OECD publishing

Please cite this paper as:

OECD (2012), "Report on Consumer Protection in Online and Mobile Payments", *OECD Digital Economy Papers*, No. 204, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5k9490gwp7f3-en

OECD Digital Economy Papers No. 204

Report on Consumer Protection in Online and Mobile Payments

OECD

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

17-Aug-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY

Cancels & replaces the same document of 15 June 2012

REPORT ON CONSUMER PROTECTION IN ONLINE AND MOBILE PAYMENTS

JT03325392

DSTI/CP(2010)22/FINAL
Unclassified

English - Or. English

FOREWORD

In 2009, the OECD Committee on Consumer Policy (CCP) launched a review of the principles in the OECD's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce*. In that context, the committee organised a conference on *Empowering E-consumers: Strengthening Consumer Protection in the Internet Economy*, which was hosted by the US Federal Trade Commission on 8-10 December 2009 in Washington, D.C. The emergence of and the need for safer and more convenient online and mobile payments were seen by stakeholders as a key driver for promoting innovation and growth in e-commerce. In light of discussion at the event, the committee agreed to undertake research and analysis in this area and to prepare this report, to help identify policy issues that stakeholders may need to address.

The report, which was declassified by the committee at its 83rd session on 23 April 2012, was prepared by Brigitte Acoca, of the OECD secretariat. It benefited significantly from input provided by governments, civil society and businesses. Issues were discussed at an *OECD Workshop on Consumer Protection in Online and Mobile Payments* held at the OECD on 15 April 2011[1]. They were also discussed with the International Consumer Protection and Enforcement Network (ICPEN), which set up a mobile payments working group in late 2011, and at a workshop on *Paper, Plastic, ... or Mobile?* which was organised by the US Federal Trade Commission on 26 April 2012, in Washington, D.C. (see www.ftc.gov/bcp/workshops/mobilepayments/). The report is published under the responsibility of the Secretary-General of the OECD.

1. See *www.oecd.org/sti/consumerpolicy/workshoponconsumerprotectioninonlineandmobilepayments.htm*

SUMMARY

The examination of payments issues is taking place in the context of the committee's review of the OECD's 1999 guidelines on e-commerce. It explores the extent to which the principles in the guidelines on payments (OECD, 1999, Part II, Section V) and related principles on consumer information, fair business practice, and dispute resolution and redress, adequately address the issues raised by new and emerging online and mobile payment mechanisms. It looks at what might need to be amplified or revised to enhance consumer trust and adoption of new and emerging online and mobile payment mechanisms. The report reflects contributions made by national delegations, business and civil society; it was discussed at a stakeholder workshop held in April 2011.

Trends

The development of innovative and easy-to-use payment systems by financial institutions and other businesses (such as mobile operators and Internet companies) has helped to support rapid growth in e-commerce, in many cases providing consumers with more effective, convenient, and secure ways to purchase an expanding variety of products, including digital goods and services. It has also helped to address problems consumers may experience with vendors when, for example, products do not meet expectations or are not delivered. However, the following analysis of online and mobile payment systems suggests that their role in facilitating transactions and empowering consumers in e-commerce could be strengthened by addressing a number of ongoing and emerging challenges.

Policy issues

The report identifies a set of issues that policy makers may need to address to strengthen consumer confidence in new and emerging e-commerce payment systems. The issues cover five principal areas:

- Clarity, transparency and completeness in information disclosure.
- Variability in regulatory and protection regimes.
- Fraudulent, misleading and deceptive commercial practices.
- Dispute resolution and redress.
- Security and interoperability.

TABLE OF CONTENTS

INTRODUCTION

The rapid development of the Internet, the growth of mobile services and other technological innovations have proved highly beneficial to consumers while, at the same time, presenting new challenges, requiring consumer policy makers to not only keep up with developments, but also find ways to address ongoing and emerging issues (OECD, 2010*a*, Chapter I). In 1999, to support Internet development, the OECD adopted *Guidelines for Consumer Protection in the Context of Electronic Commerce* ("the 1999 guidelines") (OECD, 1999). In 2008, in follow-up to the Seoul *Ministerial Meeting on the Future of the Internet Economy*, the Committee on Consumer Policy (CCP) initiated a review of the guidelines. A background report that examines how the market had developed and related consumer challenges was prepared for discussion at an OECD conference on *Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy*, hosted by the US Federal Trade Commission on 8-10 December 2009, in Washington, D.C. (OECD, 2009*a*).

Following the event, the committee reviewed the situation, deciding it would begin the review of the 1999 guidelines by exploring developments and consumer issues in new and emerging online and mobile payments systems. As illustrated in Box 1, some of these issues are directly addressed by the 1999 guidelines.

Box 1. Payment (OECD, 1999, Part II, Section V)

Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.

Limitations of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce.

Payment systems are used to transfer customer funds to merchants to pay for e-commerce transactions. They include: *i*) payment systems that employ credit/debit or use a bank account to enable e-commerce transactions (*e.g.* card payment networks such as *Visa* or *Mastercard* or online banking based payment methods); *ii*) alternative payment systems provided by non-bank institutions operating on the Internet that are associated with a payment card or bank account directly (*e.g. Google Checkout* or *Checkout by Amazon*) or indirectly (*e.g. PayPal*); and *iii*) mobile payments, which include both mobile contactless or point of sale (POS) payments (*e.g. Google Wallet*) and remote payments made through mobile devices (OECD, 2011*b*, p. 172).

In its initial assessment of the 1999 guidelines, the committee identified a number of payment issue areas for further examination. These include:

- The varying levels of consumer protection (such as limitations on consumer liability) provided in different online and mobile payments systems.
- The role that payment providers can play in strengthening consumer protection, by, for example, providing:
  - Clear and transparent information on available dispute resolution mechanisms.
  - Minimum levels of payment protection that would apply to all payment mechanisms.
  - Authentication tools and age verification systems to ensure secure payments mechanisms.

It should be noted that the 1999 guidelines do not specifically address privacy issues which are dealt with in a separate OECD instrument, namely the OECD privacy guidelines, which are currently being reviewed. Therefore, privacy issues relating to online and mobile payments are not addressed directly in this report.

The report provides background information on recent developments in online and mobile payments to help the committee determine to what extent and how the 1999 guidelines might need to be adapted to the evolving Internet economy. The report examines the characteristics and structure of the changing online and mobile payments marketplace (Section I). It identifies ongoing and emerging challenges for consumers (Section II). The work also builds on research carried out by the CCP in 2001 on payment cardholder protections (OECD, 2002) for traditional payments schemes. In preparing the report, the committee recognised that payments markets are evolving rapidly and that new issues may be emerging which are not assessed; it is important that stakeholders be prepared to respond to new challenges, in a timely manner.

TRENDS IN ONLINE AND MOBILE PAYMENTS

Ten years ago, the principal forms of payment for goods and services purchased over the Internet were by bank-issued payment cards and through offline mechanisms (such as cheques). While payment cards, at over 90% of e-commerce retail transactions in Europe in 2009, over 80% in the United States, and over 74% in Mexico (in 2008), remain the dominant payment mechanism in e-commerce, in the past few years, the payment industry has developed an array of competitive online and mobile payments services to respond to the growing consumption of physical and digital goods and services online (OECD, 2011*b*, p. 172, paragraph 283).

This section examines how online and mobile payment mechanisms have developed in recent years. It provides *i*) working definitions for different types of payments systems; *ii*) examples of current online and mobile payment mechanisms; *iii*) a look at the range of traditional and newer alternative payment providers, *iv*) a snapshot of trends in these markets; and *v*) a brief overview of issues related to consumer behaviour and preferences in this area.

I. Definitions

For the purposes of this report, e-commerce refers to orders for goods or services which are made and confirmed electronically *via* the Internet (*i.e*. online) or *via* other electronic platforms (such as those operated by mobile network operators) (see OECD, 2011*c*).

Payments for such goods and services can be made by various means including electronically (see above), or by cheque, cash, or phone (using a payment card or other payment means).

Mobile payments are payments for which payment data and instruction are made *via* mobile phones or other mobile devices. Such payments would include Internet payments using a mobile device, as well as payments made through mobile network operators (MNOs). Note that the location of the payer and supporting infrastructure is not important: the payer may be on the move or at a point of sale (Innopay, 2011).

This report focuses on electronic payments made to conclude e-commerce transactions.

II. Online and mobile payments options

Online payments means

As described in an OECD report on *Online Payment Systems for E-commerce*, online payments include the following (OECD, 2006, p. 38-53):

- Account based systems, whereby payment is made through an existing personal account (usually a bank account).
- Credit cards (including *Visa*, *MasterCard*, *American Express*).
- Debit cards (including *Visa*, *MasterCard,* and national debit card providers, such as *EFTPOS* in Australia).

- Mediating services (such as *PayPal*, and, in the United States for example, Automated Clearing House (ACH) processing[2]).
- Automated mechanisms for bill payments.
- Online wallets: To create an e-wallet account, a user must register with a payment provider. The account is generally linked to the user's email address. The user then can upload money onto the account generally by using a debit or credit card. Payments can be made after entering a username and password. Once the identity of the user is confirmed, a payment may be made and deducted from the account.
- Electronic currency systems (or prepaid payment services), whereby the user transfers value in advance to a personalised account at a payment service provider through an online wallet or to a device such as a smart card.

Additional payment mechanisms include:

- Online banking based Internet payments. Consumers using this facility are redirected from a merchant's web page to the consumer's own bank's online banking site, where an online transfer form may be filled in with the transaction's details, following which the consumer authorises the payment. Online payment banking is gaining popularity in a number of European countries including Austria (*EPS*), the Netherlands (*iDEAL*), Belgium (*Bancontact/Mister Cash*), and Germany (*Giropay*). The method is also emerging in the United States (through *Secure Vault Payments*), and Canada (*Interac Online*).
- Cash-on-delivery, which involves the payment for an item ordered online when it is physically delivered.
- Escrow services, which are often used for online auction-based purchases. A third-party intermediary is responsible for holding a buyer's payment until the buyer receives and approves the merchandise. In Korea, from August 2011, the value of the items covered by the country's escrow scheme will be lowered from USD 91 to USD 45. In the Netherlands, the postal company *TNT* is working on the development of a new online payment service enabling consumers to provide the payment upfront using online banking, which will be kept in escrow by the postal company. The payment will only be released to the merchant once the consumer confirms, *via* a special code, receipt of the products purchased.

Mobile payments means

Through their mobile devices, consumers can purchase products in two principal ways (EPC, 2010*a*, p. 58):

- Mobile, POS, contactless payments: Such payments involve goods which are purchased when buyer and seller are both present; the payment is made using contactless radio technologies, such as NFC, which is a radio-frequency standard and proximity-based technology enabling communication between electronic devices, Bluetooth or infrared technologies for data transfer.

2. In the United States, ACH providers offer a means of accepting and issuing payments from checking or saving accounts electronically. ACH gives access to online companies' products and services to a large number of customers. Recently, the US Reserve Banks began offering FedACH International Services enabling the transmission of funds between the United States and other countries using the National Automated Clearing House Association (NACHA), an organisation that develops electronic solutions to improve the ACH payment system.

- Mobile remote payments: These payments are initiated using mobile devices; transactions are carried out over telecommunication networks such as the global system for mobile communications (GSM) or Internet. Such payments, which are not location-sensitive, may be made through:
  - SMS: Under this system, an account is established by the consumer with a mobile payment service provider (MPSP). It may be linked to a bank account or a credit, debit or pre-paid card. The consumer sends an SMS to the MPSP specifying the amount to be paid and the payee's phone number; the MPSP then sends an SMS back to the consumer confirming the transaction and requesting the consumer to provide a personal identification number (PIN) to authenticate the payment. The MPSP then transfers the money to the payee's account. This payment method is oftentimes used to pay at car parks, and petrol stations, and for payments involving individuals. It is widely used in Asia and Africa.
  - Wireless application protocol (WAP): Under this system, consumers access a web merchant site using the mobile device's browser and make purchases in the same way as a traditional online purchase.

Mobile payments can be processed as follows:

- They may be charged to a consumer's mobile phone bill. This is typically the case for services purchased from telecom operators such as ringtones or themes/wallpapers for mobile devices. The approach was pioneered in Korea, in 2000, by *Danal*, a mobile payments company; it has been particularly popular with young people. By 2007, some 70% of all digital content in the country was charged onto mobile phones bills (KPMG, 2007). Use of mobile devices has, moreover, been expanding and is being used in some countries for purchases made at vending machines (Bank of Finland, 2003).
- They may be made through debit or credit cards. Many stakeholders, however, take the view that such payment means are not well adapted to mobile devices as entering a 16 digit credit card number onto a mobile device may not be convenient. Moreover, research reveals problems with the processing of payments with credit cards through mobile phones as many mobile handsets cannot support the secure software connection used in processing credit card data (Consumer Focus, 2009, p. 44). To overcome these concerns, a new approach (*Buyster*) is being developed in France by some mobile operators to enable consumers to purchase products through their mobile phones on websites without having to enter their credit card number. When registering for the first time on the *Buyster*'s website (and at that time providing the financial information that would otherwise be provided to an e-merchant), a unique code is attributed to the customer. It is that code only that will need to be provided by the consumer when making a purchase; payment will then be debited from the customer's banking account.
- They may be made through a wired or wireless integrated chip (IC) card (pre-paid payments).

III. Payment service providers

The traditional payment service providers include banks (including, in the case of card payments, the "issuing" bank, which provides the card to the card holder or consumer, and the "acquiring" bank, which is used by the merchant or seller), card networks, and payment processors (*i.e.* third parties responsible for processing payments between merchants and acquiring banks).

In recent years, new payment players, often referred to as alternative payment providers (APPs) or payment institutions, have increased their market share and gained consumer acceptance worldwide. Such non-banking organisations, which, according to research, conducted 156 million transactions in 2009

(*i.e.* some 5% of all m-payments) (Capgemini, 2010), include online payments service providers, and mobile network operators (MNOs).

Online payments service providers include *Amazon Payments*, *Google Checkout*, *PayPal* and *Bill Me Later* (which was acquired by *PayPal* in 2008). In some jurisdictions, it should be noted, these payment providers are considered as banks by regulatory bodies. In Asia, *Facebook* partnered with a Malaysian payment service provider to enable its users across Asia (including Australia, New Zealand and India) to purchase virtual goods and games from its platform. The payment ecosystem was given a further boost when *PayPal*, in late 2009, opened its platform (*PayPal X*) to software developers to promote development of new payment services.

