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

28-Mar-2014

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY

CONSUMER POLICY GUIDANCE ON MOBILE AND ONLINE PAYMENTS

JT03355276

DSTI/CP(2011)24/FINAL
Unclassified
English - Or. English

FOREWORD

In 2009, the OECD Committee on Consumer Policy launched a review of the organisation's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce*. As part of the review, the committee explored consumer benefits and challenges in mobile and online payments in an analytic report. Based on the assessment, the committee developed this policy guidance, which it adopted on 17 February 2014 and recommended that it be made available to the general public. The policy guidance is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

CONSUMER POLICY GUIDANCE ON MOBILE AND ONLINE PAYMENTS

I. Introduction

Following the 2009 *OECD Conference on Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy* (www.oecd.org/ict/econsumerconference) the Committee on Consumer Policy agreed to explore developments and consumer issues involving the use of mobile operators' networks and the Internet to make payments, as part of an overall review of the OECD's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce* (OECD, 1999). An assessment of trends and challenges was carried out during 2010 and 2011 leading to the publication of an analytic report (OECD, 2012), which was discussed with stakeholders at a workshop held in April 2011 (www.oecd.org/sti/consumer-policy/mobilepayments).

The report indicates that the development of innovative and easy-to-use mobile and online payment systems by financial institutions and other businesses (including mobile operators) has helped to support rapid growth in e-commerce in large and small businesses alike, providing consumers with more effective, convenient, and secure ways to purchase an expanding variety of goods and services. The report indicates that growth in the use of mobile devices to make payments is expected to accelerate, with the growing adoption by consumers of smartphones and computer tablets, from which a wider range of products, including intangible digital content products, may be purchased and accessed *via* a range of e-commerce channels, including traditional online retail platforms and social media. The impact of mobile payments has also been important in developing countries, where many consumers do not have bank accounts or payment cards and where basic mobile devices are increasingly being used to make person-to-person and business-to-consumer payments.

While the development of mobile and online payment systems has brought numerous benefits to consumers, the committee's work identified a number of areas where these systems could be strengthened to better address consumer interests. It concluded that consumers generally need to know more about their rights and obligations when they make such payments, especially when a number of parties (such as mobile operators, Internet service providers, and social media) are involved in a transaction. The situation is further complicated as payment systems may be subject to different regulatory schemes, which may have important implications with respect to the level of consumer protection afforded. Consumers may, in this context, have difficulty determining what their rights are, and how these may vary depending on factors, such as: *i*) the payment mechanism used (*e.g.* payment charged on mobile phone bills *vs.* credit, debit or prepaid payment card); and *ii*) the device being used (such as fixed computers, mobile phones or other portable devices). Determining which parties are responsible for addressing any problems that arise, the procedures for seeking redress, and the types of remedies that may be obtained, can also be problematic for consumers.

This guidance is intended to help shape consumer protection and industry practices in the area of mobile and online payments, keeping in mind the benefits that innovation and growth in new and evolving payment systems provide. It seeks to do so in a manner that will remain relevant as the technology used by payment systems evolves. The focus on mobile and online payments reflects the growing challenges and issues that are emerging in these areas; other forms of payment, such as those made using cash and checques are thus not covered.

In preparing this guidance, the committee built on the principles contained in the 1999 e-commerce guidelines and related policy instruments on cross-border fraud (OECD, 2003), dispute resolution and redress (OECD, 2007*a*), mobile commerce (OECD, 2008*a*), communication services (OECD, 2008*b*), consumer education (OECD, 2009*a*), online identity theft (OECD, 2009*b*), the security of information systems and networks (OECD, 2002), electronic authentication (OECD, 2007*b*) and privacy (OECD, 1980; OECD, 2013). Moreover, the committee drew on the policy assessment framework presented in the *Consumer Policy Toolkit* (OECD, 2010), as well as on instruments and reports from a number of jurisdictions and other *fora*.

II. Scope

The guidance concerns mobile and online payments made by consumers for products (including goods and services) acquired *via* e-commerce. It includes payments made *via* the Internet and those made using mobile devices, including, but not limited to, SMS and MMS payments as well as proximity-based payments made *via* mobile devices, such as those using near-field communication technology (NFC) at a point of sale. It does not include payments made by cheque or cash, nor does it include payments where credit or debit cards are presented directly to merchants or otherwise used at a point of sale.

For the purposes of the guidance, e-commerce refers to the sale or purchase of products (including goods and services) conducted over computer networks and related ICT channels, such as mobile operators' networks, by methods specifically designed for the purpose of receiving or placing orders. This guidance is limited to business-to-consumer (B2C) transactions.

III. Policy guidance

The 1999 e-commerce guidelines indicate that consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce (OECD, 1999; Part II, Section I). The committee has taken the view that this principle applies equally to evolving forms of e-commerce, such as mobile commerce and related payments.

Guidance on payments contained in the guidelines further provides that consumers should be provided with easy-to-use, secure payment mechanisms and with information on the level of security such mechanisms afford. It adds that 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 (OECD, 1999, Part II, Section V). In addition, the guidelines provide a set of basic principles on fair business, advertising and marketing practices, information disclosure, confirmation process, and dispute resolution and redress.

