

**Unclassified**

**DSTI/CP(2011)11/FINAL**

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

**18-Jan-2012**

**English - Or. English**

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY  
COMMITTEE ON CONSUMER POLICY**

**OECD WORKSHOP ON CONSUMER PROTECTION IN ONLINE AND MOBILE PAYMENTS:  
SUMMARY OF DISCUSSION**

**JT03314540**

Document complet disponible sur OLIS dans son format d'origine  
Complete document available on OLIS in its original format



DSTI/CP(2011)11/FINAL  
Unclassified

English - Or. English

## FOREWORD

On 15 April 2011, within the framework of its review of the OECD 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce*, the OECD Committee on Consumer Policy (CCP) organised a workshop exploring new trends and consumer challenges in online and mobile payments.

This report provides a summary of the discussion held among representatives from governments, major e-commerce payment providers and card networks, as well as civil society. The report was declassified by the committee at its 82<sup>nd</sup> session on 26 October 2011.

*This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.*

**TABLE OF CONTENTS**

I.	Market developments .....	4
II.	Key consumer policy challenges .....	4
	Regulatory frameworks .....	5
	Varying levels of consumer protection.....	5
	Examples of fraud and deceptive commercial practices.....	5
	Dispute resolution.....	6
	Security.....	7
	Interoperability .....	7
III.	Next steps .....	7

## **OECD WORKSHOP ON CONSUMER PROTECTION IN ONLINE AND MOBILE PAYMENTS: SUMMARY OF DISCUSSION**

In support of the Committee's work on online and mobile payments, a workshop was held on 15 April 2011 at the OECD to discuss, in light of an analytic report that had been prepared, market trends and current and emerging consumer policy issues. The following provides a summary of the discussion in which key payments stakeholders from government, business, and civil society took part.

### **I. Market developments**

Advances in online and m-payments technology and networks have supported exponential growth of e-commerce. *Visa Europe* had, for example, seen a significant shift in its business from traditional point of sale to virtual payments. In 2011, 25% of its transactions in the European Union (EU) were made on line (the United Kingdom being the largest market). These could reach 45% by 2015. A shift in consumer interest in mobile payments was also noted. *PayPal's* total mobile payment volume had for example grown from USD 25 million in 2008 to USD 750 million in 2010; it was expected to double by the end of 2011. Use of credit, debit, prepaid cards and online payments-based systems was converging into the mobile handset. But despite growth, e-payments had not reached their full potential, and the mobile payments marketplace was still nascent in many countries. Consumer misperception of risk associated with the theft of payment details was one factor inhibiting confidence in online transactions. The actual incidence of payment details theft proved, however, very low. Only 1% of EU consumers who bought goods on line experienced such a problem.

The commercialisation of proximity mobile payments relying on Near Field Communications (NFC) technology was seen as a channel that could support growth. *GSMA's Pay-Buy-Mobile* initiative being developed with 62 mobile network operators (MNOs) in a number of countries was becoming a reality, enabling consumers to benefit from multiple payments services options integrated into a single mobile device. In addition to buying products in shops, consumers would be able to (or could already) use their handset to, for example, check in and out of a hotel, receive information in museums, use public transport, buy concert, sport and flight tickets and benefit from loyalty programmes or discount offers. In the event of loss or theft of the mobile device, consumers would be able to remotely lock the payment applications (stored on the Universal integrated circuit card (UICC)). As the card could be partitioned into several security domains with an encryption key unknown to the MNO, the handset is becoming a standalone wallet.

Measures such as strong authentication tools, the need for improved consumer education on ways to protect themselves from fraud and security risks, and available mechanisms to facilitate communication between consumers and merchants, were seen as necessary to enhance confidence.

### **II. Key consumer policy challenges**

Unauthorised charges (including surcharges), fraudulent and deceptive commercial practices, privacy, security, and interoperability problems, unclear rules on parties' rights and responsibilities, and a lack of adequate education and dispute and redress mechanisms, were all mentioned as problems faced by consumers in online payments. These were seen as exacerbated in the mobile environment due to the

inherent characteristics of the device (e.g. small screen, limited memory capacity) and the involvement of new types of payments providers, such as MNOs. Participants discussed which regulatory framework should apply or be developed to address issues, and whether such rules should apply equally to all problems and payment methods used.