MNOs are also playing a growing leading role in mobile payments in a number of countries. They do so under a range of business models, which can be categorised as follows:

- *Mobile centric model*: The mobile operator acts independently to deploy mobile payment applications to NFC-enabled mobile devices. The applications may support prepaid stored values or charges may be included on a customer's wireless bill (such as *NTT DoCoMo* in Japan).

- *Bank centric model*: Under this model, banks develop a mass-market payment mechanism independently, without involving mobile operators or mobile phone manufacturers. For example, in France, the *Caisse d'Epargne* developed the *Movo* service which provides a payment channel by SMS text.

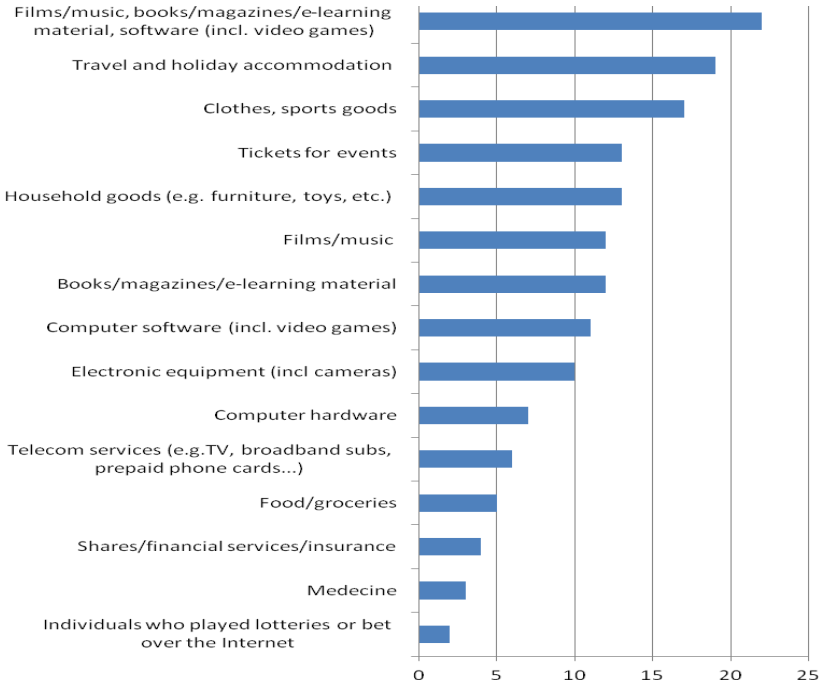
- *Partial integration model*: This involves a mobile operator creating a bank subsidiary to handle mobile payments, such as *Mobikom* in Austria, which offers a payment mechanism for vending machines.

- *Full collaboration model*: Under this model a joint venture is formed between mobile operators, banks, and other payment providers; those developed by *AT&T Mobility*, *Verizon Wireless*, and *T-Mobile USA* are examples; another is the NFC-payments pilot CITYZI project developed in Nice (France) in 2010 by major French banks, mobile operators, transport companies and local authorities. In 2011, *Google* adopted this model in the United States with the launch of *Google Wallet*, an NFC-enabled system within the framework of which a partnership has been established with Citi (the issuing bank), MasterCard (the payment network), First Data (the payment processor), and Sprint, the initial carrier. Although costly to establish, this business model may be attractive to the consumers and business entities involved as it leverages expertise from all parties (from the financial, and telecommunications sector) and enables the establishment of a single technology standard for mobile payments.

IV. Growth in online and mobile payment mechanisms

The growth in e-commerce, including mobile commerce, has been accompanied by the development of innovative, easy-to-use and more secure payments schemes. This has, in turn, helped to inspire greater consumer confidence and participation in online shopping. As shown in Figure 1, the range of goods and services consumers are purchasing on the Internet is broad, particularly in the areas of film, music, books as well as travel and holiday services.

Figure 1. Goods and services ordered by individuals over the Internet in the last 12 months EU 27, percentage of all individuals (2009)



Source: Eurostat, 2009.

Along with this growth in e-commerce, has come growth in online and mobile payments. In 2009, the worldwide value of online payments was estimated at EUR 790.1 billion; this was expected to reach EUR 1 382.3 billion in 2012 (Capgemini, 2010). The value of global m-payments, on the other hand, was estimated at EUR 41.5 billion in 2009, with the level expected to reach EUR 140 billion by 2012, mainly driven by developments in developing economies (Capgemini, 2010).

Online payments adoption and outlook

Credit cards generally remain the dominant form of online payments. Such payment preference can be explained by the existing widespread use of such cards, but it could also reflect the fact that in some countries, credit cards offer the best chargeback mechanisms and protection from fraud losses. As credit cards tend to carry higher fees for merchants than other payment mechanisms, some merchants have tried to encourage consumers to use those that cost the merchants less. Some merchants, for example, would like to be able to offer rebates to consumers for using, for example, a debit card instead of a credit card, or a credit card that does not offer a reward (Internet Retailer, 2010*b*). According to a report by Javelin Research, credit card use for online payments is slipping, albeit slowly, in the United States. They captured 43.5% of online total payment volume in 2009; this is expected to decline to 39.4% in 2014 (Javelin Research, 2010). In the United Kingdom, debit cards are gaining market share. In 2009, for the first time, more people used debit cards than credits cards in the country to shop online (UK Payments Council, 2010, p. 20). As discussed later in this paper (see the discussion on the Single Euro Payments Area – SEPA), debit cards are increasingly seen, especially in today's economic downturn, as a useful and inexpensive way for consumers to easily handle their micro-payments.

Consumers appear to be gaining confidence in APPs. According to private sector research, consumer confidence in banks that provide payment mechanisms is virtually the same as for alternate payment providers (67% for banks versus 64% for alternatives). Consumers aged 45 to 64 show a level of trust in alternate payment providers that exceeds their trust in banks (CISCO, 2008).

The development of APPs has been driven by five main factors:

- *Lower costs for merchants*. Fees imposed by APPs on merchants are often far less than those of credit card companies (Roth, 2010).
- *Data security and "portability:"* APPs provide consumers with the possibility to purchase products with a single user name and password without the need to disclose credit card details to the merchant. For example, *Obopay*, a United States company specialising in mobile payment systems, enables consumers to make purchases with credit or debit cards which are linked to the customer's mobile number, without having to disclose personal information, such as a billing address or a card number. Through *PayPal*, a consumer registers once and, whenever buying a product from a participating merchant, can click on the service's icon and process the transaction without having to re-enter personal data. The service provider pays the merchant by billing the consumer's credit card or by debiting the consumer's bank account. With *Bill Me Late*r, payments can be processed without using credit cards; instead, consumers pay online from a checking or savings account.
- *New ways to collect money*. While credit card companies impose a fee on merchants per transaction, new programmes have been put in place to minimise transaction costs. For example, Apple's iTunes and Research in Motion's payments programmes reduce transaction fees by bundling a customer's purchases before sending them to a credit card company, for processing.
- *Growth of social networking and online gaming*. A variety of products are now being purchased on social networking platforms, including digital content and virtual products. Online gaming, which is on the rise, is being boosted by the development and availability of a number of payment means, such as virtual currency, which is used in *Facebook's Credits*.
- *Rise in consumer-to-consumer (C2C) transactions*. The increase in C2C transactions has had a significant impact on the growth of certain APPs. In the United States, C2C transactions have also played an important role in the growth of ACH payment systems.

Some expect the role of APPs to increase in part because consumers feel that they are better protected from fraud under such payment methods than they are using debit cards (Javelin Research, 2010).

Payment solutions are increasingly being coupled with additional services that are implemented to increase consumer satisfaction online. Some APPs, for example, provide consumers with the possibility to convert money earned online (through online gaming, for example) into cash. *PayPal*'s debit card allows its American customers to withdraw cash from ATMs. The same is true with the UK company, *Ukash*, which allows online gamblers to withdraw money offline. In March 2010, *Visa* launched a new online wallet (*Rightclicq by Visa*) where consumers can store their payment card numbers, and through which limited amount of personal information (such as email address and *Rightcliq* password) has to be disclosed when paying at participating merchants. *Rightcliq* also enables consumers to get discounts from participating merchants and to manage their e-commerce activities (for example storing information on selected merchants and products). A social shopping feature also allows them to solicit their friends' opinions on products. The service is accessible from the *Rightcliq* platform, as well as from participating merchants' websites.

Some developing economies have also seen growing interest in e-payments. In China, the online payments marketplace has shown rapid growth, reaching CNY 555 billion (USD 81.4 billion) in 2009, an increase of 135.6% from 2008. More than 100 online payment companies operate in the country, with *Alipay* (*Taboao/Alibaba*'s payment service) leading the market with a 52% share, followed by *Tenpay* (an online payment unit of *Tencent*), with a 24.7% share. The company is reported as planning to extend its payment services across borders (The Paypers, 2010*c*). Responding to the challenges posed by online transactions, the People's Bank of China announced, in June 2010, the adoption of new rules for companies to conduct online payment services in the country, including licensing requirements to be obtained by non-banking organisations wishing to carry out third party online payment services (China Daily, 2010).

Mobile payments adoption and outlook

Purchases of products using mobile devices with high speed broadband are also expected to accelerate. Already, the number of individuals who own third-generation (3G) mobile phones far exceeds the number of payment cards worldwide. Moreover, the global penetration level of digital mobile devices is today higher than that of personal computers.

At the end of 2008, the number of mobile subscriptions worldwide reached 4 billion, with emerging economies being the most dynamic in this area (UNCTAD, 2009). In June 2010, this number reached 5 billion. Mobile devices have become a popular payment mechanism in some developing countries, particularly in those where credit cards are not widely available and many people do not have bank accounts. Such growth in mobile subscriptions and applications, coupled with the rise of social networking and online games, have increased consumer appetite for mobile payments.

Nonetheless, while mobile payments have attracted considerable attention in the past decade, they have not advanced as rapidly as many expected. The exceptions are Japan, Korea and Singapore, where mobile commerce has surged.

In Australia, according to research conducted by *eBay*, around one in four Australian mobile phone owners use their device to make online purchases, including more than 80 000 on *eBay* alone in June 2010 (Noone, 2011). In Mexico, the first mobile payments schemes were implemented in 2011. Taking into account of this nascent but promising market (in 2010, there were approximately 87 million mobile subscriptions out of the 110 million population), a new regulatory framework is being developed by the Mexican Central Bank and the Ministry of Finances, with the participation of the National Banking and Securities Commission.

In the European Union (EU), despite some attempts to commercialise contactless m-payments pilots in a few countries, m-payments are described as still embryonic. The same applies to North America. According to a 2010 study by Forrester Research, in the United States, despite the high penetration of mobile subscriptions, growth in mobile payments has been relatively modest. While 18% of adults active online express interest in mobile payments, less than 6% have ever made such a payment. In 2009, while there were 89.5% of mobile phone adopters, only 3% made mobile payments, of which 1.1% paid through contactless mobile and 2% through SMS text (FRBB, 2010*b*). Forrester indicates that despite rising consumer interest over the past three years, in the United States, in the absence of a business model that addresses the needs of all payments players, it has been difficult to convince consumers of the value of the various available payments systems and services (Forrester Research, 2010). Newer initiatives such as *Google Wallet*, which will eventually integrate with *Google Offers*, *Google*'s new pre-paid "deal of the day" offer/voucher programme, may change the situation. The report notes that countries with a high share of cash transactions have developed their mobile payments markets more rapidly than in countries with a high share of payment card transactions. Reliance on cash in Japan and Korea, for example, was 50% and

34% of overall in 2006, respectively, compared to 14% in the United States (FRBB, 2010*a*). This finding however cannot be extended to all countries. In Italy and Greece where there is a high level of cash transactions, the mobile payments marketplace still has to take off.

Increases in mobile payments are, however, nonetheless expanding in most areas. In 2009, the number of mobile payment users worldwide was estimated at 108 million, up 25.6% from 2008; it was predicted that the number would grow to 147 million in 2010 (Report Linker, 2010). ABI Research predicts that mobile payments in the United States could reach USD 2.4 billion in 2010, growing by 100% in one year (while however representing only 8% of the total projected e-commerce market) (The Internet Retailer, 2010*c*). In some countries, the number of merchants launching mobile commerce websites is increasing, as are mobile payments mechanisms. These are increasingly perceived by both merchants and consumers as a good payment solution for small value products (up to USD 25), which include:

- Travel products, parking, concert tickets.
- Mobile content and services such as games, music, ringtones, videos, pictures, news, directory enquiries, and public transport route information.
- Purchases on vending machines and various other forms of self service machines.

The sharp rise in mobile payments reflects, in part, the convenience of such payments, which, when it comes to POS payments, are seen as a good alternative to cash. The fact that individuals can make payments and prepaid purchases easily and without any bank account, may also be spurring growth. Young consumers, who are increasingly using mobile devices instead of fixed computers for Internet access, for example, may be more eager to adopt mobile payments. According to a study by Juniper Research, the availability of secure and easy-to-use payment applications and the growing realization amongst users that they can make e-commerce purchases by mobile are expected to further drive the market for both digital commodities, such as entertainment and tickets, and physical goods, including groceries, clothes, gifts and books. The research company forecasts that the value of physical and digital goods purchased by individuals *via* their mobile devices, which amounted to USD 100 billion in 2010, could double by 2012, reaching USD 200 billion worldwide (Juniper Research, 2010). Moreover, some predict that growing implementation and adoption of NFC-led mobile payments will drive further growth (Gigaom, 2011).

In 2009, the European Payments Council (EPC) confirmed such a trend in its *Roadmap for Mobile Payments*, which is exploring ways to facilitate NFC payments. As indicated at the payments workshop, since 2007, the GSM Association (GSMA) has been working together with over 60 of the largest MNOs on its *Pay-Buy-Mobile* project to develop a common vision for NFC-enabled mobile payments within and across countries. Initiatives are being commercially implemented in that regard in a number of countries, including France (in May 2010), and the United Kingdom (in May 2011). However, in many countries, much still needs to be done to stimulate widespread adoption of NFC payments. In these countries, the number of NFC readers and the willingness from the major payment players to invest in such technology and make it an integral part of their business is still relatively low. In addition, the added-value that such means of payment may bring to consumers compared to credit and debit card payments is yet to be seen.

In a few countries, however, the use of mobile phones for POS-NFC payments is well advanced and specific mobile payment solutions have been offered for a number of years by the MNOs themselves. In Korea, in 2003, *LG Telecom* partnered with *Kookmin Bank* to put in place an NFC-based system. SK Telecom implemented *MONETA*, a wired and wireless integrated financial service for mobile phones. Users need to register to get authentication from *SK Telecom*. Payments can be made by inserting a *MONETA* chip into the mobile phone. In Japan, the sales of NFC-mobile handsets reached more than 64 million as of the end of 2009 (FeliCa, 2010).

