

# TACD

TRANS ATLANTIC DIALOGUE TRANSATLANTIQUE  
CONSUMER DIALOGUE DES CONSOMMATEURS

DOC No. INFOSOC-32-05

DATE ISSUED: AUGUST 2005

---

## RESOLUTION ON MOBILE COMMERCE

---

### Introduction

Mobile commerce can be defined broadly as a business model that enables consumers to purchase goods or services using mobile phones (also integrated in other devices like personal digital assistants – PDA, etc. with access to mobile networks). While mobile commerce can provide great convenience for consumers in Europe (EU) and the United States (US), it can also pose certain risks that should be addressed now, at the early stages of its development. Mobile commerce is growing fast; Juniper Research predicts that by 2009 global mobile commerce revenues will be \$88 billion (USD), with \$39 billion in ticket purchases and \$299 million in phone-based retail POS (point of sale) purchases.<sup>1</sup>

### Types of Mobile Commerce

Currently, downloading ring tones and screen savers is the most common type of mobile commerce, but this will change over time as purchases of other types of mobile content increase. In this respect, mobile commerce is very similar to “900 number” or “premium rate” services. Mobile content can include stock quotes, weather forecasts, driving directions, and other information; it can also include interactive services such as polling, chat lines, and games. As mobile commerce develops, it will also offer the ability to purchase physical goods and services that are delivered or performed offline.

Consumers typically make purchases in mobile commerce by sending an advertised “short code,” a form of text message, to the vendor via a mobile phone. The charges may appear on the consumer’s mobile service bill, or the consumer could arrange for charges to be billed to a credit card or debited from a bank account or “e-wallet.”

Mobile devices are themselves becoming payment instruments. Consumers can hold mobile phones or for example PDAs equipped with Radio Frequency Identification Devices (RFID) next to readers in vending machines, in kiosks, in turnstiles, or at the counters in stores in order to pay for their purchases.

### Risks of mobile commerce

Consumer complaints and concerns about unfair business practices and fraudulent activities in connection with mobile commerce are increasing. They include:

- **Unauthorized purchases** made with a consumer’s mobile phone without that person’s knowledge or consent. Unless there is a PIN or some other form of

---

<sup>1</sup> <http://www.epaynews.com/statistics/mcommstats.html> accessed on July 12, 2005

authentication required, it is easy to use someone else's mobile phone to purchase something at that person's expense;

- **Marketing to children** who are using mobile phones but may not have the capacity or authorization to make purchases. Advertisements for ring tones, games, and other products or services popular with young people can be found in media (television, radio, Internet, and print publications) targeted toward children and adolescents;
- **Inadequate disclosures** in advertisements about the products and services offered, the cost, and the terms and conditions. Often the details of the transaction – for instance, that there will be a recurring monthly charge – are in fine print or are not made clear or easily-readable;
- **Deceptive solicitations** for products or services. Products and services may be misrepresented by fraudulent vendors;
- **Spam being sent** to mobile phones. Consumers may become deluged with unsolicited offers for mobile commerce;
- **Security of financial information** given to vendors to make mobile commerce transactions. Information could be intercepted in transmission or obtained surreptitiously by hidden RFID readers;
- **The disparity of dispute rights** depending on how payment is made. Dispute rights for unauthorized transactions and incorrect charges may differ according to whether the charges were placed on a telephone bill, billed to a credit card, deducted from an "e-wallet," or debited from a consumer's bank account. They also differ from country to country. In addition, consumers may not be protected from their mobile service being terminated for failure to pay disputed charges that were billed to their mobile accounts. They may also find it hard to prove the terms on which they purchased, if the details of transactions are not confirmed (e.g., on itemised phone bills);
- **Illegal activities** ranging from child pornography to gambling. Consumers may be able to partake of, and pay for, activities that are illegal in their jurisdictions;
- **Privacy and discrimination issues** related to tracking purchases and the locations of the device users. Mobile commerce vendors may be able to collect information about what goods and services consumers purchase and where they go, and use it for secondary purposes or share it with others. This could lead to more intrusive marketing and other uses of information about consumers' activities and locations that they neither expected nor desired. This information could also be used to identify the most profitable consumers and offer them the best deals, leaving less profitable consumers increasingly excluded from markets.