The committee concluded that in addition to the principles included in the above mentioned OECD instruments, it would be beneficial to provide further guidance on a selected number of issues in seven areas: *a)* Information on the terms, conditions, and costs of transactions; *b)* privacy; *c*) security; *d)* confirmation process; *e)* children; *f*) varying levels of consumer protection among payment providers and payments vehicles; *g*) protection against fraudulent and misleading commercial practices; and *h)* dispute resolution and redress. Issues concerning the interoperability of payment mechanisms are not addressed in the present guidance as they are being addressed in other contexts at the OECD.

A. Information on the terms, conditions and costs of transactions

Overview

The 1999 e-commerce guidelines call on businesses engaged in e-commerce to provide sufficient information about the terms, conditions and costs associated with a transaction so as to enable consumers to make an informed decision about whether to enter into the transaction (OECD, 1999, Part II, Section III). The section advises:

- Such information should be clear, accurate, and easily accessible and provided in a manner that gives consumers an adequate opportunity for review before entering into the transaction.
- Businesses should provide consumers with a clear and full text of the relevant terms and conditions of the transaction in a manner that makes it possible for consumers to access and maintain an adequate record of such information.
- Where applicable and appropriate, information should include:
  - An itemisation of total costs collected and/or imposed by the business.
  - Notice of the existence of other routine applicable costs to the consumer that are not collected and/or imposed by the business.
  - Terms conditions and methods of payment.
  - Details of and conditions related to withdrawal, termination, return, exchange, cancellation and/or refund policies.

Issues concerning the clarity, transparency, completeness and timeliness of information on the terms and conditions and costs of transactions follow. Disclosure issues pertaining to other aspects of transactions are addressed separately, in subsequent sections.

Issue 1: Accessibility and readability of payment-related information

The terms and conditions governing mobile and online payments may not always be easy for consumers to access and read, and they may not be available sufficiently early in the transaction process. Further, they may not always be easily retained by consumers. This material is often provided in small print and/or in scrolling text boxes. Key payment-related information is also sometimes disclosed in footnotes or requires accessing a series of additional windows.

Information challenges can increase when devices have relatively small screens or when devices, regardless of their size, have limited storage capacity and battery life. Moreover, transactions and related payments made through mobile devices are oftentimes concluded in an "on the go" context where consumers make rapid purchase decisions while in transit. In such a context, the ability of consumers to access, and/or review payment terms sufficiently before making a payment can be limited.

Failure to present key information sufficiently early in the transaction, and in a clear, conspicuous and easy-to-read manner, could result in consumers having to invest considerable amounts of time to draw together the information needed to make well-informed decisions. In addition to the time that might have to be spent, consumers may nonetheless not gather and evaluate sufficiently complete information because of the difficulties in locating, accessing and/or deciphering it. This would include information on loyalty

and reward programmes, which could be important factors in a consumer's decision to use a particular payment mechanism.

The situation can be further complicated when vendors present initial "headline" prices that are designed to attract customers, without including additional, mandatory charges, such as booking, credit card, handling fees and, in some jurisdictions, taxes; this would also include customs and other charges applying to cross-border transactions. Studies of the practice, known as "drip" or "partition" pricing, suggest that the potential to mislead consumers is high, and that the tendency for many consumers to focus on headline prices in making their decisions could result in their purchasing products from higher priced sources. In some jurisdictions, the practice is not allowed.

In such instances, consumers may neither seek out all, or part of the information, nor understand it. As noted in the OECD's *Consumer Policy Toolkit* (OECD, 2010), research on consumer economics indicates that, when consumers are time-pressed or are confronted with information that is not suitable, they may end up using heuristic "rules of thumb" to make purchasing decisions, which may result in unsatisfactory choices. The time required to evaluate offers and possible frustration and confusion over payment and related issues could result in consumers limiting their searches and, eventually, paying more than they expected for a product, purchasing a product that does not otherwise meet their expectations or losing interest in purchasing a product altogether.

Guidance

To help ensure that payment-related information is easily accessible, and readable:

i. *Key payment and related transaction information should be provided to consumers early in a transaction process in a clear, conspicuous and easily accessible manner. It should be presented in formats that can be easily read on the different types of devices being used to engage in e-commerce, including mobile devices with small screens that are often used in an "on the go" context.*

ii. *Headline prices should include fixed compulsory charges. Information on the existence of variable compulsory charges and optional charges should be disclosed clearly and conspicuously to consumers on the same page or screen as headline prices, and with appropriate prominence. The amount of such charges should be disclosed clearly and conspicuously to consumers as soon as they are known by the business concerned, and well before consumers need to complete the transaction.*

iii. *The difficulties that consumers might encounter in accessing information on the details of a payment transaction in an "on the go" context, should be addressed by optimising disclosures so that consumers can easily access such information, and by streamlining, simplifying, and, where appropriate, standardising the presentation of payment information. The use of mechanisms, such as graphics and icons, to make disclosures clear, conspicuous and easily accessible, should be explored. Such mechanisms should themselves be conspicuous, easily understandable, and not misleading.*

iv. *Consumers should be provided with options for preserving information on payments and related transaction information. Such options could include printing, e-mailing or otherwise electronically storing the information. To the extent possible, these options should be available for all types of devices that are used in e-commerce.*

Issue 2: Complexity of payment terms and conditions

The terms and conditions relating to mobile and online payments are often presented in lengthy and technical legal terms that can be difficult for consumers to understand. Surveys carried out in a number of countries suggest that a majority of consumers purchasing products *via* e-commerce do not fully read or understand the terms and conditions, including those relating to loyalty and reward programmes, due to the complexity of the information and the time that would be required to review it. As a result, consumers may not be sufficiently aware of the nature, length, level and scope of the financial commitments that they are making. Moreover, consumers may not be aware of the significance of any additional "hidden" costs. In the case of certain transactions, this could result in surprisingly high bills (*i.e.* "bill shock"), dissatisfaction with a good or a service that did not meet expectations and frustration with the procedures and cost that could be incurred in terminating such services.