Geographically, mobile payments usage varies from country to country. In general, m-payments have been mainly used to process low-value transactions. In the United States and Canada, mobile payments are being used primarily to purchase digital and virtual goods (such as music, ringtones, and "in-game" items). In some Asian and European countries, mobile payments are made to purchase a broader range of products, including transport tickets, movie downloads and physical goods (Mopay, 2010).

In March 2009, in Japan, electronic money on mobile phones reached JPY 12.1 million, representing 11.5% of the total amount of electronic money, including the money on prepaid cards, credit cards and cash cards issued by banks (Bank of Japan, 2009). As of March 2010, *NTT DoCoMo* had registered 14.2 million of subscribers for its payment brand iD, of which 11.3 million were *DCMX* customers. However, according to *NTT DoCoMo*'s representatives, most of the payments made through the company's payment services are low value and the contactless mobile payment market place has not reached its full potential yet. Mid to high value transactions are said to be lagging behind. Some electronic payment services (which may or may not be NFC mobile payments) are also available, for example, in the form of either prepaid or credit. One study shows that, in fiscal year 2009, *Nanaco*, a payment service provided by *Seven & I Holdings Co.*, the largest distribution and retailing company in Japan, was the most used prepaid electronic payment service, both for mobile and non-mobile payments, accounting for 25.9% of all electronic payment transactions (M's Communicate, 2010). It was followed by *Suica*, provided by JR East, a railway company, with a share of 22.2%. The success of these payments service providers has, in part, resulted from the advantage of integrating payments services into their business; *Nanaco*, for instance, is widely used for payment in all of the chain retail stores of the company group. *Suica* is primarily used for public transportation, but is also widely accepted for purchases at stores and kiosks. Some companies, such as *NTT DoCoMo* further offer mobile credit payment services to their subscribers.

In North America, in 2009, some 44% of *iPhone* owners were reported to be purchasing digital goods (including applications and games), compared to 28% registered in 2008. In terms of payment options, credit cards and *PayPal* were the top preferences, with 51% of buyers indicating having used these methods; 16% of digital goods buyers used *Facebook Credits* for payment (The Paypers, 2010*b*). In the United States, in June 2009, *Boku*, a mobile payment services provider, launched a payment service allowing users to purchase virtual goods *via* their mobile phones on social networking sites and game portals. Since then, the company has developed mobile payment processing relationships with a large number of game and application developers. Its mobile payments service is available from 190 carriers worldwide in 58 countries (a potential 1.8 billion customers) (Virtual Goods News, 2010).

In China, according to data provided by iResearch, the mobile payments sector has seen a 202% year-on-year increase in transaction value, totalling EUR 286 million in 2009. Continued growth is expected in both 2011 (EUR 5 billion) and 2012 (EUR 13.8 billion) (The Paypers, 2010*d*). In May 2010, eighteen Chinese banks, card associations, MNOs, handset manufacturers and industry suppliers formed an alliance aimed at creating standards and a business model for the introduction of a single and open platform to be used by businesses throughout China to offer NFC and mobile payments services. In other developing economies, such as Kenya, Philippines and India, where the share of persons with bank accounts is quite low, the mobile payments marketplace is also regarded as promising. In 2008, a majority of the 361 million 3G mobile subscribers worldwide resided in emerging and transition economies (UNCTAD, 2009). However, it should be noted that in these countries, m-payments are mainly used to process person-to-person payments and remittances (fund transfers).

CONSUMER CHALLENGES IN ONLINE AND MOBILE PAYMENTS

There are three types of consumer challenges for policy makers and other stakeholders in the online and mobile payments markets.

The first set of challenges relates to regulatory frameworks, which involve both legal rules and their relationship to private sector measures. As discussed in Section I of this report, a number of parties, including financial institutions and non-financial institutions are involved in e-commerce payment transactions with consumers. The rules governing their operations, which cover the telecommunications, competition, and financial services regulations areas, as well as consumer protection (specific to e-commerce and/or payments, or general) may differ. In some cases, consumers, merchants and other parties involved in transactions may not fully understand what legal and/or voluntary framework applies to a particular transaction, what the responsibilities are for the parties in the case of fraud or security problems, or what types of dispute resolution mechanisms or redress rights may be available to consumers in the event of a problem. Further complicating the matter are the different views that these parties may have on their responsibilities (FRBB, 2010). This may be particularly relevant in the case of mobile payments where a number of parties, including mobile network operators, payment organisations, debit/credit card networks, clearing/settlement organisations, software solution providers, merchants and applications developers, might be involved and may bear at least partial responsibility when there are problems. In many OECD countries, there is no specific legislation governing mobile commerce and payments specifically and the extent to which general consumer protection rules cover mobile payments may be untested.

The second set of challenges includes general consumer issues, such as unauthorized payment charges, non delivery, late delivery and non conformity of products, as well as dispute resolution and redress. Closely related are also issues concerning consumer information, empowerment, and education.

The third set of challenges concerns technical payments issues that are related to transactions. These include security-related issues, such as digital identity management. Issues relating to interoperability, consumer payments choice, and cross-border e-commerce are also important.

I. Regulatory challenges

The availability and level of consumer protection in online and mobile payments vary significantly within and among countries, depending on (OECD, 2005, p. 14):

- The tool being used to process a payment (debit/credit cards, SMS, pre-paid card, *etc*.).
- The medium used to make the payment (online, versus mobile devices where, for example, payment is charged to a mobile phone bill).
- The payment organisation involved (bank or non-banking organisation).
- The nature of the problem (non delivery, late delivery, non conformity, processing/billing errors, as well as deceptive practices such as misrepresentations and unauthorised charges).
- The nature of the purchased product (tangible or intangible). At both the *OECD Roundtable on Digital Content Products* and the payments workshop, stakeholders noted a lack of specific consumer protection laws governing the purchase of intangible products (such as eBooks and games).
- The nature of the transaction (person to person payments, versus B2C payments).

In light of the above, there are questions as to whether new payment methods such as those made using prepaid cards, and mobile payment schemes (where the payment is processed by an MNO), are covered by the legal and regulatory regimes applicable to traditional credit and debit cards (see TACD, 2009). Such differences are highlighted by the US Federal Trade Commission in its *Consumer Guide to E-Payments* (US FTC, 2003). It notes that consumers using prepaid cards do not benefit from the same types of protection as those afforded when using, for example, a *PayPal* account that is tied to a bank account or a credit card. Research further indicates that most countries do not provide consumers with many legally binding rights to remedies and redress in case of defective or undelivered mobile content products (Consumer Focus, 2009). In the United Kingdom, the question as to whether mobile payments, which allow the consumer to spend up to a certain amount and pay later, may be regarded not as a payment service, but as a credit agreement, is being considered. If the latter solution was favoured, consumers may benefit from the chargeback protections offered by the country's *Consumer Credit Act 1974* (Consumer Credit Act, 1974), as well as from the anti-fraud protections.

The extent to which consumers are aware of the different levels of protection attached to the various payments mechanisms is unclear. Exploring the factors that drive consumer choice of payments methods would be helpful in addressing issues.

Existing regulatory frameworks

The regulatory environment governing online and mobile payments is continuously evolving. Some countries have specific legislation that applies to online and/or mobile payments, while others apply to general consumer protection, telecommunications, or financial regulation.

Korea provides specific regulation. Under its 2007 *Electronic Financial Transactions Act* (EFTA) and the *E-commerce Consumer Protection Act* (ECPA), payment service providers involved in e-commerce are required to:

- Use order forms that enable consumers to change or confirm their order before validation.
- Provide consumers with information about the seller (which should also be available on the seller's website) and about available dispute resolution mechanisms.
- Protect consumer personal information disclosed within the context of the payment process.

Other jurisdictions are in the process of developing and implementing new regulations. In Canada, a major review of the payments framework is being carried out to determine how existing rules should be adapted, or new rules developed, to adequately tackle emerging issues, with recommendations to be made to the Minister of Finance by the end of 2011. Box 2 provides a summary of developments in other jurisdictions.

Box 2. Regulatory developments

Russian Federation: In 2010, the *National Payment System Bill* was approved by the government; the bill is designed to regulate e-payments, requiring e-money operators to obtain a license from the Central Bank (The Paypers, 2010*e*).

United States: In July 2010, the US Congress passed the Dodd-Frank *Wall Street Reform and Consumer Protection Act* (Dodd-Frank Act, 2010). The Act requires the Federal Reserve to establish standards for debit card swipe fees (known as interchange fees) that are reasonable and proportional to the cost of processing debit card transactions and reloadable prepaid debit card transactions. It also allows merchants to set the minimum amount that consumers can charge on a credit card purchase, provided the minimum does not exceed USD 10, and it allows merchants to offer discounts if consumers, for example, pay by cash rather than credit card so long as such discounts do not differentiate on the basis of the issuer or the payment card network. The Federal Reserve Board issued a final implementing rule in June 2011, which establishes standards for assessing whether debit card interchange fees received by debit card issuers are reasonable and proportional to the costs incurred by issuers for electronic debit transactions. Under the final rule, the maximum permissible interchange fee that an issuer may receive for an electronic debit transaction will be the sum of USD 0.21 per transaction and 5 basis points multiplied by the value of the transaction. Moreover, the Act gives the new US Consumer Financial Protection Bureau regulatory, supervisory and enforcement authority over a broad range of entities that provide consumer financial products and services. This includes entities that provide payment mechanisms through technological means such as online banking systems or mobile telecommunications networks. The agency, which began operating on 21 July 2011, will also have broad authority over unfair, deceptive, and abusive acts and practices in the consumer financial services area.

EU: Various regulatory instruments aimed to harmonize, secure, and enhance consumer trust in online payments have been developed in recent years in the EU with a view towards creating a single borderless marketplace. These include:

- **Directive 2007/64/EC on payment services (PSD) in the internal market** (Directive, 2007): The PSD was adopted to create an EU-wide single market for cross-border non-cash payments processed in the European Economic Area (EEA, including Norway, Iceland and Liechtenstein). The instrument covers offline, online and mobile payments. The PSD provides rules on transparency, timing of payments and information requirements. The latter includes information on the terms and conditions related to the payment services offered, security and fraud prevention measures, and rights and obligations of users and providers of payment services, including liability rules in case of defective or non-performance of a payment transaction, or fraudulent use of a payment instrument. The directive provides a framework for protecting consumers against unwanted recurring transactions, enabling them to contact their bank to stop processing payments yet to be made. It should be noted, however, that as regards payments that have already been made, banks usually require consumers to contact the merchant first to settle disputes. The Directive introduces a licensing regime to encourage non-banking organisations to provide payments services.

- **Directive 2009/110/EC on electronic money** (Directive on e-money, 2009): To be read in conjunction with the PSD, the instrument aims to regulate the conditions under which non-banking organisations, in addition to credit institutions, may issue e-money. The concept of electronic money is defined as monetary value issued on receipt of funds and stored on an electronic payment device or remotely at a server and managed by the money holder through a specific account for electronic money (this would include alternative payment providers). It was developed as a response to the emergence of and increasing use of pre-paid electronic payment products, which are used in particular to process micro payments through mobile phones.

- **Directive EC/2000/31 on e-commerce** (Directive on e-money, 2000)**:** A review of the effectiveness of the Directive has been launched by the European Commission in 2010.

- **Directive on consumer rights** (Directive on consumer rights, 2011): Following the EC's review of the *Consumer Acquis* launched in 2004, a directive on consumer rights was adopted in July 2011 with the aim to strengthen and fully harmonize legislation applicable to distance sales across EU Member States. The instrument aims to ensure adequate consumer protection, in particular in the purchase of digital content products, and in cross borders transactions. Its Article 9 requires disclosure of mandatory information to consumers prior to concluding any distant transaction (which includes most online and mobile transactions), including the arrangements for payment, delivery, performance, and complaint handling policy. EU Member States will have to transpose the Directive into their national law by 13 December 2013.

In light of its *Green Paper* on an integrated EU market for card, Internet and mobile payments (EC, 2012*a*), the EC will develop, through 2012, a strategy aimed at notably assessing barriers to entry and competition on these markets, and ensuring that payments services are transparent for consumers and sellers (EC, 2012*b*).

General industry-led initiatives

In addition to regulatory initiatives, there have been numerous industry-led developments in the online and mobile payments markets.

SEPA, E-SEPA, and Mobile SEPA

To implement the above described EU legal instruments, the banking industry, strongly supported by EU institutions, has been developing rules and standards aimed at creating a single euro payments area (SEPA). Under SEPA, consumers would be able to make payments within the internal market through a set of common euro-denominated payment instruments, whether within or across national borders, under the same conditions with respect to rights and obligations, regardless of their location. To oversee the initiative, the banking industry created a consortium, the European Payments Council (EPC), to examine how SEPA would work in practice for any business wishing to participate in the scheme (see EPC, 2010*b*). The European Commission has recently come forward with a proposal for setting migration dates to pan-European credit transfers and direct debits.

Work is underway to ensure that the new borderless marketplace also covers online and mobile payments. As regards the latter area, the EPC is working with banks, payment institutions and mobile network operators towards harmonising standards for mobile payments so as to support the development of mobile payments within banks (EPC, 2010*a*). In 2011, the EPC, which considers mobile payments a good channel for leveraging and promoting the use of SEPA payment instruments, published an implementation guide on mobile payments (EPC, 2011).

Trust marks schemes

A number of trust mark schemes have been introduced to enhance consumer confidence in e-commerce. These are designed to ensure consumers that merchants comply with a number of rules aimed at strengthening security, privacy and combat unfair commercial practices and that certain standards are met with respect to payments. Such domestic trust marks are frequently backed by standards enforcement mechanisms (EMOTA, 2010).

An example of such a trust mark is the Swedish *Trygg E-handel* which was introduced in 2007 in a coalition between private and public organisations. Its role is to support clear and unified guidelines for consumers and e-commerce companies (Figure 2). Under the scheme, an administrator carries out random check-ups. Members of the trust mark are also given a financial rating. An external party audits members' homepages. Issues covered include:

- Company and product information.
- Information on the total cost of a product.
- Timeframes for shipping.
- Warranty information.
- Information on cancelling a contract.
- Provisions for complaints.
- Provisions for dealing with consumers under age.
- Financial security and safe payments solutions.

