

International Consumer Protection and Enforcement Network Report on Mobile Payments

July 2014

Table of contents

Introduction.....	3
Executive summary	7
1. Market analysis.....	11
2. Consumer challenges related to mobile payments.....	17
3. Consumer protection – policy and law.....	21
4. Enforcement	24
5. Initiatives for mobile payments from industry associations and others.....	26
Conclusions.....	27
Annex I – ICPEN questionnaire on mobile payments.....	29
Annex II – Websites of responding authorities	33
Annex III – Policy developments and references	34

Introduction

In the past, consumers used mobile payments mainly to purchase digital services that they consumed on their mobile devices. Recently, however, consumers' use of mobile payments for purchases has expanded and now includes a wide range of goods and services. With consumers' increasing use of mobile devices, which now includes smartphones and computer tablets, this expansion is ongoing.

To gain more knowledge about mobile payments and related consumer challenges, the International Consumer Protection Enforcement Network ("ICPEN"), a network of more than 50 governmental consumer protection agencies from around the world, initiated a project on mobile payments.¹ The objective was to identify consumer issues relating to mobile payments and to produce a report on the types of challenges reported by consumers and consumer protection authorities regarding these issues.

To this end, ICPEN formed a working group on mobile payments ("Working Group"). The Working Group is currently led by the Norwegian Consumer Ombudsman and consists of consumer agency representatives from Canada, Italy, Latvia, Portugal, Sweden, the United Kingdom (UK), and the United States (U.S.), as well as members of the Secretariat of the Committee on Consumer Policy of the Organization for Economic Co-operation and Development ("OECD"). This report summarizes the information collected and analyzed by the Working Group, and contains numerous examples of consumer challenges and initiatives to address them. It also contains a section on conclusions and highlights some suggestions by ICPEN members for next steps to improve consumer protection in this rapidly changing area.

A. ICPEN

ICPEN is a network of governmental consumer protection authorities from over 50 countries around the globe. It was founded in 1992 by consumer protection agencies from several OECD countries, and has expanded in recent years to include agencies from Africa, Latin America, and Southeast Asia.² The network operates under a rotating presidency, currently held by Sweden's consumer agency, Konsumentverket.

ICPEN members share information about cross-border commercial activities affecting consumers and encourage international enforcement cooperation among its member consumer protection agencies. ICPEN conducts its work through three main steering groups: Enforcement, Intelligence, and Best Practices. ICPEN also carries out work through ad hoc working groups.

¹ See International Consumer Protection and Enforcement Network at <https://icpen.org>.

² Delegates from Australia, Austria, Belgium, Canada, Denmark, France, Finland, Germany, the Netherlands, Hungary, Ireland, Japan, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and the United States established the Network in 1992, with participation from representatives of the OECD and the European Union (EU). Greece, Italy, and Luxembourg joined shortly thereafter. Mexico became a member of the network in 1994. Malta, the Republic of Korea, Poland, Slovakia, and the Czech Republic joined in 1996, followed by Latvia and Estonia in 2002, Lithuania in 2003, Cyprus and Chile in 2005, Azerbaijan and China in 2006, Costa Rica, Egypt, El Salvador, and Turkey in 2010, Barbados and Panama in 2011, Bulgaria, Mongolia, and Papua New Guinea in 2012, Israel, Nigeria, Vietnam, and Colombia in 2013, and the Dominican Republic, the Philippines, the Seychelles, and Zambia in 2014. Partner organizations represent five countries and include Angola, Suriname and Peru in 2013 as well as Kosovo and Kenya in 2014. Partners are eligible for membership after two years and active engagement in ICPEN.

In recent years, ICPEN members have developed enforcement training manual resources to assist newer agencies in developing tools and techniques for consumer protection enforcement, conducted web-surfing sweeps to identify cross-border e-commerce issues, and facilitated “best practices” workshops and training events. Several of the newer ICPEN projects have been specifically designed to focus on emerging threats to consumers, including work regarding children’s online games and apps, negative options (recurring billing) and civil-criminal law enforcement efforts.

One of the key ICPEN collaborative efforts is econsumer.gov, a cross-border complaint portal for consumer protection agencies. The project consists of the multilingual public website, on which consumers lodge cross-border complaints, and the password-protected website, through which the incoming complaints are shared with the participating consumer protection authorities.

As noted above, many ICPEN members are members or observers of the OECD, and participate in the activities of the OECD’s Committee on Consumer Policy. In connection with its work on mobile payments, ICPEN members have contributed to the OECD’s work on mobile payments, which includes a *Consumer Policy Guidance on Mobile and Online Payments* issued in March 2014.³ Accordingly, this report includes some references to the OECD’s document.

B. Scope, Methodology and Limitations

1. Scope

For the purposes of this report, the Working Group has defined “mobile payment” as any sort of payment for goods or digital/regular services initiated, transmitted, or confirmed via a mobile phone or device, billed by a mobile network operator, card company/bank, or other.⁴ The broad definition is intended to include as many different types of mobile payments as possible.

This report, however, does not cover payments made using a mobile phone browser as part of traditional e-commerce. Specific aspects of fraudulent or exploitative schemes, such as malicious mobile phone apps and premium rate scams, are also outside the scope of this report.⁵ The Working

³ The Organization for Economic Development and Cooperation (OECD), *Consumer Policy Guidance on Mobile and Online Payments*, April 4, 2014, available at: http://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-mobile-and-online-payments_5jz432cl1ns7-en . A background report on mobile and online payments was also issued by the OECD in April 2012.