### ***Regulatory frameworks***

A number of countries had implemented existing generic consumer protection rules to address issues, along with self- and co-regulatory initiatives. In Australia, a mobile premium services code had for example been introduced in 2009 by industry, requiring information disclosure on the premium service on offer, available complaints handling and opt-out mechanisms. To prevent consumers from contracting with suspect content providers, rules had also been developed by the Australian Communications and Media Authority (ACMA) considering in breach of law any MNO contracting with a content provider who was not listed on an industry register.

### ***Varying levels of consumer protection***

Despite the benefits that online and mobile payments provide to consumers, variations in the level of protection within and across countries, depending on the payment method used, the problem at stake, the nature of the product (tangible or intangible), and the parties involved (traditional financial institutions and emerging payment providers such as MNOs), was seen as a factor undermining confidence (Box 1). It was pointed out that the strong protections attached to the use of a credit card in most countries were not accessible to those who do not have a bank account (e.g. children, low income people).

The question of whether an equal level of protection should apply to all payments, regardless of the method used and the product bought (including intangible products), was thus raised. Ensuring that existing legislation be equally applied to all payment providers (including MNOs) was also highlighted. Mention was made in that regard of a legislative proposal developed by the Finnish Consumer Agency and under consideration, under which MNOs could be also held liable in case of problems with payments they had processed.

#### **Box 1. Legal and industry-led consumer payments protection in the United States**

**Credit card:** Under existing legislation, consumers may be held liable for up to USD 50 in case of unauthorised charges, non conformity, and non delivery.

**Debit card:** Delivery and conformity problems are not covered by any legal protection.

**Prepaid card:** The availability of any legal protection is unclear.

**Mobile payments:** The rules mentioned above would apply if a mobile payment was made with a credit, debit or prepaid card. So would the voluntarily protections implemented by payment card networks (e.g. *Visa* and *MasterCard*) introducing zero liability policies for credit and debit. But if the charge was made on the phone bill, under most US laws (except in California), consumers would have no legal protection for any problems associated with the payment.

### ***Examples of fraud and deceptive commercial practices***

A presentation was made on an emerging problem in Japan associated with payments intermediaries (so-called “payments agents”) which mainly affected e-transactions. Such entities, which can act in the place of merchants in the conclusion of a payment transaction with a Japanese credit card entity, are often operating overseas. Their intervention is appreciated by merchants who can benefit from low cost sale and customer information management. In growing instances however, some overseas payment agents have been used to conclude 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

difficulty in contacting overseas payments agents and getting refunds from them in case of payment-related issues, consideration is being given by the Consumer Affairs Agency to develop a publicly-available online registry containing information about payments agents and how these or other relevant stakeholders may be contacted by consumers in case of problems.

An example of mobile payments fraud in the United States was also provided. Consumer rules had been applied in a case where millions of SMS (including advertising of loan modification) sent to mobile phones had affected consumers who, depending on their mobile phone programme, had to pay a per message fee or go beyond the monthly limit of the number of messages they could receive.

While online and mobile fraud were seen as similar to offline fraud, an increase in potential consumers falling victim was noted by participants, in light of the following factors:

- Online and mobile payments in particular are increasingly accessed by children and individuals who may not know how to protect themselves in such a distant and rapidly evolving technology-based environment. 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, which had led to expensive bills.
- Private individuals may act as merchants.
- Payment is often requested in advance of delivery.
- Mobile devices can be easily lost or stolen.

Participants noted that enhancing consumer protection should be a shared responsibility between payment providers and merchants. The latter should in particular ensure that their e-commerce system is adequate, transparent, and safe. Consumer ability to take collective action against rogue traders was also seen as an important protection tool.