Figure 2. An example of a trust mark: Svensk Distanshandel in Sweden

II. General consumer protection issues

General consumer protection issues related to payments include: *i*) unauthorised charges; *ii)* deceptive and fraudulent commercial practices, *iii*) non delivery, late delivery, non conformity of products; *iv*) dispute resolution and redress; and *v*) consumer information, empowerment, and education.

Unauthorised charges

Unauthorised charges in online and mobile payments include; *i*) charges debited from an online consumer's account following misuse of financial or other personal information (such as a password enabling access to an online account, or credit/debit card number processed online); and *ii*) charges that are otherwise debited from an online account without consumer consent. They may result from fraud, but this is not necessarily the case. For example, they may arise through a payment being processed by a child in the absence of parental knowledge and/or consent.

Unauthorised charges occur when a third party uses a consumer's financial information to purchase something online without the consent and/or knowledge of the consumer. Stakeholders indicate that this type of fraud remains a major issue for online and m-payments. In many instances, such fraud is committed when a fraudster acquires and uses the personal data that a consumer has disclosed previously online; this is referred to as inline identity theft (see OECD, 2008*a* and *b*).

Despite efforts to enhance security, most online payment systems remain vulnerable to the problem of unauthorised charges. The types of vulnerability vary according to the payment means. Credit and debit cards, for example, were not originally designed for Internet use; those who steal credit card details can use the information to purchase an item without the need to physically possess the card.

Legal protection

Substantial efforts have been made by regulators to address concerns through the implementation of chargeback mechanisms. These are defined as remedies provided by payment card issuers to consumers when problems with purchases arise. In the United States, for example, under the *Fair Credit Billing Act* (FCBA), consumer liability for lost or stolen credit cards is limited to USD 50. In a case where only the consumer's credit card number has been used without any authorisation, zero liability applies. Under the *Electronic Fund Transfer Act* (EFTA), the unauthorised use of a debit card may lead to consumer liability that ranges from USD 50 to USD 500 or more, depending on when the loss or theft of the card is reported. In the European Union (as well as in Iceland, Liechtenstein, and Norway), in accordance with the *Payment Services Directive*, consumers are entitled to an immediate refund for unauthorised charges or billing errors (EC, 2007). It should be noted, however, that the PSD introduces a balance between consumers and merchants' liability. Consumers are not held liable only if they notify the trader as soon as possible or within 13 months of the fraudulent transaction. In Finland, the *Payment Services Act* provides limitations on consumer liability for unauthorised use of credit cards, debits cards and certain mobile payments. In France, under the Monetary and Financial Code, a cardholder is not held liable for a payment which has been made without his authorisation, at a distance, and without any physical usage of the card. In Mexico, under Regulation 34/2010, users notifying their issuer bank that their credit card was stolen or lost are not

liable for charges incurred after the notification. A cardholder may file a complaint before the issuer bank within 90 days after the payment was made. In Canada, consumers' maximum liability is CAD 50. Recent research in the United Kingdom reveals that among the 6% of all Internet users who lost money as a result of online identity theft, the victims managed to recover their losses from their payment provider in three quarters of cases (UK OFT, 2010, p. 16).

Industry protection

Industry has also taken steps to provide consumers with protection through chargeback mechanisms. In the United Kingdom, under the *Banking Code* a cardholder will generally not have to pay anything if someone else uses their card details without permission (BBA, 2008, paragraph 12.12). Under *PayPal*'s *User Agreement*, full refund can be provided to consumers for unauthorised charges or processing errors, provided that notification of any unauthorised transaction are made to the company within 60 days after the problem first appears in the consumer's account. Otherwise, the consumer will be held liable for related losses that occur after the 60 days period, if the company can prove that it could have stopped the losses, had it been aware in time. Such time period may be extended over 60 days if notification was made impossible due to "a good reason, such as a hospital stay" (PayPal, 2010). In addition, *Visa*, *MasterCard* and *American Express* have implemented voluntary schemes, generally referred to as zero-liability commitments, whereby customers are not liable for any unauthorised use of their credit card. For debit card purchases, the *Canadian Code of Practice for Consumer Debit Card Services* outlines industry practices and consumers' and the industry's responsibilities with respect to debit cards. This voluntary code, which is endorsed by banks, credit unions and *caisse populaires*, expressly states that consumers are not liable for losses resulting from circumstances beyond their control.

Mobile payment liabilities

As regards mobile payments, some have called for enhanced protection of consumers against unauthorised charges. While incidents of theft and unauthorised charges are frequent, in a number of countries, consumers in most cases bear liability for potential financial loss (Consumer Focus, 2009). Under most countries' frameworks, if a consumer makes a mobile payment using a credit card or debit card (through a remote mobile payment), the consumer is entitled to the protections attached to the card. However, if a payment service is provided directly by a mobile operator and the charges appear on the consumer's mobile phone bill, there may be no legal protections (MacCarthy & Hillebrand, 2010). Moreover, if a mobile operator asks a consumer to make a prepaid deposit to cover future charges, protections may also be absent. Under *Facebook*'s *Spare Change* payments application, which may be downloaded onto mobile phones to make low value payments, refunds are not available (Facebook, 2009).

A few countries have put in place mobile-specific laws. In Denmark, the Subscriber Identification Module (SIM) card in mobile phones is explicitly regarded as a means of payment like any other payment cards. As a result, the issuer is liable to compensate the mobile phone holder for any loss caused by unauthorised use (OECD, 2007*c*, p. 27). In Norway, if a mobile phone has been reported stolen to the carrier, the consumer is not liable for any charges subsequently registered. The Finnish *Communications Market Act* also provides for limitations of consumer liability for unauthorised use of mobile devices. Legislation in Canada, Sweden and the United States may cover some cases of unauthorised use of mobile phones. In the United States, the California Attorney General entered into a settlement with *AT&T Mobility* under which the cell phone company will not charge customers for unauthorised services. The settlement requires the company to credit a consumer's bill or immediately investigate a consumer's report that the calls were made after the phone was lost or stolen. The company may only charge a customer if an investigation determines that the customer actually authorized the charges. Other US telecommunication companies have adopted similar policies. In Finland, the Consumer Agency has put forward a legislative proposal (under consideration) whereby MNOs processing payments for the purchase of products would be

held liable in case of problems associated with a transaction. The EC Directive on consumer rights, which contains provisions relating to consumer chargeback mechanisms, is technology neutral and covers mobile payments related issues (Directive on consumer rights, 2011).

Deceptive and fraudulent commercial practices

Deceptive and fraudulent commercial practices are often tied to inadequate or misleading disclosure. With mobile devices, disclosure issues are exacerbated, due to the small screen size and the associated difficulties with navigating through multiple links and pages containing information material to a consumer's purchase decision. It should be noted however that with the increasing prevalence of mobile devices with larger screens and higher memory capacity, such as smart phones and tablet computers, some of these concerns may be easing. In certain circumstances, terms and conditions may not even be accessible on m-commerce platforms due to technological limitations.

Key information, such as the actual total cost of a transaction, can be hidden in the terms and conditions, thus increasing the risk of consumers not being aware of, or understanding, the costs. Further, in instances where charges appear on the consumer's mobile phone bill, rather than being billed to a credit card company, the consumer may find that he or she enjoys few, if any, of the protections credit card companies may provide. This could prove particularly challenging to consumers whose expectations have been shaped by disputes over credit card transactions; as such, clear and conspicuous disclosure of terms and conditions become even more important for mobile transactions.

The impact of deceptive and commercial practices can be considerable. For example, the Office of Fair Trading in the United Kingdom estimated in 2007 that unexpected additional charges cost customers EUR 76 to 126 million per year in the United Kingdom alone (EC, 2008*c*). The impact may be particularly significant on children who may not always realise that they can be subject to additional costs or that they have subscribed to a service for which fees are regularly debited to prepaid calling cards. In 2008, some 23.7% of Belgian teenagers reported having paid more for a ringtone than they expected and 7.5% had subscribed to such a service without realising it (OECD, 2011*a*).

To address concerns, some countries apply general provisions prohibiting unfair or deceptive practices to consumer protection issues relating to mobile commerce. For example, Canada's *Competition Act* contains a provision prohibiting misleading representations and deceptive marketing practices that is technologically neutral (OECD, 2007*c*, p. 23). In addition, the *Competition Act* was amended in December 2010, to include specific provisions and tools to address false and misleading representations and deceptive marketing practices in the electronic marketplace, including false or misleading subject matter, sender, and locator information. These amendments are expected to come into force early in 2012.

In the United States, in October 2010, Verizon Wireless, agreed to pay a USD 25 million fine to settle accusations from the US Federal Communications Commission about unauthorised charges the company had been charging its customers for a number of years. Under the settlement, *Verizon Wireless* refunded about 15 million customers more than USD 50 million. In Finland, in February 2011, the *Communications Market Act* was amended to provide new enforcement powers to the Consumer Ombudsman, enabling the authority to order a telecommunications company to close an SMS number used to offer fraudulent or deceptive mobile content services.

Data pass marketing

Data pass marketing is a practice whereby e-commerce parties link up with third parties, providing the third party with a means to entice consumers into purchasing their products or services (such as membership programmes), without the consumer necessarily realising that they are entering into a

transaction with the third party. Under such partnerships, consumer credit or debit card information may be automatically passed on by the "familiar" online retailer to the third party, without consumer knowledge and/or consent. This is often done by the third parties inserting their sales offers into the post-transaction phase of an online purchase, after a consumer has made a purchase but before the sale confirmation process has been completed (US Senate, 2009). Misleading options are presented that can cause consumers to reasonably think they are completing the original transaction, rather than entering into a new one.

In 2010, *Visa* launched an initiative aimed at preventing data pass marketing on its network. *Visa* will require consumers to re-enter their credit card information if they want to purchase a subsequent third-party product or service (Credit Union Times, 2010). In December 2010, the *Restore Online Shoppers' Confidence Act* ("ROSCA") was enacted in the United States, which prohibits data pass marketing in the online context. ROSCA requires third party sellers to provide clear pre-sale information disclosure to consumers, including the fact that they are not affiliated with the initial merchant. ROSCA further requires such sellers to obtain directly from the consumer his or her express informed consent, which must include the full amount to be charged, the consumer's contact information, and an "additional affirmative action" by the consumer.

Negative option

Negative option has been noted as an increasing challenge for consumers shopping online. This practice involves a company taking a consumer's silence or failure to cancel as acceptance of an offer and permission to bill them. A consumer, could, for example, receive a complimentary copy of an online newspaper, which is subsequently transformed into a subscription, unless cancellation is made within a set time period. While potentially convenient to consumers, a lack of express consumer consent and/or information about the offer and related financial consequences on a long term basis could be problematic.

On 1 July 2009, the Australian Communications and Media Authority (ACMA) gave legal force to an industry-developed mobile premium services code (MPSC), which notably introduces a double opt-in requirement whereby a prospective consumer will have to give two independent confirmations of a request before being able to subscribe to an ongoing premium SMS service. And since November 2010, the ACMA is able to issue a temporary *Do Not Bill* order to stop suspect content suppliers from charging customers while it investigates a service. The revision of the MPSC was followed, in 2010, by a review by the ACMA, in co-ordination with domestic industry and consumer groups, of the country's industry-developed *Telecom Consumer Protections Code* (TPSC). As a result of the review, the MPSC will be integrated into the TPSC.

Similar developments occurred in Singapore where, as of January 2011, under the revised *Telecom Competition Code*, mobile operators will no longer be allowed to automatically charge fees to consumers after a free trial service period has ended; they will have to obtain consumers' prior and express consent (IDA, 2010). In the United States, under Section IV of ROSCA, online sellers are prohibited from charging a consumer for any good or service with a negative option feature in an online transaction, unless the seller *i*) clearly and conspicuously discloses to consumers all the material terms of the transaction; *ii*) has obtained consumer consent before charging them, and *iii*) provides a simple way for consumers to stop charges. The US FTC has brought several enforcement actions involving negative option fraud.

Cramming

Concerns have been raised in relation to cramming, which involves including fees and charges on bills for services consumers did not purchase or authorise, usually after consumers responded to an email or downloaded an item that they believed was free or of nominal cost. The Mobile Marketing Association's *United States Consumer Best Practices Guidelines* (the "MMA guidelines") require vendors in the United

States market to provide consumers with a double opt-in, whereby companies must ask consumers twice to confirm that they want to make a purchase, before being charged for a premium service. Although tailored to the US market, the MMA's guidelines also contain guidance for mobile marketers relating to a number of marketing techniques that could be considered deceptive or otherwise unfair. Areas of relevance covered in the MMA guidelines include: *i*) sweepstakes and contests (the need to offer a free alternative method of entering the contest is highlighted as is the benefit of seeking legal advice in developing rules); *ii*) use of the words "free" and "bonus" (the care that should be taken in using the terms is highlighted); *iii*) affiliate marketing (guidance is provided to content providers engaged in relationships with affiliate marketers); and, *iv*) terms and conditions (guidance is provided on best practices to ensure terms and conditions are adequately and conspicuously disclosed to consumers).

In July 2011, the US Federal Communications Commission (US FCC) proposed rules on cramming. Although cramming has, to date, occurred mostly on wire line bills, the proposed rules would require telecommunications companies, including wireless carriers, to indicate on telephone bills and on their websites, how consumers may file complaints with the US FCC (US FCC, 2011). The US FCC is also seeking comment on whether telecommunications carriers, including wireless carriers, should be required to provide accurate contact information for third-party vendors on their telephone bills and/or screen third parties for prior rule violations or other violations of law before agreeing to place their charges on telephone bills.

Apps

Payments issues related to mobile devices applications have been identified as another source of concern by stakeholders at both the OECD roundtable on digital content and the payments workshop. An example was given of a case in the United States involving free games targeting children, within which additional items ("in-apps") had been purchased without parental knowledge in the absence of clear warning of charges for such in-apps that led to expensive bills.

Money laundering and terrorist financing

In 2006, the OECD's Financial Action Task Force (FATF) raised concerns about risks of money laundering and terrorist financing that may be associated with new payments methods including online and mobile payments (FATF, 2006). The FATF developed a number of recommendations to prevent or minimize risks, calling for increased regulation of Internet payments systems (FATF, 2008). According to the Task Force, online payments systems, which do not require face-to-face authentication, are processed quickly and necessitate limited human intervention, may be easily used to sell or purchase illegal products, such as drugs or counterfeit goods. The same concern has been raised regarding prepaid mobile services which do not require users to register at a point of sale. And because prepaid services can often be topped up using cash and vouchers, it may be challenging or even impossible to trace a payment and hence determine the identity of a prepaid phone user. According to a 2005 study, 9 out of 24 surveyed OECD countries require mobile operators to collect customer information for prepaid mobile services to avoid anonymity. These include Australia, France, Germany, Hungary, Japan, Norway, Slovak Republic, South Africa and Switzerland (Simon Fraser University Vancouver, 2006).