Guidance

To help ensure that consumers understand payment terms and conditions:

i. *In addition to full presentations, businesses should provide consumers with summaries of key payment terms and conditions. These should include information on the total cost of a transaction, product availability, timing for delivery, refund and return policy, withdrawal rights, recurring charges (including automatic repeat purchases and subscription renewals and ways to opt out from such automatic schemes), and dispute resolution options (including relevant contact information).*

ii. *Summaries of payment terms and conditions should be clear, conspicuous and concise. They should be presented in plain language that can be easily understood by the general population.*

Issue 3: Clarity and transparency of billing statements

Billing statements, in particular those provided by mobile operators, are sometimes not detailed enough to allow consumers to determine the nature of the products purchased and any related charges. Moreover, some payment intermediaries do not sufficiently identify the third parties involved in a transaction. As a result, consumers may have difficulty determining the accuracy of their billing statements.

Guidance

To help ensure transparency in billing statements:

i. *Billing entities should clearly:*

   - *Distinguish their charges on billing statements from those charges involving third parties.*

   - *Describe the nature of charges on their billing statements in a format that enables consumers to easily identify the goods or services purchased and what payment provider or merchant placed the charge on the billing statement.*

ii. *Billing statements should provide information that: a) confirms the price and other key transaction information; and b) enables consumers to identify and contact all parties that relate to the payment transactions, including the billing entity and, in the case of third party billing, the third party.*

B. Privacy

Overview

The mobile and online environment raises a number of payment-related challenges with potential privacy implications. These include: *i*) the determination of which party is accountable for the use and management of consumers' payment information; *ii*) the identification of the party or parties who are retaining it and for how long; *iii*) the possible use or transfer of the payment information to third parties, and *iv*) how such payment information is being safeguarded. These issues are particularly pronounced in the mobile payments context due to the larger number of companies that can be involved in processing transactions. The ways in which these matters are addressed can affect consumer confidence in e-commerce, which, in turn, could discourage further innovation and adoption of mobile payment mechanisms.

The 1999 e-commerce guidelines indicate that e-commerce should be conducted in accordance with the principles of the OECD's 1980 privacy guidelines (OECD, 1980), which contain the following eight basic principles of domestic application:

- *Collection limitation principle*. There should be limits to the collection of personal data; such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- *Data quality principle*. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for these purposes, should be accurate, complete and kept up-to-date.

- *Purpose specification principle.* The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others that are not incompatible with those purposes and that are specified on each occasion of change of purpose.

- *Use limitation principle.* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the preceding bullet point except a) with the consent of the data subject; or *b*) by the authority of law.

- *Security safeguards principle.* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

- *Openness principle.* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- *Individual participation principle.* Individuals should have the right: *a*) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; *b*) to have communicated data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them; *c*) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and *d*) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

- *Accountability principle.* A data controller should be accountable for complying with measures which give effect to the principles stated above.

The above principles were retained in the OECD's revised privacy guidelines (OECD, 2013), in which new provisions on implementation and global interoperability were added. New provisions provide that a data controller should (OECD, 2013, Part III, respectively paragraph 15 a *iii* and c):

- Have in place a privacy management programme that provides for appropriate safeguards based on privacy risk assessment.

- Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

In addition to the 1999 e-commerce guidelines, the 2008 policy guidance on mobile commerce (OECD, 2008) addresses issues relating to privacy with a focus on location-based information tracking.

Issue: Collection and use of payment data

Many different entities may have access to the mobile and online payment information that is provided by consumers when they make a purchase *via* e-commerce. For example, banks and other payment institutions, merchants, operating system platform providers, hardware manufacturers, mobile operators, application developers, data analytics companies, advertisers and coupon and loyalty programme administrators may have access to payment data in some transactions. This information could include addresses, phone numbers and location data that is used to authenticate the payment transaction and ensure that the payment can be authorised given, for example, the location or habitual residence of the buyer. This information is more accessible in the case of payments made using mobile devices, since many consumers keep those devices with them in an "always on" mode. Such data has value, as it can be used or shared with other parties, for commercial purposes.

Businesses' access and use of payment data can be beneficial for consumers; its use for targeted marketing, for example, can help consumers to identify products which meet their interests. It might also result in businesses providing certain products at a reduced price, or for free. Further, it may help to reduce fraud by providing businesses with a better basis to authenticate their customers.

On the other hand, consumers' payment data may also be used in ways that raise concerns. Consumers, for example, may not fully understand how the payment data they have provided could be used for purposes beyond completing a given transaction and the value that such data may have for businesses. Information on why personal data that is unrelated to the payment is being collected during the payment process may not be explained to consumers. The collection of such data and the related lack of transparency may raise concerns with consumers, resulting in a hesitancy to purchase products, particularly from businesses about whom they know relatively little. Moreover, consumers may not agree to their activities being tracked and their data being used or shared with third parties for commercial or other purposes. Furthermore, once their payment data has been provided, consumers may have limited ability to control its use. When purchasing "apps," for example, consumers sometimes grant permissions without being clearly informed that they are doing so; they may not even be able to check back to see what permissions were granted. Finally, businesses that over collect data increase risks to themselves and to consumers, should the data be stolen, lost or misused; this would include financial, reputation, and liability risks that could undermine consumer trust in mobile and online payment systems.

