party scheme, i.e. featuring a subject, an identity provider and a relying party (see A/CN.9/692, para. 54).[16]

24. The following topics were identified on a preliminary basis as relevant for further legal analysis: contractual performance at the identification and authentication stages; privacy; data protection; liability; enforceability; and regulatory compliance. It was noted that each of the parties involved in identity management systems had different rights and obligations in the various areas.

25. It was stated that the ultimate goal of an identity management system was to provide an identity assurance sufficiently reliable for the intended purpose. While technological measures could play an important role in achieving this goal, the ultimate protection against abuses had to be offered by the law. Thus, it was suggested that a "trust framework" would need to be established to address both the operational requirements, i.e. technical specifications, processes, standards, policies, rules and performance requirements necessary for the functioning of the identity system, and the legal rules necessary to define a trustworthy identity system.

26. It was clarified that the legal rules of the trust framework could have statutory or contractual nature. Contractual agreements could complement statutory rules but could also vary them, where so permitted. It was explained that legal rules were relevant for the trust framework in three ways. First, they made specifications, standards, and rules relating to the various components of the operational requirements legally binding on and enforceable against each party. Secondly, they defined legal rights and responsibilities of the parties, clarified the legal risks assumed by participating in the trust framework (e.g., warranties, liability for losses, risks to personal data) and provided remedies in the event of disputes among the parties, including dispute resolution and enforcement mechanisms, termination rights, and the amount of damages, penalties and other forms of liability. Finally, in some cases, legal rules could also regulate the content of the operational requirements.

27. The relation between identity systems and electronic signatures was also discussed. It was said that a number of services related to electronic signatures, such as timestamping and the guarantee of the integrity of the message, still lacked uniform legal treatment, and that those services were relevant also in the context of identity management. Moreover, fundamental matters, such as electronic signatures of juridical entities, were still under discussion in some jurisdictions. Thus, it was suggested that work on identity management could tackle and solve also those issues relating to electronic signatures.

28. In conclusion, wide consensus was expressed on the relevance of identity management to facilitate cross-border electronic transactions and on the importance

---

[16] In off-line and in simple online system, the subject may issue and verify credentials, thus discharging also the functions of identity provider.

that related legal issues would receive adequate treatment. It was noted that, while work was ongoing at the national level, very few initiatives, if any, dealt with transnational legal aspects of identity management. It was suggested that, due to its mandate, composition and expertise, UNCITRAL would be in an ideal position to work on those legal issues. It was added that such work would also clarify the scope of provisions on legal signatures contained in existing UNCITRAL texts, and would facilitate the treatment of identity management in the context of other topics potentially of interest for UNCITRAL and discussed at the colloquium, namely mobile commerce, electronic transferable records and electronic single windows facilities.

B. Use of mobile devices in electronic commerce

29. The exponential growth of mobile subscription and the increased ubiquity of mobile devices, including mobile telephones, have transformed the information and communication technologies (ICT) landscape and how electronic transactions are conducted around the world. In a recent report,[17] the United Nations Conference on Trade and Development (UNCTAD) noted that the development of the use of mobile devices had emerged as the most important ICT contributing to sustainable development and to poverty reduction (see also A/CN.9/692, para. 67, and A/CN.9/706, paras. 9-11).[18] Thus, the widespread use of mobile devices is considered to be a central factor in achieving the Millennium Development Goals.[19]

30. At the colloquium, it was stressed that work aimed at facilitating the establishment of a uniform enabling legislative framework would enhance the likelihood of reaching those goals. The example of the lower cost of payments effected with mobile devices in developing countries as opposed to those carried out through the traditional banking system was mentioned. It was added that, in that example, the difference in cost was inversely proportional to the amount transferred, and therefore the introduction of mobile technologies was particularly beneficial for "low-income" customers.

31. On the one hand, it was suggested that electronic commerce and mobile commerce shared significant technical similarities (see also A/65/17, para. 249) and that therefore the existing legal framework for electronic communications and electronic commerce, including provisions of UNCITRAL texts, might suffice to address legal issues arising from mobile commerce. It was added that expected technological progress seemed to suggest that mobile commerce would simply become mobile electronic commerce without any further distinction.

---

[17] UNCTAD, *Information Economy Report 2010: ICTs, Enterprises and Poverty Alleviation*, August 2010, United Nations publication, Sales No. E.10.II.D.17.