Offshore payments agents

In Japan, a growing number of consumer complaints have been made in recent years in relation to the involvement, in online payment transactions, of payment intermediaries (so-called "payments agents"). Such entities, which can act in the place of merchants in the conclusion of a payment transaction with a Japanese credit card entity, are oftentimes operating overseas. Merchants benefit from the low cost of their services and customer information management. Some overseas payment agents, however, are concluding

e-payments transactions on behalf of rogue traders who would not have been otherwise allowed to do so using card networks directly. With a view towards addressing consumer difficulties in contacting overseas payments agents and getting refunds from them in case of payment-related dispute, consideration is being given by the Consumer Affairs Agency to develop a publicly available online registry containing information about the agents and how these or other relevant stakeholders could be contacted by consumers in case of problems.

Non delivery, late delivery, non conforming and faulty products

Problems related to non-delivery, late delivery, non-conforming and faulty products have been linked to payments through government regulation and/or by payment providers, particularly in the area of dispute resolution. When, for example, merchants and consumers are unable to resolve differences, payment organisations often provide a means through which a settlement can be reached. In that regard, the chargeback mechanisms referred to earlier play an important role in protecting consumers. For example, in case of problems with delivery, non conforming or faulty products, the chargeback process developed by *Visa* offers a dispute resolution mechanism through which the issuer of a *Visa* card (a financial institution) can transfer the liability back to the *Visa* acquirer (the merchant). When the merchant disputes the validity of a chargeback request made by a consumer, *Visa* may ultimately resolve any dispute that has not been settled between the bank and the merchant. But as such, the *Visa* chargeback framework does not give any direct rights to the cardholder/consumer.

The levels of protection available vary significantly from country to country. Only a few OECD countries (including Finland, Greece, Japan, Korea, Norway, the United Kingdom, and the United States), for example, have developed specific legal or regulatory provisions protecting cardholders in cases of non-delivery of goods or non-performance of services. In the United States, credit cardholders can delay payment of disputed amounts or have such funds provisionally restored while the dispute is being resolved (OECD, 2005). Such legal protection is however limited to credit cardholders; it neither applies to debit cardholders nor to prepaid cardholders in case of non-delivery or non conformity.

In Korea, both credit and debit cardholders can refuse payment if goods are not delivered. In the United Kingdom, for items between GBP 100 and GBP 30 000, both the creditor and the supplier are liable in the event of breach of contract or misrepresentation. In the European Union, under the Directive on Consumer Rights, where a trader has failed to fulfil his obligations to deliver a product, a consumer is entitled to a refund by the merchant of any sums paid within seven days from the due date of delivery.

In most countries, there are no specific protections attached to the non-delivery of mobile content. In only a few countries, specific e-commerce legislation covers mobile commerce; Korea's *Consumer Protection Act on Electronic Commerce*, which regulates cases of non-delivery or incomplete download of mobile content, is a case in point. The Act requires businesses to deliver products within three working days after receiving payment from consumers or to provide a refund within three days (Consumer Focus, 2009).

As regards non conforming products, specific legislation is in place in only a few countries as well (including Finland, Greece, Japan, Korea, Norway, the United Kingdom, and the United States) to provide consumers with redress mechanisms. For some stakeholders, the consumer protection mechanisms in place in the case of non conforming products are not as developed and effective as those in place for unauthorised charges.

In some countries, industry initiatives have helped address problems. In Japan, for example, *Rakuten*, the country's leading online commerce platform, introduced mandatory escrow payment services (*Rakuten Anshin Kessai Service*, for which there is a charge) for all C2C transactions to address issues of

merchandise non-delivery. Payment is not released to the seller until the buyer actually receives the purchased item. *Yahoo!Japan* also offers possibilities of escrow services, without charging any fees. China's *Alipay* (*Alibaba*'s payment service provider) operates similarly through a partnership with banks. PayPal has implemented a number of solutions to provide consumers with protection in case of non delivery. The company has the ability to freeze the account of a seller who has not shipped purchased items. Its *Buyer Protection Policy* also states that in instances where a customer did not receive an item or if the item purchased was significantly not as described, the customer may file a buyer complaint within 45 days of the date of payment, seeking redress. Issues have however been raised with respect to the adequacy of time periods for notifying and processing claims.

In the event of a claim of a refund for a damaged product, under existing regulations, consumers often have limited rights to remedies and redress for defective intangible goods or services (such as a ringtone or application).

Dispute resolution and redress

The second issue relates to disputes between merchants and customers with respect to the receipt, nature or quality of the good or service purchased where payment intermediaries are only indirectly involved. In this context, some payment providers have implemented measures to resolve online disputes related to the receipt, nature or quality of goods. Some countries require such measures through their legal regimes, while in other countries, these initiatives are private.

As discussed earlier, specific mechanisms, known as "chargebacks" may offer consumers effective protection in case of problems with a payment transaction. Protection can take the form of liability limitations, including the ability for consumers to have billing errors corrected, or redress for when there are delivery problems or problems with the purchased product (OECD, 2007*b*, Annex, Section IV.2*c*). The protection can be far-reaching. In Canada, for example, certain provinces have included provisions within their consumer protection laws that require credit card issuers to refund amounts where a contract has been cancelled in accordance with provincial law and the buyer has not been refunded by the merchant.

Besides chargeback mechanisms, other dispute resolution schemes have been put in place to help settle disputes between the seller and the consumer. A number of third-party options can be pursued, either at government or at industry level. These often involve payment institutions. The third-party options seem particularly important in the case of mobile and online payments, as consumers may find it difficult to contact sellers directly, and opportunities for face-to-face discussions may not be possible. When problems regarding the purchase of goods or services, or the payment itself arise, consumers need to know who to contact in order to resolve issues in a cost effective manner. One of the challenges is to design processes which are viable when low-value products are involved. Another is to have mechanisms in place to deal effectively with transactions involving cross-border trade.

In 2001, the European Commission launched FIN-NET, a financial dispute resolution network of national out-of-court complaint schemes in the European Economic Area countries (the European Union Member States plus Iceland, Liechtenstein and Norway) that are responsible for handling disputes between consumers and financial services providers (including banks, insurance companies, and investment firms). The schemes co-operate to provide consumers with easy access to out-of-court complaint procedures in cross-border cases. In the event a consumer in one country has a dispute with a financial services provider in another country, FIN-NET members will put the consumer in touch with the relevant out-of court complaint scheme and provide the necessary information about it.

Research indicates that consumers are not well informed about available dispute resolution schemes, and the potential role of payment providers, particularly in the mobile payments area. According to a 2009

survey, in the case of mobile transactions disputes including payments, 46% of vendors did not provide consumers with adequate information on the party that would take responsibility for handling a claim, while 71% failed to inform consumers about the applicable dispute resolution procedures (Consumer Focus, 2009, p. 8).

As Internet usage continues to expand, interest has grown in designing efficient mechanisms for resolving online shopping disputes. More traditional mechanisms, such as litigation, can be time-consuming and expensive for consumers. Online dispute resolution (ODR) schemes are increasingly being explored by stakeholders as a means for resolving disputes. Defined as "a means of dispute settlement whether through conciliation or arbitration, which implies the use of online technologies to facilitate the resolution of disputes between parties," online mediation can provide substantial savings when compared with traditional litigation.

As concluded at an international conference hosted by the United Nations Commission on International Trade Law (UNCITRAL) on 29-30 March 2010, in a cross-border context, online mediation tailored to small value transactions may be in fact the only cost-effective option for consumers (UNCITRAL, 2010*a*). While recognising the benefits ODR may bring to consumers, consumer organisations indicate a number of challenges associated with such procedures. These include: *i*) a lack of direct interpersonal contact that may limit consumer ability to explain their problem to a merchant; and *ii*) a required degree of consumer knowledge and familiarity with sophisticated web technology that may be an obstacle for some consumers. Stakeholders take the view that more efficient, low-cost, fair and convenient dispute resolution and redress mechanisms that could be implemented worldwide are needed. Based on these conclusions, UNCITRAL launched work on the development of a legal standard online dispute resolution related to cross-border e-commerce transactions in December 2010 (UNCITRAL, 2010*b*). Draft procedural rules were discussed at the Working Group III's meetings held in May and November 2011 (UNCITRAL, 2011).

Some private companies and governments have developed online redress systems that have proved efficient. For example, PROFECO in Mexico runs *ConciliaNet*, which is an online dispute resolution scheme. According to PROFECO, consumer use of the scheme has considerably helped reduce the time spent for resolving disputes (by nearly 50%), while increasing the number of settlements to up to 96% of the queries. Some 97% of the consumers surveyed by PROFECO reported that they would use the mechanism again.

In 2009, *eBay* announced changes in the dispute resolution mechanisms made available to consumers purchasing products on its platform and using *PayPal* as a payment scheme. While *eBay* used to refer such consumers to *PayPal*'s resolution centre to address the problem, consumers may now try to have the dispute resolved directly through *eBay*, regardless of the payment method used in the disputed transaction.

Consumer information, empowerment, and education

More may need to be done to ensure that education about consumer rights and obligations in online and mobile payments are being provided to consumers and that these are helpful, concretely understood, and acted on. Such a need has been noted in the 1999 guidelines (Section VIII, Part II), a CCP's 2002 report on credit cardholder protection (OECD, 2002), OECD policy guidance on mobile commerce (OECD, 2008*c*), OECD recommendations on consumer education (OECD, 2009*b*, Annex II), and, more recently, at the payments workshop (OECD, 2011*c*).

A recent report from the Office of Fair Trading in the United Kingdom supports the view that consumer information about the conditions under which the online and mobile transaction may be processed is essential to enable consumers to make informed choices (see OECD, 1999, Section IV, C)

(OFT, 2010*b*). The report indicates that education designed to provide consumers with help to understand their rights online should be enhanced. The study reveals that 80% of Internet users know that they can claim their money back from their credit card company if the goods or services are not delivered, three quarters are aware that they would be entitled to return goods within seven day for a full refund, and two thirds are aware they can claim back from the seller if products are not delivered by the due date or within 30 days of the order (OFT, 2010*b*, p. 11).

At the payments workshop, stakeholders also highlighted the need to enhance consumer information about potential problematic vendors. In Mexico, PROFECO developed an online database (available at *http://burocomercial.profeco.gob.mx/BC/faces/inicio.jsp*) containing information about more than 450 traders selling products at the national level, related complaints and adhesion contracts, which may be accessed by consumers and help them make informed purchase decisions.

It is also often difficult for consumers to know what protections they have when purchasing products from another country. Some governments have alerted consumers about the potential differences in the protections that may be attached to, respectively, domestic and cross-border online purchases. The Australian Competition and Consumer Commission (ACCC) has, for example, warned Australian consumers that in the event of a purchase made with an online seller based overseas, they may not have the same basic rights as those that they have when buying from domestic sources. Given the possible practical difficulties in obtaining a remedy from an overseas-based seller, the agency advises consumers to check the terms and conditions of a proposed contract before making an online purchase (ACCC, 2010).

When problems arise, there are possibilities to share experiences by lodging a complaint with *econsumer.gov*, a multilingual public website and initiative of the International Consumer Protection and Enforcement Network (ICPEN).

III. Technical payment issues

Security

A lack of consumer confidence in the security in online and mobile payments continues to be reported as one of the most important factors affecting the development of e-commerce. Most surveys show that consumers' lack of trust is linked to concerns over the security and the misuse of payment data. Results from a survey conducted in Japan, the United Kingdom, and the United States reveal that 86% of mobile phone users are worried about the security risks associated with their devices, while 55% of respondents are concerned about mobile payments (McAfee, 2008). However, some stakeholders take the view that such lack of trust may result more from a misperception of the potential security risks associated with online and mobile payments. Within the European Union, consumer misperception of the level of risk associated with the theft of payment details is seen as inhibiting confidence, while the actual incidence of theft of payment details is quite low; in 2010, only 1% of EU consumers who bought goods online experienced such a problem (EC, 2011).

Moreover, there is a reported lack of consumer awareness of who should be responsible for ensuring the security of payments systems. In Australia, according to the ACMA, consumers expect providers of new mobile payment services to be responsible for protecting them against security threats (Noone, 2011). Consumers are also unaware of the need to be proactive in helping to secure mobile payments (through, for example, responsible behaviour).

It is generally acknowledged among stakeholders that security threats on mobile devices may be more challenging than for personal computers as the mobile devices may be more easily lost or stolen. Hackers may also obtain data through various means such as Bluetooth, RFID, or the device may be infected

through application downloads. Policy guidance developed by the OECD in 2008 touches on this, encouraging participants in mobile commerce to (OECD, 2008*c*):

- Ensure that consumers are informed about potential security and privacy challenges they may face in m-commerce and the available measures which can be used to limit the risks.
- Encourage the development of security precautions and built in security features.
- Encourage mobile operators to implement data security policies and measures to prevent unauthorised transactions and data breaches.

Many stakeholders take the view that there are multiple approaches to enhancing consumer security in online and mobile payments. As indicated at the OECD's workshop on *The Role of Internet Intermediaries in Advancing Public Policy Objectives* held on 16 June 2010 (OECD, 2010*c*), these include legislative and non-legislative mechanisms. For example, a number of technical standards, codes of conducts, and best practices have been implemented by industry. Several payment card networks (including *Visa*, *MasterCard*, and *American Express*) have developed a harmonised set of security standards (so-called "Payment Card Industry Data Security Standards" – PCI DSS); the standards include twelve requirements to help ensure adequate security. In either context, the commitment of all the parties involved (including merchants and payments organizations) to achieve this goal is essential (EC, 2008, p. 5). Implementation of the above security framework has, however, been challenging. Results of a survey suggest that only about one third (39%) of online retailers actually understand the definition of PCI DSS compliance, while 65% do not believe that they are responsible for addressing payments fraud associated with their site.

One of the key developments in recent years has occurred in the field of digital identity. (Identify Management), which is understood as a set of rules, procedures and technical components that implement an organisation's policy related to the establishment, use and exchange of digital identity information (OECD, 2008*d*). IdM in the commercial sector has been recognised as perhaps the most successful security tool in the area of electronic payments in which a number of parties are involved and exchange information relating to consumers' financial information (OECD, 2008*d*, p. 9). Among the various IdM processes, authentication and age verification (discussed below) are regarded as complementary tools to combat security threats and ensure trust in the Internet economy. In 1998, on the occasion of the Ottawa ministerial conference *"A Borderless World: Realising the Potential of Global Electronic Commerce*," ministers recognised the importance of authentication as a useful tool to help e-commerce develop (OECD, 1998). The OECD, through its Working Party on Information Security and Privacy (WPISP) developed a number of projects aimed at enhancing security in the Internet economy. These include the following works:

- OECD guidelines for the security of information systems and networks: which provide a framework for fostering consistent domestic approaches in addressing security risks (OECD, 2002).