Guidance

To help ensure that payment data is not used in ways that are contrary to consumer interests:

i. *Businesses should include privacy protection safeguards when designing and developing their mobile and online payments systems. Safeguards that are already being used in existing payment systems should be reviewed, and, as appropriate, incorporated into new or updated systems.*

ii. *Businesses should in general limit the collection of personal data gathered as part of mobile and online payment transactions to information that is: i) directly related to the payment transaction; ii) required by the payment provider; iii) legally required, or iv) used for account and risk management, authentication, fraud prevention or legal compliance purposes. Such information may include, but is not limited to the consumer's name, postal code, phone number, payment card number, bank account numbers and sort codes for accounts at banks or other financial institutions as well as authenticating data.*

iii. *If, during the payment process, businesses collect and use personal data other than that specified in ii) that is not legally required or needed to complete the payment, they should provide consumers with clear and prominent notice of such collection at a relevant time and provide them with appropriate choice mechanisms to allow them to limit or deny the collection and use of such data. Businesses should obtain express consent before collecting sensitive data, such as individualised geo-location data, health information, financial information or information about children.*

iv. *Businesses should be transparent about their data collection and use practices in the mobile and online payments context. They should explain: i) why personal data from consumers is being collected and stored; ii) the ways that such information may be used and/or shared; and iii) any controls available to consumers.*

v. *Standardised privacy disclosures and choice mechanisms that are understandable and easily accessible on different types of device should be developed by stakeholders. The disclosures should be presented in a clear and consistent manner at appropriate points during the payment transaction.*

C. Security

Overview

The 2002 security guidelines (OECD, 2002, Part III) contain nine complementary principles that are relevant to the security of mobile and online payment transactions:

- *Awareness principle*. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

- *Responsibility principle*. All participants are responsible for the security of information systems and networks.

- *Response principle*. Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

- *Ethics principle*. Participants should respect the legitimate interests of others.

- *Democracy principle*. The security of information systems and networks should be compatible with essential values of a democratic society.

- *Risk assessment principle*. Participants should conduct risk assessments.

- *Security design and implementation principle*. Participants should incorporate security as an essential element of information systems and networks.

- *Security management principle*. Participants should adopt a comprehensive approach to security management.

- *Reassessment principle*. Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

The 2007 recommendation on electronic authentication provides that OECD member countries should foster the development, provision and use of electronic authentication products and services that embody sound business practices, including technical and non-technical safeguards to meet the participants' needs, in particular with respect to security and privacy of their information and identity (OECD, 2007*b*).

The 2008 policy guidance on mobile commerce provides that it might be beneficial for participants in mobile commerce to provide consumers with timely and effective methods of redress when their data is compromised and/or they suffer financial loss (OECD, 2008, Section IV).

Issue: Payments security

Without adequate security, transaction data provided in the context of e-commerce payments could be lost, stolen or otherwise misused. The situation is of particular concern in the case of payments made using mobile devices, due to the higher risk of the devices being lost, stolen or otherwise compromised. In such a context, security risks, and potential consumer detriment, grow when larger volumes of consumer personal data are collected. Although technology advances offer the potential for increased data security, some consumer concerns about the level of protection remain; these concerns may be impeding the use of mobile payments systems. Mobile devices that employ "end to end" encryption and dynamic data authentication, if utilised, could help to address concerns, thereby increasing consumer confidence in mobile payments.

Guidance

To protect the security of consumer payment data collected and used in the context of mobile and online payments:

i. *Payment providers should put in place appropriate safeguards to protect the security of their systems, and should encourage the adoption of such measures by all entities having access to consumer data related to payments.*

ii. *In addition to notifying consumers, payment providers should provide them with timely and effective redress mechanisms when their data is compromised and/or they suffer financial losses caused by security breaches.*

iii. Stakeholders should work together to raise consumer awareness about payment security issues, and about the actions that consumers can take to protect themselves in such transactions.

D. Confirmation process

Overview

E-commerce payments are part of an overall transaction process which is divided into a number of steps. These include:

- A pre-contractual phase, where consumers are provided with information about the product, the transaction and the business. Consumers use such information to help them decide whether to conclude a transaction, or not.

- A contractual phase, whereby consumers' agreement to the transaction leads to the processing of a payment.

- A post-contractual phase whereby consumers may seek to correct any errors made in their order, or may exercise, when available, a right of withdrawal.

To avoid ambiguity concerning a consumer's intent to make a purchase, the 1999 e-commerce guidelines indicate that consumers should be able, before concluding a purchase, to: *a)* identify precisely the goods or services they wish to purchase; *b)* identify and correct any errors or modify an order; *c)* express an informed and deliberate consent to the purchase; and *d)* retain a complete and accurate record. Moreover, the guidelines provide that consumers should be able to cancel a transaction before it has been completed (OECD, 1999, Part II, Section IV).