[18] At the end of 2009, global mobile subscription penetration was estimated at 68 per cent, up from 60 per cent the year before. Penetration in both developed and transition economies exceeded 100 per cent while in developing countries it stood at 58 per cent. In least developed countries, there were more than 25 mobile subscriptions per 100 inhabitants.

[19] See, in particular, Millennium Development Goals, Goal 8: Develop a Global Partnership for Development, Target 18: "In cooperation with the private sector, make available the benefits of new technologies, especially information and communications technologies".

32. On the other hand, it was indicated that mobile commerce presented, and was likely to retain for the foreseeable feature, peculiar features due to the specificities of mobile devices (for more information on such specificities, see below, paras. 33-34, 36 and 40-44), and that those features might deserve dedicated legal treatment. It was added that some legal obstacles to the use of mobile devices could arise from legislation in other areas, such as informational requirements in financial and other transactions. Thus, while there was broad consensus that provisions on electronic transactions and electronic commerce should be applied to mobile commerce, support was also expressed for undertaking work on additional specific rules for mobile commerce with a view to fully enabling the use of mobile devices. It was reiterated that any additional legislative provision on mobile commerce should take into full consideration the many points of commonality between electronic and mobile commerce.

Definition of "mobile commerce"

33. It was recalled that mobile commerce had been defined as "commercial transactions and communication activities conducted through wireless communication services and networks by means of short message services ("SMS"), multimedia messaging service ("MMS"), or the Internet, using small, handheld mobile devices that typically had been used for telephonic communications."[20] It was explained that that definition highlighted two fundamental aspects of mobile commerce, i.e., wireless communication and the use of mobile devices. However, it was commented that, while that definition could provide a useful starting point, it might adhere too strictly to the technological status quo and therefore might not fully accommodate progress. In this respect, it was illustrated that not only several dedicated technologies had already been developed to facilitate the use of mobile devices for exchanging electronic communications,[21] but also mobile devices existed that provided wireless connection without using mobile telephone networks.[22]

34. It was suggested that the term "mobile" should not refer to mobile phones but rather to the mobility of devices, as restricting any definition of mobile commerce to mobile phones might exclude other mobile handheld devices that equally enable ubiquitous computing. It was added that any definition of mobile commerce should not distinguish among devices based on their ability to access mobile telephone networks, and that a broader and more "technology-neutral" definition of mobile commerce could be more appropriate.

---

[20] OECD, *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce*, June 2008.

[21] Those technologies include SMS, MMS, Wireless Application Protocol (WAP) browser and Mobile Explorer (ME), Universal Subscriber Identity Module (USIM) Integrated Circuit (IC) Chip, Near Field Communication (NFC). Near Field Communication is used for "proximity transactions" since the device needs to be held close to a reader; other technologies may be used for "remote transactions".

[22] Devices able to access wireless networks independently of their ability to connect to a mobile telephone network include Mobile Internet Devices (MID), Tablets and Smartphones, depending, among other criteria, on size and input method. Handheld devices that do not provide the telephonic communications functions include earlier Personal Digital Assistants (PDAs), Portable Media Players (PMPs), eBook readers and game-related devices.

35. In this line, the following definition of mobile commerce was suggested as a starting point for future discussions: "any commercial transaction and communication activity conducted through wireless communication services and networks using handheld mobile devices designed to be used in mobile or other wireless communications networks". As a matter of illustration, it was indicated that parties involved in mobile commerce included mobile network operators (MNO), mobile vendors, mobile subscribers and trusted service managers (TSM).[23]

Legal standards applicable to mobile commerce

36. It was explained that the use of mobile devices for commercial transactions raised a number of concerns with respect to security of the transmission, secure identification of the parties, formation of contract, options for payment of the price of the goods or services purchased, privacy and data retention, and consumer protection. While those issues were not specific to mobile commerce, it was added, some specific features of mobile devices and their use might require additional consideration.

37. It was recalled that the adoption of UNCITRAL texts on electronic communications would facilitate establishing an enabling legislative framework for mobile commerce, thus helping to address many of the related concerns. Relevant UNCITRAL texts included the Electronic Communications Convention; the UNCITRAL Model Law on Electronic Signatures, 2001;[24] and the UNCITRAL Model Law on Electronic Commerce, 1996, with additional article 5 bis as adopted in 1998.[25]

38. In particular, it was explained that the definition of "data message" contained in UNCITRAL texts was sufficiently broad to encompass information transmitted with mobile devices. It was added that the legal status of transactions carried out with mobile devices would be unclear without a general recognition of the legal validity of electronic transactions.