- OECD guidance and recommendation on electronic authentication: *i*) the guidance sets out principles aimed at helping OECD countries to establish and modernise their approaches to e-authentication; *ii*) the recommendation encourages countries to establish compatible, technology neutral approaches for effective domestic and cross-border electronic authentication of persons and entities (OECD, 2007*a*).

- Digital identity management: Building on the work on e-authentication, and the Seoul ministerial declaration in 2008, the WPISP prepared a report which explains why digital identity management is fundamental for the further development of the Internet economy and highlights the need to address limitations in current approaches related to the complexity of credential management and the robustness required for high value services. The report provides guidance to

government policy makers for setting efficient framework conditions for innovation across the public and private sectors while enhancing security, privacy and trust in the Internet Economy. (OECD, 2011*d*).

- Protecting children online: in 2011, the WPISP published a report examining the various threats faced by children in the digital environment, including security (OECD, 2011*a*). Building on the findings in the report, a Council recommendation is being developed in the area.

Authentication and fraud detection tools

Authentication is a process enabling a payment provider and/or the retailer to verify the identity of a potential payer before processing a payment. The verification can provide consumers with added confidence in a payment transaction, and can reduce fraud.

A number of initiatives have taken by regulators and industry to improve authentication in payments, sometimes in partnership with public authorities. In Mexico, the National Banking & Securities Commission has set up a special unit which supervises and checks the level of security of electronic payments systems including those made at POS. Banks have, for example, implemented a "3D Secure Internet Security Protocol" aimed at authenticating buyers in real time, to help ensure that only authorised persons would be able to use the payment card. Under the protocol, liability for authenticating the buyer and checking any claim that the purchase was not authorised by such buyer lies in the hands of the financial institution that issued the card, and not the merchant (which has traditionally been the case).

In addition, "EMV" cards, which contain both a chip and a PIN have been introduced in most countries. The EMV Contactless Communication Protocol Specification standard was developed by *EMVCo*, a joint venture between major payment networks *American Express*, *JCB*, *MasterCard*, and *Visa*. This standard establishes specifications for the manufacture of contactless payment instruments that are meant to replace the magnetic stripes on credit, debit cards, and mobile phones. Paradoxically, the more secure cards are expected to entice fraudsters to shift their attention to card-not-present transactions, which could result in increases in online fraud (see EC, 2008*b* and Innopay, 2010).

In November 2010, *American Express* launched *SafeKey*, a fraud prevention tool using *Visa*'s 3D Secure Protocol. In a number of countries, such as the United Kingdom and France, some banks offer enhanced controls to consumers in cases involving high value transactions. They do so by providing a consumer with a "fictitious" credit card number that can only be used one time, thereby ensuring that the merchant does not have access to the consumer's "permanent" credit card number (Box 3). In the European Union in 2009, some 300 000 retailers accounting for almost 37% of e-commerce transactions volume supported the service with over 50 million cardholders enrolled (Visa Europe, 2009, p. 30).

Box 3. An example of e-authentication: French e-Carte Bleue

French *Visa e-Carte Bleue* (launched in 2002): Through a downloadable application, each time a consumer wishes to purchase products online, the *e-Carte Bleue* generates a one-time "fictitious" credit card number that is associated with the actual credit card number. The virtual number is the only financial information disclosed to the merchant. In July 2010, *Visa* launched a new card (*Visa CodeSure*) with a built-in screen and numeric keypad. The card, which is the size of a normal credit card, includes an LCD screen and a tiny keyboard, powered by a battery. When shopping online or logging in to an online banking service, the cardholder will need to *i*) press the Verified by *Visa* option button on the card's keypad; and *ii*) enter a PIN number using the keypad. A unique one-time-code will then appear on the card's display, to be used by the cardholder for authentication online.

Moreover, in order to prevent and mitigate security breaches and losses, a number of technical measures have been developed by industry to help enhance confidence. These include tamper-resistant

chips on payment cards and the use of sophisticated encryption techniques, limits on the amount of value that can be stored on consumers' electronic devices and limits on the value of transactions and use of a PIN code for authorising payments.

Further, as part of the authentication process, online retailers and banks are increasingly using more efficient fraud detection tools that make cards more secure when shopping online. These include both automated and manual fraud detection tools. In the United States and Canada, in 2009, some 97% of online merchants used one or more automated validation tools (generally provided by card networks) to help authenticate cards and cardholders. Automated order-screening systems are also widely used to help evaluate incoming orders in real time. For example, in the event an order exceeds a certain amount, or the shipping and billing addresses do not match, the order is flagged as potentially fraudulent and placed into a review queue in the merchant's management system for further inspection. In addition, most merchants carry out manual fraud reviews for some of their orders, following the initial automated screening phase. While 1 out of 4 online orders have been subject to manual fraud reviews on average in the United States and Canada, such processes can be quite expensive for merchants (OECD, 2011*b*).

As regards authentication in mobile payments, there is some debate as to whether a mobile phone number should be used to identify the payer and the payee in a mobile payment transaction. A large volume of transactions is based on SMS for which only the device's PIN-code access is required.

Age verification

Children are actively engaged in purchasing products online and through their mobile devices without always appreciating the associated risks, and despite the fact that in most countries they do not have the legal right to enter into commercial transactions. One way to protect them is to ensure that their age and identity is verified online prior to making a purchase. Research indicates that this is rarely done, with one report pointing out that 76% of purchases made using mobile devices do not require any age verification step (Consumer Focus, 2009, p. 47). Even where such steps are included, unlike face-to-face transactions, it can be relatively easy for children to pose as adults online. The need for effective age verification systems is highlighted in the OECD 2008 policy guidance (OECD, 2008*c*). It should be noted, however, that age verification tools may not provide the only way to effectively protect children in online and mobile payments. At the 2009 OECD e-commerce conference, stakeholders recognised the shared responsibility between parents, e-commerce, and mobile service providers and payment organisations, in educating and raising awareness among children about the potential risks associated with online and mobile purchases and ways to protect themselves against those threats.

Consumer knowledge and skills

With rapid technological changes, consumers may also not be able to evaluate risks and to know how best to guard against fraud and preserve security. Education and awareness can help to address this. Such a need has been repeatedly pointed out in the 1999 guidelines (Section VIII, Part II), the OECD policy guidance on, respectively, online identity theft (OECD, 2008*b*), and mobile commerce (OECD, 2008*c*) as well as the OECD recommendations on consumer education (OECD, 2009*b*, Annex II).

In its 2002 report, the CCP highlighted the need for enhanced consumer education about, specifically, the use and safety of credit and debit cards online (OECD, 2002). According to a report (EC, 2008, p. 27), consumers' capacity to protect themselves from payment fraud and related security threats should not be overestimated. Consumers, and, in particular, children and other vulnerable or disadvantaged consumers, oftentimes do not know how to stay safe online, despite numerous consumer education and awareness campaigns. More may need to be done to ensure that education is being provided to consumers and that such education is understood and acted on. The 2004-2007 EU *Action Plan to prevent fraud on non-cash*

means of payment in that regard recommends that individuals be provided with clearer information on payment security, while merchants should themselves be given improved educational material and adequate tools to protect themselves from data breaches (EC, 2007*b*). Research further suggests that consumers should be much better informed about security risks affecting mobile payments (Consumer Focus, 2009, p. 9). There are, however, limits to the effectiveness of awareness and education initiatives. Consumers oftentimes do not know how to stay safe online, despite numerous education and awareness campaigns (OECD, 2010*a*, p. 24).

Interoperability, payment choice, and cross-border e-commerce

Consumer use of online payments schemes varies among countries and regions. In Western Europe, a large majority of consumers pay for online purchases by credit or debit card. In Germany direct debit is the main form of payment. According to a 2010 report, "while in the Netherlands, the online banking payment method *iDEAL* takes a prominent position, Danes pay with their debit card, the French by credit card, and Eastern Europeans primarily by cash-on-delivery" (Innopay, 2010). The difference in the payment methods across countries has been identified as one of the barriers slowing the growth of cross-border e-commerce. As regards mobile payments in Europe, a lack of open standards for interoperability between card issuers and mobile network operators has been identified by the European Payments Council (EPC) as a major barrier to successful commercial deployments (EPC, 2010*a*, p. 52). To address the problem, the EPC is working with the GSMA on harmonising payments standards across the region.

Enhanced interoperability of payment mechanisms, technology, and systems is regarded as essential to help facilitate cross-border e-commerce. According to a survey conducted in 2010, online merchants in the United Kingdom willing to sell products across borders could not do so due to the multitude of payment systems used across EU countries. Merchants indeed need to accept multiple payment methods, including those from Visa Inc., MasterCard Worldwide, MasterCard's Maestro debit system, American Express Co., direct debit, *ELV* in Germany, and *iDeal* in the Netherlands (The Internet Retailer, 2010*d*). As a result, consumer choice online is inhibited by a continuing lack of merchant acceptance of means of payments. Most merchants selling across borders require payments through internationally accepted credit and debit cards.

Another industry initiative has been launched to promote interoperable online banking payments systems across countries. Under the *Online Banking Enabled e-Payments* (OBeP) scheme, a consumer who wishes to purchase goods or services does not have to provide financial information to an online merchant. Rather, at the time of payment, the consumer is redirected to the bank site of the consumer. The consumer is then presented with details of the transaction and confirms an instruction to the bank to make a payment to the nominated merchant. Efforts are underway to expand the scope of the OBeP scheme, through the development of global standards. An International Council of Payment Network Operators (ICPNO) has been established to build the framework and establish the rules and standards for joining the global OBeP networks. Key issues such as technology, international settlement, legal compliance, security, communications, fee structures and exchange rate mechanisms are to be examined.

In addition, partnerships have been established among companies across countries to help boost cross-border e-commerce. An alliance was for example launched between *Taobao* and *Yahoo! Japan* in June 2010 to facilitate cross-border purchases between Japanese and Chinese consumers (Box 4).

Box 4. Yahoo!Japan Corp. and Taobao China's Cross-Border E-Commerce Alliance

On 1 June 2010, *Yahoo!Japan Corp*. and *Taobao* in China began operating complementary online shopping services, which enables Japanese consumers to purchase products from Chinese merchants and Chinese consumers to purchase products from Japanese merchants. Under the joint scheme, which aims to help eliminate cross-border e-commerce barriers (such as language, regulatory complexity, delivery logistics, and payment issues):

- Japanese consumers can buy products from *Taobao* merchants in China through *Yahoo!Japan* China Mall *(http://chinamall.yahoo.co.jp),* a new website opened within Yahoo! Japan, and
- Chinese consumers can buy products from *Yahoo!Japan* through the new *TaoJapan (http://japan.taobao.com)* website opened as part of *Taobao*.

A similar partnership was launched in 2008 between *Alipay* (a payment service provider owned by the China's largest e-commerce platform *Alibaba*) and *Paymate* (a payment service provider in Australia). Moreover, in July 2010, a Memorandum of Understanding (MoU) was signed between some Korean and Japanese companies to enable consumers to purchase products from merchants in both countries. Under the MoU, consumers will be able to download a mobile payment application onto their smart phone, which will be equipped with NFC technology.

IMPLICATIONS FOR CONSUMER POLICY

The consumer challenges discussed above have policy implications for a number of areas. These were discussed by the committee with business and civil society as the work progressed, including at a workshop held in April 2011. The issues are discussed below. The assessment is serving as a basis for the development of policy guidance in the area of online and mobile payments.

Clarity, transparency and completeness in information disclosure

The terms and conditions of transactions and related payments details and procedures may not always be easy for consumers to access, read, retain, and preserve.

Online and remote mobile transactions often take place in an "on the go" context that might affect consumers' decision making. As a result, consumers may not be able to easily access, read, review and/or preserve the terms before making a payment. In addition, the terms and conditions in online contracts are often provided in small print and/or in scrolling text boxes. Key payment-related information is sometimes buried in footnotes or requires accessing additional windows. Disclosure problems may be exacerbated in the mobile payments environment due to mobile devices' small screens and limited processing capacity, and battery life. It is worth noting, however, that the situation might be changing with growing consumer use of mobile devices, such as smart phones and tablet computers, which have larger screens, greater memory, and expanded functionalities.

Key information on consumer rights and potential liabilities associated with online and mobile payments is not always provided to consumers in a clear, timely, and transparent manner.

Section III of the 1999 guidelines pertaining to online disclosures provides a list of key information items that should be provided to consumers at the time of a sale. Many of the items relate in one way or another to payments. In practice, the information provided is often presented in technical and lengthy terms that are difficult for consumers to use and understand. In other cases, information is not provided until the latter stages of the payment process. Moreover, it is often not clear which of the entities involved in a payment transaction should be providing information to consumers, what type of information they should provide, and when, during the payment process, they should be doing so.

A number of ways to improve information on payment systems and areas linked to payments were discussed by stakeholders at the payments workshop. A number of participants called for better information on how consumers could opt-out or cancel purchases. Others suggested that information on delivery times, any rights of withdrawal and available dispute resolution and redress mechanisms (including online and alternative dispute resolution programmes) should be provided to consumers prior to making a payment. In the event of problems with a transaction, clear information on whom to contact, and how, should also be available to consumers, by phone, for example, or through a link to a website accessible through the merchant's e-commerce platform. It was further suggested that more should be done to make consumers who are purchasing online subscriptions, aware of the fact that initial rates may only be applicable for a limited time period. In addition, better information is needed to be provided to consumers on the product add-ons that they may, sometimes unwittingly, be buying, and the pricing of such add-ons.

Variability in regulatory and protection regimes

Consumers engaging in online and mobile commerce may not fully understand which regulations apply to a payment transaction and how these may differ, depending on the payment method and platform used, the parties involved in the payment transaction, and the nature of the product purchased.

The lack of understanding results from the fact that a number of financial and non-financial institutions may be involved in a given payment transaction, including banks and cards networks, alternative payment providers, such as mobile network operators, and other non-bank institutions operating on the Internet. Their operations are often overseen by different regulatory bodies, which operate under different sets of regulations. Consumers may therefore find it difficult to determine: *i)* what redress rights they have (relating to correction of orders, returns, exchanges or refunds); *ii*) which entity to turn to if there is a payment-related problem; and *iii)* which regulatory body to appeal to if a problem cannot be resolved with a merchant directly. The situation is even more complex when transactions are cross-border.