The 2008 guidance on mobile commerce notes the difficulties that consumers may sometimes have in fully accessing contractual information prior to making a decision when using a mobile device. It provides that consumers using mobile devices should be provided with clear and full information on the proposed transaction prior to concluding the contract so that they can confirm the goods or services ordered, or correct any errors; consumers should also be provided with the possibility to retain or print out adequate records of the transaction, including contract terms.

Issue: Transaction uncertainty

In some instances, consumers purchasing products *via* e-commerce may not realise when they are confirming a transaction. For example, consumers using mobile devices to make "on the go" purchases through "apps" might not realise that by simply clicking on an icon, they have agreed to a purchase and that payment is due. As a result, consumers might end up being billed for products that they did not intend to buy. On the other hand, consumers may inadvertently supply wrong payment information and may, without their knowledge, wind up having their transaction cancelled or rejected. In some circumstances, consumers may be unaware that this has occurred. There may also be uncertainty about the status of the transaction when, for example, the connection on a mobile device is lost during the confirmation process.

Guidance

To help ensure that consumers understand when a transaction has been concluded and that payment is due, or that a transaction has not been fully processed:

i. The point at which consumers are being asked to commit to a transaction, after which time payment is due, should be clear and unambiguous, as should the steps consumers would need to

follow to complete a transaction. Consumers should also be provided with an opportunity to confirm their payment information, or cancel an entire transaction, prior to concluding it.

ii. Consumers should be clearly notified when a transaction for which payment information has been provided, is not fully processed.

E. Children

Overview

The 1999 e-commerce guidelines provide that businesses should take special care in advertising or marketing products that target children, who may not have the capacity to fully understand the information which they are presented (OECD, 1999, Section II, Part II).

The 2008 policy guidance on mobile commerce provides examples of situations where problems could arise when children who have access to mobile devices use them to purchase products without the knowledge or consent of their guardians (OECD, 2008, Section III). The problems are notable in the case of mobile devices as purchases can be made without a child having to provide appropriate authentications before making any payment commitment. To address this issue, the 2008 mobile commerce guidance provides that stakeholders could:

- Provide parents with the ability to set a ceiling that would limit the amount of charges that children could accrue using mobile phones, by, for example, setting a limit on the number of text messages, or establishing monetary limits on downloadable purchases.

- Encourage mobile devices to be designed in a way that users could limit the types of transactions.

- Encourage mobile operators to send warnings/notices to parents when expenditures exceed an established ceiling level.

The committee's 2009 recommendations on consumer education further indicate that it is important to educate parents and children about their respective responsibilities online, as well as the techniques that are frequently used online to market products (OECD, 2009*a*, Annex II).

Issue: Charges incurred by children accessing goods and services

Growing usage of the Internet and mobile devices to buy products *via* e-commerce without having to enter financial information for every purchase has exposed children to a number of risks including charges in online games or "apps" that have allowed children to make multiple purchases without having to enter a password every time. Although in most countries children generally do not have the legal capacity to make payment commitments, once signed onto a mobile account, they may be in a position to incur charges without the account holder's knowledge or consent, in which case the purchase may be invalid. These situations most often occur with devices that have been made available to children by their parents or guardians. Related concerns have been raised in a number of countries regarding children's usage of products, which, while being labelled as "free," may require a payment to access specific features or content.

Guidance

To enable parents or guardians to monitor and limit children's mobile and online payments for goods and services, businesses, governments and other stakeholders should:

i. *Consistent with the guidance contained in section A, issue 1, on "Accessibility and readability of payment-related information", work together to provide parents and guardians, prior to the children's purchase of or access to goods or services that are likely to generate charges incurred by children, with clear, conspicuous and easily accessible information on the costs that may be incurred in acquiring, accessing or using goods and services, and information on how to avoid those costs.*

ii. *Develop effective mechanisms that enable parents or guardians to ensure that payments initiated by children are subject to their authorisation.*

iii. *Develop tools which enable parents or guardians to exercise different types of controls over the purchases they authorise their children to make; this would include, for example, tools to prevent children from making purchases without express parental consent or tools that enable parents or guardians to establish ceilings on the amounts that could be charged to an account during defined periods.*

iv. *Inform parents or guardians about the availability of such tools in a clear and conspicuous manner.*

F. Varying levels of protection among payment providers and payments vehicles

Overview

The 1999 e-commerce guidelines provide that 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 that use should be encouraged in the context of electronic commerce (OECD, 1999, Part II, Section V).

Considerable progress has been made in implementing this principle in jurisdictions, through actions taken by governments and businesses. In many instances, protection has gone beyond unauthorised and fraudulent use of payments systems, to include problems involving non-conforming and undelivered products. The level of protection, however, varies within and across jurisdictions, according to the:

- *Payment means used*. In most OECD countries, consumers enjoy strong legal protection, as well as supplementary payment-related protection provided by financial intermediaries, when payments are made using payment cards. They may also enjoy some legal protection for bank debits. It should be noted that such protection applies regardless of the device being use to make a payment; this would include, for example, situations where NFC technology is used to make a payment that is linked to a payment card. The protections cover problems relating to unauthorised charges (which may result from billing or processing errors or from fraudulent transactions where a payment card is lost or stolen or where card details are stolen or misused); it may also cover problems relating to product conformity and delivery. The protection attached to payment cards can depend on the company sponsoring the card, and/or the jurisdiction where the card is issued; the level of consumer rights may also vary from one type of card to another within the same company. In general protection for credit cards is higher than for debit cards or bank debits. In the case of the latter, consumers usually face variable liability limits for unauthorised charges, but a lack of protection in case of conformity and delivery problems. Some level of uncertainty about the level of protection associated with the use of debit cards may also stem from factors, such as: *i*) limited consumer awareness of their rights and obligations; *ii*) limited transparency about such rights and obligations by the issuing financial organisation; and *iii*) the

variety of card scheme rules in this area. Moreover, in a number of OECD countries, there is little or no statutory protection associated with the use of stored value money in prepaid and gift cards, or payments made *via* mobile phone bills.