39. It was further explained that only a few laws dealt explicitly with mobile commerce and that their treatment of the matter was limited to certain aspects.[26] In other cases, the law provided that the modalities for the satisfaction of informational

---

[23] Mobile operators provide services to mobile subscribers; mobile vendors sell goods and services through mobile platforms, either directly, or through intermediaries, including website operators and mobile aggregators; mobile subscribers pay for a mobile phone subscription; trusted service managers guarantee the security and confidentiality of mobile transaction.

[24] United Nations publication, Sales No. E.02.V.8.

[25] United Nations publication, Sales No. E.99.V.4.

[26] See, e.g., article 58, on the elements of the contract to be displayed on a mobile device, and article 62, on the elements of the acknowledgment of receipt to be displayed on a mobile device, of the Loi n° 045-2009/AN de 10 novembre 2009 portant réglementation des services et des transactions électroniques au Burkina Faso. See also Commission of the European Communities, COM(2008) 614 final, *Proposal for a Directive of the European Parliament and of the Council on Consumer Rights* (8 October 2008), article 11(3): "If the contract is concluded through a medium which allows limited space or time to display the information, the trader shall provide at least the information regarding the main characteristics of the product and the total price referred to in Articles 5(1)(a) and (c) on that particular medium prior to the conclusion of such a contract. The other information referred to in Articles 5 and 7 shall be provided by the trader to the consumer in an appropriate way in accordance with paragraph 1."

obligations in radio-telecommunications end devices (i.e. mobile phones) were to be detailed in a separate regulation.[27]

40. It was noted that one impediment to mobile commerce was the so-called "media discontinuity"[28] occurring when users were required to switch to other means to initiate or complete a procedure. For instance, in some instances users could conduct a transaction via mobile device except for initial registration to the service. It was remarked that such approach did not promote the broader use of mobile services.

41. With respect to issues specific to the use of mobile devices that might deserve additional legislative consideration, it was highlighted that differences in technical specifications of mobile devices, such as data storage capacity, could penalize users of "low-range" models, such as users in developing countries and "low-income" consumers. Furthermore, it was suggested that the possibility of input or other man-made error on mobile devices could be higher than on an ordinary computer due to the size of the device. The possibility of limiting the user's liability for consequences of loss or theft of mobile devices to be used as part of an authentication method, e.g. for accessing mobile finance applications, was also mentioned.

42. One challenge in the use of mobile devices related to the possibility of accessing large documents as required by law. It was recalled that mobile devices, being of small dimensions, offered limited display size and screen resolution and might restricted also input methods. It was added that "low-range" mobile devices might offer as sole option scrolling through long texts, which was not user-friendly.

43. It was added that due to display limitations and the cost of transmitting data over mobile telephone networks originally designed for voice, a practice had developed of designing dedicated websites for mobile devices.[29] Due to their intended goal, such dedicated mobile websites could offer less information, including legally relevant one, and could also be updated less frequently, than their conventional equivalents.

44. With respect to electronic signatures, it was noted that, while mobile devices could normally be used to identify the author of a communication, few of them could technically be able at the present time to meet a higher standard for "advanced", "qualified" or "digital" signatures associated with legal presumptions. As an example, reference was made to the common use of a smart card and card reader combination to generate higher standard signatures, and to the fact that that combination could currently operate only with a limited number of "high-range" mobile devices. It was further noted that the quantity of information to be transmitted was proportional to the level of security of the signature, and that "larger-size" transmissions might be more difficult and more expensive in areas with reduced connectivity, thus discouraging users in those areas from using more secure signature technologies.

---

[27] Article 28 of the French Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[28] Referred to as "Medienbruch" in the German language.

[29] The top-level domain name ".mobi" is an example of a mobile website which is used by mobile devices for accessing Internet resources.

45. Moreover, it was explained that users of mobile devices would typically change device frequently and that those devices were prone to damages by both usage and non-usage. It was added that certain components of mobile devices could affect their life cycle, and that synchronization and backup processes could also pose difficulties. Therefore, it was concluded that mobile devices were not designed for long-term storage of a large quantity of data. These circumstances were likely to impact on the ability of those devices to meet legislative requirements for data retention and archiving of information. Possible alternatives could envisage forwarding the information to be stored to more adequate devices or to dedicated storage service providers.