There appears to be general agreement that the situation could be improved by informing and educating consumers more effectively about their rights and responsibilities and applicable rules. Some stakeholders, however, have proposed that additional actions be taken to rationalise and simplify the regulatory environment. This has been done in some countries, where generic consumer protection rules have been applied along with self- and co-regulatory initiatives.

Mobile commerce is a particular concern for some. The mobile marketplace is still nascent in many countries and payments providers have cautioned that introducing new regulations might be premature and have unintended, adverse effects on mobile development. In ensuring a level playing field for all payment providers, policy makers should ensure that any initiatives neither slow down innovation nor limit competition.

Consumers engaging in online and mobile commerce do not benefit from the same level of protection when using different payment mechanisms within jurisdictions, which can complicate obtaining redress when a problem arises. In addition, protection regimes differ from country-to-country, which could discourage cross-border transactions.

Payment protection and rights vary, within and across countries, depending on: *i*) the payment methods being used (*e.g.* credit/debit card, pre-paid, mobile phone bill); *ii*) the nature of a problem (*e.g.* unauthorised charges, fraud, delivery and/or conformity); *iii*) the nature of a product purchased (*e.g.* goods and services may be treated differently, as could tangible and intangible products); and *iv*) the payment providers that are involved (alternative payments providers, such as mobile network operators and other non-financial institutions, may fall outside the scope of some regulatory frameworks, given their non-bank status in some jurisdictions).

Discussions among stakeholders suggest that, at the very least, consumers should be better informed about the protection levels available when they use different payment mechanisms. Strengthening education and awareness is seen as helping in this regard. Beyond this, some stakeholders support the idea of establishing a minimum level of consumer protection that would apply no matter what payment mechanism is being used within a jurisdiction. The minimum level of protection could be established by laws and regulations or be less formal. The establishment of such minimum level of protection would not, however, prevent payment providers from offering additional protection; this flexibility was seen by some as necessary for maintaining competition and enabling consumers to have a choice. How the situation could be improved across borders is seen as more complex; convergence of systems could be helpful, but difficult to pursue from a practical standpoint.

Fraudulent, misleading and deceptive commercial practices

Fraudulent, misleading and deceptive commercial practices associated with online and mobile payments are ongoing challenges that can cause consumer harm and may undermine consumer confidence more broadly, within and across jurisdictions.

Online and mobile transactions are sometimes different from those made *via* traditional retail outlets: *i)* consumers often cannot validate the identity and integrity of vendors; *ii)* consumers often cannot inspect products prior to making a purchase; and *iii*) while the conclusion of an online or mobile commerce transaction may be done quickly, consumers are not always in a position to understand the terms and conditions or to think thoroughly before acceptance. In some cases, the opportunities for and risks of fraudulent, misleading and deceptive practices are seemingly much higher for certain types of online and mobile commerce transactions, particularly when the vendors involved are remote and do not have established track records. The challenges, it should be noted, do not apply to all mobile payments as mobile devices employing near field communication (NFC) technology are also being used to make payments for products purchased in traditional retail settings.

Regardless of the payment context, there is general agreement that protection against fraud is a shared responsibility between payment providers and merchants. The latter should in particular ensure that their e-commerce systems are adequate, transparent, and safe. Some stakeholders have suggested putting in place tools to reinforce protection; these include escrow accounts whereby payment is processed only if the consumer receives the good ordered. In addition, effective dispute resolution processes and vigorous efforts against rogue traders could, it was noted, contribute significantly to building consumer confidence. Some countries have already taken measures in this regard, implementing regulations, for example, that limit consumer liability in the case of fraud.

Dispute resolution and redress

The multiplicity of parties that can be involved in a payment transaction can make it difficult for consumers to understand whom to turn to in case of problems.

Stakeholders have suggested that it may be beneficial for payment providers, merchants, and other parties involved in a payment transaction to work together to ensure that consumers are provided with clear and complete information on whom a consumer should contact in the case of a problem with a payment transaction and whom the consumer should contact in the case of a problem with the underlying product or service purchased or used.

Discussion among stakeholders suggests that payment providers could work jointly with merchants and other stakeholders to develop effective dispute resolution and redress systems.

Other issues

Many consumers are hesitant to engage fully in e-commerce via online and mobile payments mechanisms because of concerns about the security of the payments systems.

Consumer concerns about security are likely to inhibit their online and mobile activities, whether or not the concerns have merit. Greater awareness of the actions businesses have taken to ensure security would help to dispel any misperceptions, as would education aimed at enhancing knowledge of what consumers could do to avoid compromising their financial and personal information. Some stakeholders noted that related educational initiatives need to be taken with merchants so that they are better prepared to deal with emerging security threats. Much continues to be done to address issues from a technological perspective. These include security keys that generate random numbers that are then sent to a user through

SMS, or tokens to connect with a user ID and password, as well as e-mail identification and authentication applications which may be downloaded to determine whether an e-mail received from a payment provider is genuine.

There is concern among stakeholders over the challenges that online and mobile payment systems may present for vulnerable and disadvantaged consumers (especially children).

One of the principal concerns is that of parents, with respect to the activities of their children in the digital environment. In some countries, use of smart mobile devices by children has expanded significantly, reflecting a growing preference for using them instead of their computers. This has exposed them to payment-related challenges that they are not always able to understand. A number of recent episodes reported widely in the media have shown that children can easily engage in expensive transactions using mobile devices without the direct knowledge or consent of their parents. The growing sophistication, power and complexity of mobile devices is a contributing factor as many parents are simply unaware of and/or do not comprehend what their children can do with their mobile devices (including, for example, paying for the purchase of virtual goods or services without a credit card). Solutions, which include age identification technologies and spending limits, can however be elusive given the dynamism of the technologies involved and market developments.

More generally, there is recognition of the need to protect and educate vulnerable or disabled consumers including the elderly and specific societal groups which may be particularly susceptible to deceptive commercial practices or have difficulties fully understanding payment mechanisms.

There are a variety of payment means and platforms in place within and across jurisdictions which are sometimes not interoperable; this can discourage consumers from engaging in online and mobile commerce.

Within countries, some payment means may not be accepted by merchants for technical or commercial reasons. The problem is exacerbated at the international level, where, in some instances, consumers located in one country are unable to use their payment card to purchase a product from a merchant located in another country.

REFERENCES

Australian Competition and Consumer Commission (ACCC) (2010), *Online shopping - When Things Go Wrong*, *www.accc.gov.au/content/index.phtml/itemId/268478,* accessed on 6 January 2011.

Bank of Finland (2003), *Card, Internet and Mobile Payments in Finland*, Financial Markets Department, March 2003, *http://129.3.20.41/eps/dev/papers/0405/0405004.pdf.*

Bank of Japan (2009), *Developments in Electronic Money in Japan during Fiscal 2008*, Payments and Settlement Systems Department, 24 August 2009, at: *www.boj.or.jp/en/type/ronbun/ron/research07/data/ron0908b.pdf.*

BBA (British Bankers' Association) (UK) (2008), *UK Banking Code*, March 2008, *www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf.*

BILETA (2002), *Enhancing Consumer Confidence in Electronic Commerce: Consumer Protection in Electronic Payments*, 17th BILETA Annual Conference, at: *www.bileta.ac.uk/Document%20Library/1/Enhancing%20Consumer%20Confidence%20in%20Electronic%20Commerce%20-%20Consumer%20Protection%20in%20Electronic%20Payments.pdf.*

Bin Tang - YeePay CEO (2009), *Innovations in China's e-Payment Market*, November 2009, at: *http://iis-db.stanford.edu/docs/189/epayment_bin_tang.pdf.*

Capgemini (2010), *World Payment Report 2010*, 19 October 2010, *www.fr.capgemini.com/ressources/publications/le-world-payment-report-2010/.*

China Daily (2010), *Third Party Payments Regulated*, 22 June 2010, *www.chinadaily.com.cn/bizchina/2010-06/22/content_10001206.htm.*

CISCO (2008), *Consumer Online Shopping and Payment Experience Shape In-store Expectations, Cisco Internet Business Solutions* (IBSG) Primary Research, September 2008, at: *www.aboutcisco.biz/web/strategy/docs/finance/ConnectedPaymentsExecSummary_092208.pdf.*

Credit Union Times (2010), *Additional Consumer Protection Strategy is Launched by Visa*, 12 May 2010, *www.cutimes.com/Issues/2010/May-12-2010/Pages/Additional--Consumer-Protection-Strategy-Is-Launched-by-Visa.aspx.*

Consumer Focus (2009), *Pocket Shopping*, Consumer Focus, December 2009, at: *www.consumerfocus.org.uk/assets/1/files/2009/06/Pocketshopping.pdf.*

Court of Justice of the European Union (CJEU) (2010), *Verbraucherzentrale Nordrhein-Westfalen eV v. Handelsgesellschaft Heinrich Heine GmbH*, Case C-511/08, in Official Journal of the European Union C 148, dated 5 June 2010, p. 6, *http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:148:0006:0007:EN:PDF.*

CSN (Consumer Sentinel Network) (2010), *Data Book for January-December 2009*, US Federal Trade Commission, February 2010, *www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.*

CyberSource (2010), *Online Fraud Report*, 11th Annual Edition, 2010, *http://forms.cybersource.com/forms/FraudReport2010NACYBSwwwQ109*.

Directive 2000/31/EC of the European Parliament and the Council on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (E-commerce Directive), 8 June 2000, Brussels, Belgium, Official Journal (OJ) L 178, p. 1-16, 17 July 2000, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT*.

Directive 2007/64/EC of the European Parliament and of the Council on Payment Services in the Internal Market (PSD), 13 November 2007, Brussels, Belgium, OJ L 319, p. 1-36, 5 December 2007, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML*.

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions (E-money Directive), Brussels, Belgium, OJ L 267, 10 October 2009, p. 7-17, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF*.

Directive 2011/83/EU of the European Parliament and of the Council, 25 October 2011 on Consumer Rights (Directive on consumer rights), Brussels, Belgium, Official Journal of the European Union L 304/64, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:EN:PDF*.

Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), Public Law 111-203, H. R. 4173, Washington, D.C., United States of America, 21 July 2010, *www.gpo.gov/fdsys/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf*.

EC (European Commission) (2007), *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol - A new EU Action Plan 2004-2007 to Prevent Fraud on Non-Cash Means of Payment*, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0679:EN:NOT*.

EC (2008*a*), *Key Challenges for Consumer Policy in the Digital Age, Roundtable on Digital Issues*, Speech by Meglena Kuneva, London, 20 June 2008, *http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/347*.

EC (2008*b*), *Report on Fraud regarding Non-Cash Means of Payments in the EU: the Implementation of the 2004-2007 EU Action Plan*, Commission Staff Working Document, SEC(2008)511, Brussels, 22 April 2008, *http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf*.

EC (2011), Preliminary findings from a *Market Study on the Functioning of E-commerce in Goods,* presentation provided at the OECD *Workshop on Consumer Protection in Online and Mobile Payments*, held on 15 April 2011 at the OECD in Paris.

EC (2012*a*), *Green Paper Towards an Integrated European Market for Card, Internet and Mobile Payments*, Brussels, 11 January 2012, COM(2011)941 final, *http://ec.europa.eu/internal_market/consultations/docs/2012/cim/com_2011_941_en.pdf*.

EC (2012*b*), *Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Coherent Framework for Building Trust in the Digital Single Market for E-commerce and Online Services*, Brussels, January 2012, COM(2011)942, *http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/COM2011_942_en.pdf*.

ECC-Net (European Consumer Centre Network) (2008), *The European Online Marketplace: Consumer Complaints 2007*, May 2008, *http://ec.europa.eu/consumers/redress_cons/docs/ECC_E-commerce_report.pdf.*

E-commerce News (2010), *Report Finds Disconnect Between Alternative Payment Preferences and Offerings*, 22 October 2010, *http://ecommercejunkie.com/2010/10/22/report-finds-disconnect-between-alternative-payment-preferences-and-offerings/.*

European E-Commerce and Mail Order Association (EMOTA) (2010), *Trustmark Schemes Across Europe*, *www.emota.eu/consumer-trust.html.*

EPC (European Payments Council) (2010*a*), *White Paper on Mobile Payments*, 1st Edition, 18 June 2010, Brussels, *www.europeanpaymentscouncil.eu/documents/EPC492-09%20White%20Paper%20Mobile%20Payments%20version%202.0%20finalrev.pdf.*

EPC (2010*b*), *Driving Forward the SEPA Vision*, Annual Report 2009, *www.europeanpaymentscouncil.eu/documents/EPC050-10%20EPC%20Annual%20Report%20v%201.0%20final.pdf.*

EPC (2011), *Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines*, 16 November 2011, Brussels, EPC Secretariat, www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=EPC178-10 v2.0 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines.pdf.

Facebook (2009), *Spare Change*, frequently asked questions, *http://apps.facebook.com/sparechange/buyerFAQ.action?page=buyerFAQ*, accessed on 6 January 2011.

KPMG (2007), *Mobile Payments in Asia Pacific*, 2007, *www.kpmginsiders.com/pdf/Mobile_payments.pdf.*

Federal Reserve Bank of Boston (FRBB) (2010*a*), *Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects*, 17 May 2010, Marianne Crowe, Marc Rysman, and Joanna Stavins, *www.pymnts.com/mobile-payments-in-the-united-states-at-retail-point-of-sale-current-market-and-future-prospects/?hpb.*

FRBB (2010*b*), *The Mobile Payment Landscape*, presentation by Marianne Crowe, 23 February 2010, *www.bosfed.org/economic/cprc/presentations/2010/Crowe022310.pdf.*

FATF (Financial Action Task Force) (2006), *Report on New Payment Methods*, 13 October 2006, OECD, Paris, *www.fatf-gafi.org/dataoecd/30/47/37627240.pdf.*

FATF (2008), *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, 18 June 2008, OECD, Paris, *www.oecd.org/dataoecd/57/21/40997818.pdf.*

FeliCa (2010), *A Message from our President*, *www.felicanetworks.co.jp/en/company/message.html*.

Forrester Research (2009), *Western European Online Retail and Travel forecast 2008-2014*, March 2009, referred to by *Les Echos*, 12 June 2009, *www.lesechos.fr/medias/2009/0612//300355565.pdf.*

Forrester Research (2010), *US Consumers Continue To Show Limited Interest in Mobile Payments*, 20 October 2010, *www.internetretailer.com/2010/10/20/consumers-are-mobile-companies-still-have-catching-do*.