- *Parties involved*. In some countries, payment mechanisms provided by institutions which are not generally treated as financial institutions (such as mobile operators) are not subject to the same consumer protection rules as banks or other credit providers. In other jurisdictions, all payment providers, including mobile operators, are subject to the same rules when participating in the payment process.

Issue 1: Information on consumer protection

Information on the different rights and protections that are available to consumers from payment providers is not often available at the time of a purchase; this can complicate the situation for consumers who may not understand the differences between the various funding sources. Obtaining such information can, for example, oblige card holders to phone the issuing institutions, or request that the information be sent by post. Related information on applicable laws and regulations may also be difficult to access. This can make it difficult for consumers to know what their rights are when purchasing a product. The situation is further complicated when payment for a product supplied by a business is being billed by a third party, such as a mobile operator.

Guidance

To help ensure that consumers are adequately informed about their rights and obligations in payment transactions:

i. *Governments, payment providers, businesses, civil society and other stakeholders should work together to provide mechanisms that consumers can easily access to determine: a) what their rights and protection are when making a purchase; and b) the extent to which protection (including limitations of liability, return, exchange, price reduction, and refund policies and procedures) may vary, depending on factors such as the payment mechanism used.*

ii. *Payment providers involved in cross-border transactions should clearly indicate in their terms and conditions how consumer rights and protections associated with the use of their mechanism may be affected by the cross-border nature of the transactions.*

iii. *Payment providers, businesses, civil society and other stakeholders should work together to educate consumers about payment options and related protection issues, and to raise awareness of key matters.*

Issue 2: Levels of payment protection

Consumers can benefit considerably by using payment mechanisms that provide high levels of protection, even if they have to pay a premium for such coverage. Such protection helps consumers to avoid the detriment that would otherwise arise, when they are the victims of fraud or unauthorised payments. In these instances, payment providers may provide the only effective means for obtaining redress. This can be particularly important in the case of cross-border transactions, where consumers may have limited means to pursue matters.

Guidance

To help ensure that consumers are provided with adequate remedies in case of problems with transactions:

i. *Governments and payment providers should work together to develop minimum levels of consumer protection for mobile and online payments transactions, regardless of the payment mechanism used. Such protection should include regulatory or industry-led limitations on liability for fraudulent and unauthorised charges that pertain to all mobile and online payment mechanisms.*

ii. *Governments and payment providers should: a) explore other areas where greater harmonisation of payment protection rules among jurisdictions would be beneficial; and b) seek to clarify how issues involving cross-border transactions could best be addressed when payment protection levels differ.*

G. Fraudulent, misleading, deceptive and other unfair commercial practices

Overview

The 1999 e-commerce guidelines call on businesses engaged in e-commerce to pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices (OECD, 1999, Part II, Section II). Businesses are: *a)* called on not to make any representation or omission or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair; and *b)* encouraged to establish limitation of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms. In addition, governments are called on to co-operate at the international level to combat cross-border fraudulent, misleading and unfair commercial conduct, through information exchange, co-ordination, communication and joint action.

The 2003 cross-border fraud guidelines provide further guidance with respect to government policies. These guidelines encourage governments to put frameworks in place that would help limit, prevent and deter fraudulent and deceptive commercial practices involving business and individuals. In particular, the guidelines state that governments should provide for effective mechanisms: *a)* to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices; *b)* to stop businesses and individuals engaged in fraudulent and deceptive commercial practices; and *c)* that provide redress for consumer victims of fraudulent and deceptive commercial practices (OECD, 2003, Section II, A).

In addition, governments are called on to:

- Develop mechanisms for co-operation and information sharing between and among their own consumer protection enforcement agencies and their other law enforcement authorities, for the purpose of combating fraudulent and deceptive commercial practices.

- Review their own domestic frameworks to identify obstacles to effective cross-border co-operation in the enforcement of laws designed to protect consumers against fraudulent and deceptive commercial practices, and consider changing domestic frameworks, including, if appropriate, adopting or amending national legislation to overcome any barriers.

- Educate consumers about fraudulent and deceptive commercial practices, undertaking joint initiatives as appropriate.

The 2007 guidance on electronic authentication provides that by providing a level of assurance regarding the identity claimed by parties engaged in an online relationship, authentication reduces uncertainty inherent in transactions at a distance, thus fostering trust in electronic interactions, and participates to the broader fight against online threats and criminal activities. The recommendation further provides that OECD members should take steps to raise the awareness of all participants, including non-members, of the benefits of the use of electronic authentication at national and international levels (OECD, 2007*b*).

The development of payment systems since these guidelines were developed has done much to reduce the risks of fraudulent, deceptive and misleading practices in e-commerce; these issues, however, remain areas of concern for consumers, who are confronting some of these practices on their mobile devices in new formats, such as through "apps."