46. It was suggested that the above challenges might find adequate solution by extending the functional equivalent approach to substantive requirements. According to that proposal, it would first be necessary to identify the purposes or functions of those protection rules whose fulfilment with mobile devices might be difficult. Then, it would be possible to prepare provisions containing simplified requirements compatible with the use of mobile devices and able to achieve those purposes previously identified. Whenever those special rules could be met, contractual parties would be considered in compliance with general provisions, too.

47. As an illustration of the above proposal, it was indicated that the purpose of information duties mandated before the conclusion of the contract was to ensure an informed consent, especially for contracts concluded remotely. In that case, the suggested equivalent mechanism might consist of limiting the information to be provided prior to the conclusion of the contract to core one, and to complement that information at a later stage, including by granting an additional right of withdrawal. Similarly, the purpose of information and conservation duties imposed after the conclusion of the contract was the provision of the information needed during the performance of the contract, including for evidence in case of dispute. In that case, an equivalent mechanism could foresee the provision of the information on a different medium available at a later stage, or the use of third-party providers of data archiving services.

Mobile payments and mobile banking

48. It was indicated that the use of mobile devices was of growing importance in the area of payments and banking. It was explained that applications in this field could be categorized as mobile payments, electronic mobile money and mobile banking.

49. It was explained that mobile payments referred to “any payment in which a mobile device was used for the purpose of initiation, activation or confirmation of the transaction”. Transfers of sums of money carried out using mobile devices could take place through direct mobile billing or mobile credit card schemes. Regulations applicable to payments, such as anti-money-laundering and “know your customer”, would apply to mobile payments, too. However, it was added, mobile payments services could be designed in a manner not to provide access to credit, so that mobile network operators offering payment services would not fall under the purview of rules on the supervision of financial institutions.

50. A trend to establish joint ventures between financial institutions and mobile network operators with a view to creating platforms parallel to the financial

payment systems governed by central banks was reported. It was indicated that the goal of those platforms was to promote alternative means of payment enabling mobile commerce.

51. It was also explained that direct mobile billing allowed customers to purchase goods and services online by charging their price to mobile phone bills issued by a mobile network operator. In a typical scheme, a customer purchased goods or services from a merchant who was enabled to access the payment gateway. The payment gateway facilitated the exchange of electronic information on the transaction between the merchant and the mobile network operator. The mobile network operator paid the price of the good or service purchased to the seller and eventually charged the customer's mobile phone bill.

52. Mobile credit card services allowed customers to make payments with a credit card contained in a subscriber identity module (SIM) card inserted in the mobile phone or with a credit card downloaded over the air on the mobile phone. Purchases were charged to the credit card and paid under the terms of the credit card agreement.

53. It was further explained that both bank-based and non-bank-based models were possible in mobile commerce. In the latter, the parties were not linked to the banking system and therefore did not fall under the scope of competent supervisory authorities, but rather under different types of control and supervision applicable to non-traditional payment service providers. The non-bank-based model could feature electronic and mobile money issuers, cash-in and cash-out agents in charge of converting cash into electronic mobile money and vice versa, and traditional merchants.

54. Electronic mobile money was described as a certificate of transferable monetary value issued and stored in electronic form and installed in mobile devices. It was explained that electronic mobile money was currently used mainly for micropayments such as public transportation, parking and tunnel fees and payment of small sums at convenience stores. It was further explained that stored-value products, defined as payment methods in which a prepaid balance of funds, or "value", was recorded on a device held by the consumer, and the balance was decreased when the device was presented for payment, might not coincide with electronic mobile money.

55. It was said that mobile banking referred to the possibility of accessing conventional bank accounts through mobile devices. The access could be limited to informational purposes, or enable some or all banking and financial transactions permitted under electronic banking. The high level of security required for such transactions often required the download on the mobile devices of dedicated software applications. It was recalled that that type of service would fall under the oversight and controls applicable to banking and financial institutions.

56. It was suggested that, due to the automated and remote nature of the transactions, it might be advisable to allocate on financial institutions, mobile financial business operators[30] and payment service providers the risk for

[30] Mobile financial business operators encompass providers of mobile electronic money and of direct mobile billing services.

unauthorized financial transactions, except in case of fraud or gross negligence attributable to the user. According to the same suggestion, mobile network operators might be held liable for transaction errors occurred during operations under their control, while a duty to indemnify any loss caused by their negligence might be imposed on trusted service managers. Finally, users would have a duty to notify immediately the loss of the mobile device and any other event that might facilitate unauthorized transactions and would bear consequences for not doing so.