FCC (Federal Communications Commission (US) (2011), *FCC Proposes Rules to help Consumers Identify and Prevent "Mystery Fees" on Phone Bills, Known as "Cramming,"* news release, 12 July 2011, *http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0712/DOC-308351A1.pdf.*

FTC (Federal Trade Commission) (US) (2003), *A Consumer Guide to E-Payments*, March 2003, *www.ftc.gov/bcp/edu/pubs/consumer/tech/tec01.shtm*.

FTC (2008), *"Free Software CD" Internet Operation Settles FTC Charges*, Press Release, 11 June 2008, *www.ftc.gov/opa/2008/06/manay.shtm.*

Gigaom (2011), *Mobile payments worth $670 billion by 2015*, by Ryan Kim, 5 July 2011, *http://gigaom.com/2011/07/05/mobile-payments-worth-670-billion-by-2015/.*

GSM Association (GSMA) (2010), *New Report Predicts Explosive European Growth for Mobile Broadband*, 12 January 2010, *www.gsmworld.com/newsroom/press-releases/2010/4549.htm.*

Innopay (2010), *Online Payments 2010, Increasingly a Global Game*, May 2010, *www.innopay.com/index.php/plain/ezfileshop/download/8634/5D6E5FEC12426FC50C53C82A6EB03ECBCA18F4F2.*

Innopay (2011), *Mobile Payments 2012, My Mobile, My Wallet?*, September 2011, *http://www.innopay.com/publications/mobile-payments-2012-my-mobile-my-wallet.*

Internet Retailer (2010*a*), *Credit Cards Are Losing Some Luster with Online Shoppers*, 19 February 2010, *www.internetretailer.com/2010/02/19/credit-cards-are-losing-some-luster-with-online-shoppers.*

Internet Retailer (2010*b*), *Credit Card Rules Change*, 4 October 2010, *www.internetretailer.com/2010/10/04/credit-card-rules-change*.

Internet Retailer (2010*c*), *US M-Commerce Sales to Hit $2.4 Billion This Year, ABI Research Predicts*, 1 March 2010, *www.internetretailer.com/2010/03/01/u-s-m-commerce-sales-to-hit-2-4-billion-this-year-abi-researc.*

Internet Retailer (2010*d*), *U.K. Retailers Feel Ill-Prepared to Handle International Payments*, 8 July 2010, *www.internetretailer.com/2010/07/08/uk-online-merchants-face-variety-payment-schemes.*

Javelin Research (2010), *Online Retail Payments Forecast 2010 – 2014*, February 2010, *https://www.javelinstrategy.com/uploads/files/1005.P_OnlineRetailPaymentsForecastSampleReport.pdf.*

Juniper Research (2010), *Mobile Payment Transactions to Double in Value to 200 billion USD by 2012*, Press Release, 16 June 2010, *www.juniperresearch.com/viewpressrelease.php?pr=190.*

M's Communicate (2010), *Denshi Money*, *www.emscom.co.jp/report_detail_76.html* (in Japanese only).

MacCarthy, Mark & Hillebrand, Gail (2010), *Viewpoint: Mobile Payments Call For Clear Consumer Protections*, American Banker, 10 August 2010, *http://www.americanbanker.com/issues/175_152/vp-hillebrand-mobile-protections-1023818-1.html.*

McAfee (2008), *Mobile Security Report 2008*, February 2008, *www.mcafee.com/us/research/mobile_security_report_2008.html*.

Mallat, Niina (2007), *Exploring Consumer Adoption of Mobile Payments - A Qualitative Study,* Niina Mallat, Helsinki School of Economics, 2007, at: *http://portal.acm.org/citation.cfm?id=1322013*.

Marketwire (2010), *China's Digital Generations 2.0: Digital Media and Commerce Go Mainstream*, Boston Consulting Group report, 6 May 2010, at: *www.marketwire.com/press-release/Explosive-Growth-Internet-Use-Is-Fundamentally-Changing-Chinas-Economy-Society-Says-1160501.htm.*

Microsoft (2009), *Mobile Payments*, *White Paper*, Microsoft, September 2009, at: *www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9997243d-5f1b-405b-b0cb-f14ecdfb8566.*

Mobey Forum (2010), *Mobile Remote Payments General Guidelines for Ecosystems, White Paper*, June 2010, *www.mobeyforum.org/files/Remote%20Payments%20White%20Paper%20FINAL.pdf.*

Mopay (2010), *Mopay Becomes the First Provider to Enable Mobile Payments for the Purchase of Physical Goods Around the Globe*, Press Release, 18 May 2010, *http://mopay-inc.com/fileadmin/templates/mindmatics/images/pressreleases/en/20100518_PM_physical_goods.pdf.*

Morgan Stanley (2010), *Internet Trends*, presentation at the CM Summit, New York, 7 June 2010, *www.morganstanley.com/institutional/techresearch/pdfs/MS_Internet_Trends_060710.pdf.*

New York Times (2010), *PayPal Hopes Open Platform Will Spur Innovation*, Claire Cain Miller, 21 October 2009, Web 2.0 Summit, San Francisco, at: *http://bits.blogs.nytimes.com/2009/10/21/paypal-hopes-open-platform-will-spur-innovation/.*

NFC Times (2010), *Report: Japan's M-Payment Players Discover that Points Count*, 11 June 2010, *www.nfctimes.com/news/report-japan-s-m-payment-players-discover-points-count.*

Nomura Research Institute (2010), *Denshi Money Ni Kansuru Aanketo Chosa*, August 26 2010, *www.nri.co.jp/news/2010/100826.html* (in Japanese only).

Noone, Claire (2011), *Consumer Policy Challenges: Regulatory Frameworks*, presentation provided at the OECD Workshop on *Consumer Protection in Online and Mobile Payments* held on 15 April at the OECD in Paris.

OECD (Organisation for Economic Co-operation and Development) (1998), *A Borderless World: Realising the Potential of Global Electronic Commerce*, Ottawa, Canada, *SG/EC(98)14/FINAL* www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final .

OECD (1999), *Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, Paris, 1999, *www.oecd.org/dataoecd/18/13/34023235.pdf.*

OECD (2002), *Consumer Protection for Payment Cardholders [DSTI/CP(2001)3/FINAL], OECD, Paris, 2002, at: www.olis.oecd.org/olis/2001doc.nsf/LinkTo/NT0000099E/$FILE/JT00128255.PDF*.

OECD (2005), *Consumer Dispute Resolution and Redress in the Global Marketplace*, OECD, Paris, 2005, *www.oecd.org/dataoecd/26/61/36456184.pdf.*

OECD (2006), *Online Payment Systems for E-commerce*, [DSTI/ICCP/IE(2004)18/FINAL], OECD, Paris, 2006, at: *www.oecd.org/dataoecd/37/19/36736056.pdf.*

OECD (2007*a*), *OECD Policy Guidance and Recommendation on Electronic Authentication*, OECD, Paris, June 2007, *www.oecd.org/dataoecd/32/45/38921342.pdf.*

OECD (2007*b*), *OECD Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, 2007, *www.oecd.org/dataoecd/43/50/38960101.pdf.*

OECD (2007*c*), *Mobile Commerce*, OECD, Paris, 2007, *www.oecd.org/dataoecd/22/52/38077227.pdf.*

OECD (2008*a*), *Scoping Paper on Online Identity Theft*, *www.oecd.org/dataoecd/35/24/40644196.pdf.*

OECD (2008*b*), *Policy Guidance on Online Identity Theft*, OECD, Paris, 2008, *www.oecd.org/dataoecd/49/39/40879136.pdf.*

OECD (2008*c*), *OECD Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce*, OECD, Paris, 2008, *www.oecd.org/dataoecd/50/15/40879177.pdf.*

OECD (2008*d*), *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, OECD, Paris, 2008, *https://www.eid-stork.eu/dmdocuments/public/TheRoleOfeIDMInTheInternetEconomyJune2009.pdf.*

OECD (2009*a*), *Conference on Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy, Background Report*, OECD, Paris, 2009, *www.oecd.org/dataoecd/44/13/44047583.pdf.*

OECD (2009*b*), *Consumer Education, Policy Recommendations of the Committee on Consumer Policy*, OECD, Paris, October 2009, *www.oecd.org/dataoecd/32/61/44110333.pdf*.

OECD (2010*a*), *Consumer Policy Toolkit*, OECD, Paris, July 2010, *www.oecd.org/sti/consumer-policy/toolkit*.

OECD (2010*b*), *Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy, Summary of Key Points and Conclusions*, OECD, Paris, 2010, *www.oecd.org/dataoecd/32/10/45061590.pdf.*

OECD (2010*c*), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, Workshop Summary, OECD, Paris, 2010, *www.oecd.org/dataoecd/8/59/45997042.pdf.*

OECD (2011*a*), *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them,* OECD, Paris, 2011, *www.oecd-ilibrary.org/docserver/download/fulltext/5kgcjf71pl28.pdf?expires=1312971854&id=id&accname=guest&checksum=A6DFC0B52932638891E80E50EEEBE52B.*

OECD (2011*b*), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD, Paris, 2011, *www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2010)11/FINAL&docLanguage=En.*

OECD (2011*c*), *OECD Guide to Measuring the Information Society 2011*, OECD, Paris, 2011, *www.oecd.org/sti/measuring-infoeconomy/guide.*

OECD (2011*d*), *Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy, Guidance for Government Policy Makers*, OECD, Paris, 2011, *www.oecd-ilibrary.org/docserver/download/fulltext/5kg1zqsm3pns.pdf?expires=1326713300&id=id&accname=guest&checksum=DAC8875B63BCBC385A6F62897698F741.*

OFT (Office of Fair Trading) (2010*a*), *E-Consumer Protection, A Public Consultation on Proposals*, July 2010, *www.oft.gov.uk/shared_oft/consultations/eprotection/oft1252con.pdf.*

OFT (2010*b*), *Attitudes to Online Markets*, report by FDS International for the OFT, August 2010, *www.oft.gov.uk/shared_oft/consultations/eprotection/oft1253.*

OFT (2010*c*), *Investigation into an Online Retailer relating to Non-Delivery of Orders and Failure to Provide Refunds*, case closed in December 2009, *www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-completed/shop4tek/.*

Payments Council (UK) (2010), *The Way We Pay 2010*, *www.paymentscouncil.org.uk//files/payments_council/the_way_we_pay_2010_final.pdf.*

Payments Administration (UK) (2010), *Card Fraud Facts and Figures*, *www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/.*

PayPal (2010), *User Agreement*, 2010, https://cms.paypal.com/us/cgi-bin/marketingweb?cmd=_render-content&fli=true&content_ID=ua/BuyerProtComp_full&locale.x=en_US.

Report Linker (2010), *China Mobile Payment Survey Report, 2010*, *www.reportlinker.com/p0318794/China-Mobile-Payment-Survey-Report.html.*

Senate (US) (2009), *Aggressive Sales Tactics on the Internet and their Impact on American Consumers*, Committee on Commerce, Science and Transportation, Staff Report for Chairman Rockefeller, 16 November 2009, *http://commerce.senate.gov/public/?a=Files.Serve&File_id=594bd7e1-c14b-42ac-b473-0ef90330efea.*

The Paypers (2010*a*), *Mopay Enables Mobile Payments for the Purchase of Physical Goods,* 19 May 2010, *www.thepaypers.com/news/mobile-payments/mopay-enables-mobile-payments-for-the-purchase-of-physical-goods/741247-16.*

The Paypers (2010*b*), *Virtual Goods: the Next Big Opportunity in the US?*, Vol. 3, Issue 11, 7 June 2010,.

The Paypers (2010*c*), *Alipay Reaches 500 Million User Milestone*, 26 November 2010, www.thepaypers.com/news/online-payments/alipay-reaches-500-million-user-milestone/742633-3.

The Paypers (2010*d*), *Mobile Payments Surge in China*, 31 May 2010, www.thepaypers.com/news/mobile-payments/mobile-payments-surge-in-china/741312-16.

The Paypers (2010*e*), *Russian Government Approves E-Payment Bill*, 19 November 2010, www.thepaypers.com/news/online-payments/russian-government-approves-e-payment-bill/742567-3.

Ramezani, Elham (2008), *Mobile Payment*, June 2008, *http://webuser.hs-furtwangen.de/~heindl/ebte-08-ss-mobile-payment-Ramezani.pdf.*

Roth, Daniel (2010), *The Future of Money, It's Flexible*, wired.com, 31 May 2010, *www.wired.com/magazine/2010/02/ff_futureofmoney/all/1.*

Sage (UK) (2009), *68% of Online Retailers Admit Payment Fraud Threatens Business Growth*, 19 May 2009, *www.sage.co.uk/press_office/payment_fraud.aspx.*

Simon Fraser University (2006), *Privacy Rights and Prepaid Communication Services: A Survey of Prepaid Mobile Phone Regulation and Registration Policies among OECD Member States*, Research report for the office of the privacy commissioner of Canada, March 2006, *http://www.sfu.ca/cprost/prepaid/docs/Gow-PrivacyRightsAndPrepaidCommunicationServices.pdf.*

TACD (Trans Atlantic Consumer Dialogue) (2009), *Resolution on E-commerce*, December 2009, *http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=260&Itemid.*

UNCITRAL (United Nations Commission on International Trade law) (2010*a*), *Possible future work on online dispute resolution in cross-border electronic commerce transactions*, Note by the Secretariat, Forty-third session, New York, 21 June-9 July 2010, *www.underhills.us/Docs/PDFS/UNCITRAL-Possible_future_work_online_dispute_resolution_in_cross-border_e-commerce.pdf.*

UNCITRAL (2010*b*), *Report of Working Group III (Online Dispute Resolution) on the work of its twenty-second session (Vienna, 13-17 December 2010)*, *http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V11/801/48/PDF/V1180148.pdf?OpenElement*.

UNCITRAL (2011), *Report of Working Group III (Online Dispute Resolution) on the Work of its Twenty-Third Session*, New York, 23-27 May 2011, *http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V11/834/61/PDF/V1183461.pdf?OpenElement.*

UNCTAD (United Nations Conference on Trade and Development) (2009), *Information Economy Report 2009*, New York and Geneva 2009, *http://unctad.org/en/docs/ier2009_en.pdf.*

Virtual Goods News (2010), *Boku Takes $25M Series C Round*, 19 January 2010, *www.virtualgoodsnews.com/2010/01/boku-takes-25m-series-c-round.html.*

Visa Europe (2009), *Annual Report 2009*, www.visaeurope.com/en/about_us/annual_report.aspx.