Issue 1: Inconsistent payment-related information

In some instances, information provided to consumers on prices and other payment-related issues is misleading, inconsistent or contradictory.

Guidance

To avoid misrepresentations:

Businesses should not provide consumers with information on prices and other payment-related issues that is misleading or deceptive. Information on prices and other payment-related issues should be consistent throughout the payment transaction. The practice of presenting payment-related information that is false or misleading to consumers and then providing the correct information later in the transaction process should not be allowed.

Issue 2: Renewable contracts, renewable subscriptions and repeat purchases

Consumers are sometimes not clearly informed, at the time of a purchase, that the terms and conditions contain provisions for automatic repeat purchases of goods or automatic contract or subscription renewal. There have been some instances where, for example, consumers purchasing software online were informed in their end-user licensing agreements that they would have the option to renew the agreement upon expiration; in practice, however, the agreement was renewed automatically, resulting in consumers being charged for products they may not have wanted. In other instances, consumers purchasing ringtones through their mobile phones did not realise that they had, at the same time, subscribed to an ongoing service.

Guidance

To help ensure that consumers are adequately informed about automatic repeat purchases and contract and subscription renewals:

i. Businesses should, early in the transaction process clearly and conspicuously inform consumers when their offers for goods or services:

- *Involve a repeat purchase or subscription for the product on offer or are tied to repeat purchases or subscriptions for other products*.

- *Involve a contract or subscription that is renewed unless a consumer takes steps to cancel it (i.e. negative option billing). This should include disclosure of the amount and frequency of any recurring charges*.

ii. *Consumers should be provided with clear, easy-to-use procedures for preventing automatic renewals of contracts and for terminating recurring charges; such procedures should be communicated to consumers in the confirmation of the transaction.*

iii. *Unless the option is waived by a consumer, notification should be provided (to the consumer) when an automatic repeat purchase will be made or when a subscription will be automatically renewed. Such notification should be made sufficiently in advance to enable the consumer to cancel the purchase or renewal; it should include information on how the cancellation may be made.*

iv. *Payment providers should work with businesses to ensure that consumers are provided with adequate alerts and notifications about repeat purchases and automatic subscription and contract renewals.*

Issue 3: Unexpected charges

Consumers are sometimes charged for products that they thought were free, did not authorise or did not knowingly purchase. Complaints have been made, for example, about fees for products being charged automatically after a trial service period had ended, without having received sufficient notification. Moreover, consumers have reported concerns about charges associated with mobile applications ("apps") that have been purchased by consumers or acquired at no direct cost (i.e. "free" "apps"). In many instances, consumers were unaware that additional charges would be applied to "apps"-related or enhanced products or services ("in-app" purchases). In the context of payments charged on mobile phone bills by mobile operators, consumers have also reported problems with a practice known as "cramming," whereby fees and charges were made to their mobile phone bills for: *a*) purchases they did not authorise; *b*) products they did not receive or *c*) products whose cost was higher than the consumer was led to believe. Such charges are often made by third parties.

Guidance

To help protect consumers from unexpected additional charges that could result when trial periods have lapsed or when use of a product, such as an "app", results in new charges:

i. *When products are provided to consumers on favourable terms for a limited period of time (i.e. a trial period), information on the length of the trial period and the charges that will be incurred once the trial period has elapsed, should be provided clearly and conspicuously to consumers, as should information on the steps to be taken to discontinue purchasing the good or service.*

ii. *Consumer consent should be obtained for continuing a commercial relationship beyond a trial period, before consumers pay or incur any additional financial charges.*

iii. *If use of a product results in additional charges, consumers should be so informed and their consent for such charges should be required.*

To help protect consumers from unexpected charges from third parties, in particular in the context of charges on mobile phone bills:

i. *Businesses should provide consumers with options for limiting or blocking the ability of third parties to bill them for goods and services. This would include the ability to block charges on sub-accounts, such as individual accounts operated by children.*

ii. *Businesses should clearly and prominently inform their customers when third-party charges may be placed on their accounts without their express authorisation and explain how to limit or block such charges.*

iii. *Businesses should establish a clear and consistent process for consumers to dispute charges on their accounts and obtain reimbursement.*

To help protect consumers from unexpected charges associated with "in-app" purchases, businesses and other stakeholders should work together to:

i. *Provide consumers with clear, conspicuous, consistent, and easily accessible information on the possibilities to use an "app" to make purchases, and on the costs that could be involved in using the "app" so that consumers can make informed choices whether to use such "apps," or, where possible, limit their use.*

ii. *Obtain consumers express consent for any "in-app" purchases.*

Issue 4: Consumer confidence

E-commerce transactions that are not proximity-based present a number of risks that are not present in more traditional retail settings: *a)* consumers often cannot easily confirm the identity and integrity of vendors and *b)* they cannot evaluate products prior to making purchases in the same manner as those purchased in retail stores. Unauthorised purchases and charges, often through identity theft, continue to be a significant problem for consumers in this regard. Although payment providers and businesses have developed new methods to address such risks, many consumers still perceive the risk associated with such purchases as significantly higher than for more traditional purchases from local retailers. This could result in reluctance on their part to adopt new payment mechanisms.