57. From the regulatory perspective, it was mentioned that oversight and controls applicable to traditional financial institutions might not be adequate for mobile financial business operator and that therefore additional rules might need to be developed.

Relation to UNCITRAL Model Law on International Credit Transfers

58. It was suggested that UNCITRAL texts on international payments such as the UNCITRAL Model Law on International Credit Transfer, 1992,[31] which covered issues related to payment in the form of orders to a bank to transfer money from an existing account to a beneficiary, could assist in regulating electronic credit transfers used in mobile financial transactions.

59. However, it was also said that that Model Law did not provide for all potential legal issues arising from electronic or mobile financial transactions. In particular, it was noted that mobile payments and mobile banking could pose peculiar challenges related to the use of mobile devices that might deserve dedicated legislative treatment. An illustration of the allocation of liability for loss arising from fraudulent use or from errors in the transmission or processing of the electronic information was provided. Moreover, it was mentioned that further consideration of the legal status of the network service operator in mobile financial transactions might be desirable with a view to clarifying when that operator should be considered an agent of the sender, an agent of the payment system provider or the payment system provider itself.

60. Examples of specific legislation for electronic financial transactions, applicable also to mobile financial transactions, were provided.[32]

61. Furthermore, it was said that mobile payments featured instruction and payment flows different from other payment systems and thus it might be useful to develop dedicated rules. In this regard, on the one hand, the view was expressed that a revision of that Model Law to include aspects of mobile payments was not advisable and that new rules should be independent of that text.

62. On the other hand, the view was also expressed that a thorough revision of the UNCITRAL Model Law on International Credit Transfers would be desirable. It was indicated that while that Model Law offered a very good starting point for providing adequate legislative treatment to mobile and other electronic payments, technological and other developments required the preparation of a more modern instrument.

---

[31] United Nations publication, Sales No. E.99.V.11.

[32] The Electronic Financial Transaction Act, 2008, of the Republic of Korea; see also Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, *Official Journal L* 319, 5 December 2007, pp. 1-36.

63. The following issues were mentioned as relevant for such revision: the introduction of separate rules for credit and debit transfers, in line with modern payment legislation; liability of mobile network operators, including by clarifying the notion of "commercial reasonableness" in this context; the transposition of rules on electronic communications, including those on electronic signatures and data storage, in the field of payments; and the interaction between general provisions on the allocation of liability and special payment systems agreements. It was also mentioned that a revised version of the UNCITRAL Model Law on International Credit Transfers might take into special account the needs of developing countries with a view to facilitating legislative enactments in those countries.

International remittance transfers

64. International remittance transfers were identified as a cross-border payment service deserving special consideration. It was explained that such remittances were relatively low in value and often performed by migrant workers. They consisted mostly of credit transfers initiated by an instruction sent by the transferor, including via a mobile device, to a remittance service provider. The typical scheme of an international remittance transfer foresaw the presence of two remittance service providers, one capturing the transfer order and the other disbursing the sum transferred to the beneficiary.

65. It was explained that low-value credit transfers fell under the scope of the UNCITRAL Model Law on International Credit Transfers but did not represent a primary concern for the drafters of that Model Law. It was also recalled that that Model Law did not deal with consumer protection issues and that its explanatory note clarified that dedicated consumer legislation might prevail over legislation based on the Model Law.

66. Taking the above into account, it was indicated that the UNCITRAL Model Law on International Credit Transfers provided sufficient basis to adequately address legal issues relating to international remittance transfers. In particular, reference was made to its article 5, paragraphs (2), (3) and (4), establishing rules on authentication systems in case of payment orders. However, it was added that originators of the remittance transfer would benefit from a different loss allocation scheme for unauthorized credit transfers, which, under the Model Law, might be inadequate for consumers protection. Additional contractual disclosures, also meant to favour consumers, might also be considered.

Other mobile device applications

67. It was indicated that a number of mobile commerce services based on different technologies such as location-based services, voice-based services and SMS-based services were gaining popularity. It was illustrated that those services could be used in a number of commercial and non-commercial fields such as election monitoring, earthquake relief and mobile micro-insurance.[33] In this respect, a trend towards greater use of mobile devices for accessing e-government services was noted. It was said that that trend could become relevant also for commercial transactions, especially with respect to the use of mobile devices for authentication purposes.

[33] See also UNCTAD, *Information Economy Report 2010*, cit., p. 19.