Adding to these concerns is the fact in some countries mobile commerce may not fall under existing laws or regulations. For example, in the U.S. it is not clear whether the Federal Trade Commission's 900 Number Rule, which requires specific disclosures, prohibits specific practices, and provides specific dispute rights in regard to pay-per-call services, applies to mobile commerce. Therefore, it is unclear what protections consumers have, where they can turn to for help if they have problems, and what authorities are empowered to bring action to stop bad practices and seek redress for consumers. Furthermore, since the applicable laws may differ from country to country, it is difficult for consumers to know what their rights are as they travel and use mobile commerce, for multinational companies to know what their responsibilities are, and for law enforcement agencies to take effective cross-border action.

## **Recommendations**

### **TACD therefore resolves that the EU and US governments should:**

1. Assess whether existing laws and regulations apply to mobile commerce, identify gaps, and examine inconsistencies in laws and regulations among EU member countries and between Europe and the US;
2. Solicit public input about appropriate consumer protections for mobile commerce via formal rulemaking proceedings, consultations, workshops, forums, and other means;
3. Examine the laws and regulations that may apply to mobile commerce in other regions of the world;
4. Fund research into the impact of mobile commerce on consumers, particularly those who are disadvantaged or vulnerable, such as children and low-income people. This research must be undertaken in a transparent, independent, and scientific manner;
5. Implement laws and regulations that are consistent and that:
  - Protect consumers from unauthorized transactions and provide cooling-off rights for situations where, for instance, consumers have purchased goods or services that have not yet been delivered, or where required disclosures have not been made;
  - Enable consumers to refuse payment or demand refunds for disputed charges without fear that their mobile accounts will be terminated;
  - Require vendors to take steps to ensure that purchases cannot be made by children without their parents' knowledge and consent;
  - Require clear and full disclosures about the products and services offered, the cost, and the terms and conditions in any commercial communication as well as immediately before any individual transaction;
  - Prohibit fraud and deceptive and misleading solicitations, and provide especially strong sanctions against such solicitations targeting vulnerable consumers;
  - Give special protection to children and restrict marketing practices targeting children;
  - Prevent unsolicited advertisements for products and services from being sent to consumers' mobile devices;
  - Provide effective and consistent payment dispute rights;
  - Provide consumers with the right to terminate any subscription of premium content or services with short notice;
  - Prohibit types of mobile commerce activities, such as gambling, based on the applicable laws of their respective countries;
  - Require that consumers' financial information is secured against external and internal abuse;
  - Protect consumer privacy in mobile commerce and prohibit use of any personal data (including purchase and location information) for purposes that consumers have not explicitly agreed to or that unfairly disadvantage them.

### **TACD further resolves that the EU and US governments should:**

Encourage mobile commerce vendors, billing and payment intermediaries, and other businesses involved in mobile commerce to develop best practices and self-regulatory programs that:

- Provide effective means of authenticating purchasers to prevent unauthorized transactions;
- Provide clear disclosure of cancellation rights and policies, and easy means for consumers to cancel;
- Mitigate losses for unauthorized transactions by limiting the amount of charges that consumers may make in mobile commerce transactions within specific time periods and for single transactions;
- Give all mobile phone users easy and inexpensive means to block all premium content and services to mobile phones, including the ability for parents to do so on phones they intend to provide to their children;
- Help parents identify content that may be objectionable for children through the use of uniform pictograms;
- Provide effective means for consumers to resolve disputes concerning mobile commerce;
- Set reasonable policies based on applicable laws in the countries in which their customers reside for the types of products and services that will be offered in mobile commerce and for which billing services will be provided;
- Prevent fraud and deception through careful screening of vendors for whom services will be advertised and billing services will be provided;
- Set good standards for advertising that will ensure clear and full disclosures;
- Prevent unsolicited marketing for mobile services and enable consumers to easily exercise their rights not to receive such solicitations;
- Protect the security of consumers' financial information through use of encryption and other technical measures, and by implementing effective internal security measures;
- Protect the privacy of consumers' personal information and refrain from using it for purposes that consumers have not explicitly authorized or for purposes that unfairly disadvantage them.