### ***Dispute resolution***

It was noted that as a first step in their attempt to resolve a problem, consumers should try and contact the merchant from whom the product was bought. However, this might not always be easy. Given, for example, the variety of parties potentially involved, consumers may be confused about who to turn to in case of problems. In the event of unauthorised charges, consumers may not even know who the merchant is and where to contact him.

It was suggested that when payment operators allow merchants to use their systems, the former should also have some level of responsibility towards the consumers (in the event a consumer tried to contact the merchant first). Civil society indicated that such responsibility may take the following forms:

- Ejecting a merchant from the payment system.
- Providing a toll free number of a party who could respond to consumers.
- Removing unauthorised charges or re-crediting the debit.
- Implementing easy-to-use dispute mechanisms which could be supplemented by alternative dispute resolution programmes and/or government recourse.
- Mechanisms aimed to help consumers protect themselves (such as parental control) should be free of charge.

- Educating consumers about their rights and responsibilities.

The upcoming review by the Committee of the 2007 *OECD Recommendation on Consumer Dispute Resolution and Redress* ([www.oecd.org/dataoecd/43/50/38960101.pdf](http://www.oecd.org/dataoecd/43/50/38960101.pdf)), it was noted, would examine payment issues.

### ***Security***

Security was singled out as one important factor that could enable and maintain consumer confidence in an e-commerce system. While such confidence was reported as growing in the United Kingdom, results of a mystery shopping survey showed that consumer perception and fears of payment security represented a barrier to online shopping across borders. In light of their difficulty to manage their own security in such a complex environment, consumers expected a role for online platforms, and mobile operators in particular, in providing redress and education about risks and ways to protect themselves.

### ***Interoperability***

A presentation was made on work being developed by the European Commission on the *Digital Agenda for Europe*. Preliminary findings showed a level of fragmentation of online and mobile payments means and a certain lack of interoperability of not only the technology being used but also the various systems in place. A clearer vision of how online and mobile payments should evolve in the future was needed. In such a context, in addition to regulatory thinking, standard compliance, industry-led initiatives, including trust marks, were all seen as helpful means to enhance confidence.

### **III. Next steps**

There was general agreement that the rising importance and rapid development of mobile commerce warranted ongoing attention.

Participants also commented on the way in which the existing guidelines could be applied to respond to current and emerging online and mobile payment issues. Looking at ways to empower consumers and improve education about online and mobile payment procedures, risks, as well as consumer rights and responsibilities in such an environment, were seen as important in this regard. What exactly such education, which should serve the purpose of helping consumers make informed choices when considering a transaction, should include, was however questioned.

Some felt it might be beneficial to explore ways that protection rules could be harmonised across payment platforms and jurisdictions. However, it was recognised that although important, such a task might be very difficult to achieve. Payment providers cautioned that the mobile payment marketplace is still nascent in most OECD countries and consumer rights and responsibilities are still evolving; it did not seem to be the right time to be exploring the issue of regulation and harmonisation.

A suggestion was made to examine the extent to which the existing framework could be applied to address issues. Looking at ways to empower consumers and improve education about online and mobile payment procedures, risks, as well as consumer rights and responsibilities in such an environment, was seen as important. In addition to education, the work could explore ways to improve consumer experience in online and mobile payments, looking at the issues raised in the payments background report including dispute resolution problems, specific mobile payments issues, and security. In doing so, the Committee could scrutinize which areas of the 1999 OECD e-commerce guidelines ([www.oecd.org/dataoecd/18/13/34023235.pdf](http://www.oecd.org/dataoecd/18/13/34023235.pdf)) should be completed to address these issues.

It was agreed that the Secretariat would work with the working group to develop policy issues that could be explored more fully. These would serve as a basis for the development of policy guidance in the area, which could include hypothetical examples, as was the case in the 2008 OECD policy guidance on mobile commerce ([www.oecd.org/dataoecd/50/15/40879177.pdf](http://www.oecd.org/dataoecd/50/15/40879177.pdf)). The work could look at how rules may impact on related areas, such as competition and trade. A first draft would be prepared for discussion at the CCP's October 2011 meeting.