Guidance

To help strengthen consumer confidence, payment providers, businesses, and other stakeholders should:

i. *Work together to develop effective practices and regulatory tools to help prevent payment fraud.*

ii. *Develop tools to help consumers detect and protect themselves against deceptive, misleading and fraudulent practices. This would include providing consumers with means to remotely freeze an account when unauthorised use is suspected; this would include the ability to disable their mobile phones and "apps" which, when used, could result in payments being made.*

iii. *Work together to improve the effectiveness of electronic authentication systems.*

iv. *Work on the development and implementation of comprehensive anti-fraud programmes designed to protect consumers, which would include avoiding installing and doing business with businesses and mobile and online applications providers who appear to be involved in or accomplice of fraudulent, deceptive, and misleading commercial practices.*

H. Dispute resolution and redress

Overview

The 1999 e-commerce guidelines call on businesses, consumer representatives and governments to work together to continue to use and develop fair, effective and transparent self-regulatory policies and procedures, including alternative dispute resolution mechanisms, to address consumer complaints and resolve consumer disputes, with special attention to cross-border transactions (OECD, 1999, Part II, Section VI, B). These self-regulatory procedures go beyond the legal remedies that are available in jurisdictions. The 2007 guidelines on dispute resolution and redress elaborate on this principle, establishing a framework for such procedures. The latter guidelines encourage payment card issuers to voluntarily provide consumers with remedies for disputes arising out of transactions for goods and services; they suggest that such protection could include limitations on liability to pay for non-delivered or non-conforming goods and services (OECD, 2007, Annex, Section IV, 2.*c*).

The 2008 mobile commerce guidance recommends that mobile operators, mobile vendors, website operators, mobile aggregators and governments work together to establish fair, effective and transparent self-regulatory mechanisms, policies, and procedures to address consumer complaints and resolve consumer disputes arising from complex mobile commerce transactions. It further recommends that participants in this market consider implementing dispute resolution and redress mechanisms such as customer satisfaction codes, chargeback mechanisms, and alternative dispute resolution services, as recommended in the 2007 OECD Recommendation on Consumer Dispute Resolution and Redress (OECD, 2008, Section II and OECD, 2007).

Issue 1: Roles and responsibilities of parties

The roles and responsibilities of parties involved in transactions in addressing and resolving disputes are often not clear, making it difficult for consumers to know whom to turn to when problems arise. This can result in delays in consumers having problems resolved in a satisfactory manner, and, in some cases, failures to obtain redress.

Guidance

To help ensure that consumers have adequate access to dispute resolution and redress mechanisms:

i. *Governments, payment providers, platform operators and other stakeholders, should work together to clarify the options that are available to consumers to address payment-related disputes, and the procedures that should be followed when a problem arises. This should include:*

   - *Clear information about which party should be contacted to address payment-related problems, and how that party should be contacted.*

   - *Information on referrals that can be made to regulatory bodies, law enforcement agencies, ombudsmen, or self-regulatory bodies, in the event problems are not resolved in a satisfactory manner with businesses and payment providers.*

ii. *Payment intermediaries involved in e-commerce transactions should be encouraged to provide consumers with adequate, low cost and easy-to-use dispute resolution and redress systems.*

iii. *When a consumer is entitled to reimbursement, such reimbursement should be made without unreasonable delay*.

iv. *Payment intermediaries involved in e-commerce transactions should consider requiring third parties, such as aggregators, to maintain sufficient and accessible records of consumer authorisations of individual charges, so as to facilitate the resolution of disputes.*

Issue 2: Cost of seeking redress

The cost, time and effort required to resolve e-commerce disputes can be significant, which could discourage consumers from seeking redress, especially in low value transactions. When a problem arises in a low value e-commerce transaction and the dispute cannot be resolved directly with businesses, traditional litigation may be too time consuming and expensive for consumers to pursue. As a result, consumers may not bother engaging in a dispute resolution process, which could result in financial losses.

Guidance

To provide consumers with meaningful dispute resolution and redress mechanisms:

Governments, payment providers, merchants and other stakeholders should develop low-cost, easy to use alternative dispute resolution and redress mechanisms which would, inter alia, facilitate resolving claims over payments involving low-value transactions. Such mechanisms could include the development of effective online dispute resolution systems. Alternative dispute resolution and redress mechanisms should not prevent parties from pursuing other forms of redress, as permitted by applicable law.

REFERENCES

OECD (Organisation for Economic Co-operation and Development) (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

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

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks*, OECD, Paris, 2002, www.oecd.org/sti/ieconomy/15582260.pdf.

OECD (2003), *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/sti/crossborderfraud.

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

OECD (2007*b*), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*, OECD, Paris, 2007, www.oecd.org/sti/ieconomy/38921342.pdf.

OECD (2008*a*), *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment issues in Mobile Commerce*, *OECD Digital Economy Papers*, No. 149, OECD Publishing, doi: 10.1787/230363687074.

OECD (2008*b*), *Policy Guidance for Protecting and Empowering Consumers in Communication Services*, OECD, Paris, www.oecd.org/dataoecd/49/38/40878993.pdf..

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

OECD (2009*b*), *OECD Policy Guidance on Online Identity Theft*, in OECD, *Online Identity Theft*, OECD Publishing, doi: 10.1787/9789264056596-5-en.

OECD (2010), *Consumer Policy Toolkit*, OECD, OECD Publishing, doi: 10.1787/9789264079663-en.

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

OECD (2013), *Revised Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 2013, www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.