⁴ This report follows the definition provided in the European Commission’s Green Paper *Towards an integrated European market for card, internet and mobile payments*, published in January 2012, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0941:FIN:EN:PDF>. The recently released OECD *Consumer Policy Guidance on Mobile and Online Payments*, which covers mobile and online payments, contains a similar definition: ...“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.” (2014:5)

⁵ The London Action Plan (“LAP”) is a network of government and public agencies responsible for enforcing laws concerning spam and other messaging abuses that was founded in October 2004 by 27 countries with the purpose of promoting international spam enforcement cooperation. Since inception, the LAP has expanded its mandate to include online and mobile threats, including malware, SMS, spam and Do-Not-Call. See www.londonactionplan.org . Several ICPEN members also participate in the LAP. The LAP works closely with the industry-affiliated Mobile, Malware and Messaging Anti- Abuse Working Group (“M³AAWG”). See

Group notes, however, the close link between general consumer challenges with mobile payments and the possibility that mobile payment systems can be used by fraudulent operators to tap into consumers' financial accounts, obtain consumers' personal information illegally, or otherwise compromise their privacy and security. It does, however, touch on mobile banking as this is the most common or only form of mobile payment in some of the survey respondents' countries.

2. Methodology

To survey the market for mobile payments, and to identify current and future consumer challenges with mobile payments, the Working Group issued a questionnaire, which was circulated among ICPEN members, partners, and observers during the spring of 2012.

The questionnaire (see Annex I) consisted of five sections: (1) Market Analysis; (2) Consumer Challenges; (3) Consumer Protection – Policy and Law; (4) Enforcement; and (5) Industry Initiatives. The Working Group received 28 responses to the questionnaire from ICPEN member countries, partners, and observers. Of these, consumer agencies from European countries provided more than one-half of the answers (16) while consumer agencies from North and South America provided one-quarter of the answers (7). Countries in Oceania (2), Asia (2), and Africa (1) also provided survey responses. (A list of the websites of responding authorities is set forth in Annex II.) This report follows the same structure as the questionnaire and incorporates the results of each section of the questionnaire.

3. Limitations

The development of mobile payments has reached different stages in different markets with noticeable variations in market conditions. As a result, some respondents were unable to answer some of the questions in the questionnaire, while others raised local variations of mobile payment mechanisms of which the Working Group was not previously aware. Moreover, at the time of the questionnaire, some survey respondents may not have had a complete overview of the market situation in their country, perhaps causing some omissions in the report compared to the actual market conditions. This report endeavors to take into account these differences by referring to, and to some extent, trying to compare interesting local or regional developments in mobile payments.

Understanding that the market for mobile payment services is evolving rapidly, and many new technologies and business models have surfaced in the two years since the Working Group first disseminated the questionnaire, this report may not reflect all developments in this area. Indeed, while compiling this report, the Working Group received notice from some survey respondents that market conditions in their countries had already changed from the time when they first answered the questionnaire to the present. This rapid development calls for a certain approach to the information and conclusions in this report: Instead of focusing on any particular technology or development, the report emphasizes cross-cutting issues that may cause consumer challenges across differing mobile payments markets, business models, and technologies. The report also highlights

www.maawg.org . The two organizations developed a joint report *Best Practices to Address Online and Mobile Threats*, October 15, 2012, available at: http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf .

ideas and solutions ICPEN members are developing to address these issues that may have broad applications as new mobile payment systems and new business models emerge.

Executive summary

This report summarizes and analyzes the issues new and emerging mobile payment systems and mechanisms present for consumers and consumer protection agencies. It is based on responses to the questionnaire developed by the ICPEN Working Group on Mobile Payments as well as independent reports and policy documents. It is divided into five sections: (1) Market Analysis; (2) Consumer Challenges; (3) Consumer Protection – Policy and Law; (4) Enforcement; and (5) Industry Initiatives. After providing an overview of these five issues based on the survey responses, the report draws some conclusions, and then provides some suggestions for future steps.

(1) Market analysis

Mobile payments are a small but growing financial service in most ICPEN countries. While official statistics are scarce, some form of mobile payments is available to all consumers with a mobile phone. The number of active smartphones capable of containing a variety of mobile payment options is growing in most markets, and some estimate that the value of mobile payments transactions will exceed \$700 billion by 2017.

There are various pilot projects underway in many ICPEN countries, often as a joint effort between one or more mobile network operators and financial institutions.

In other countries, consumers are already using mobile payment mechanisms. Although mobile payments relating to premium SMS (Short Messaging Services) charged to consumers' mobile carrier bills remain the most widely used mobile payment mechanism, new mobile payment business models and services are emerging.

(2) Consumer challenges

In many responding countries, mobile payments relating to premium SMS services present the most problems for consumers. In particular, unclear and insufficient information can lead consumers to pay for services they thought were free, or to subscribe to services with recurring charges that they thought were only one-off charge services. In addition, consumers are often faced with fraudulent or unauthorized charges on their mobile carrier bills, a practice often referred to as "cramming." Some ICPEN respondents see stronger authentication and authorization procedures as a solution to address this type of problem as long as implementation of such schemes is weighed against the usability of the payment service.

Unclear billing information from the mobile network operators regarding mobile payments is another reported consumer challenge, which makes it difficult for consumers to fight unlawful charges on their bills or to recover prepaid credit.

Many children have access to mobile devices that they can use to make purchases using a mobile payment mechanism. As children may not be aware of the binding nature of the transactions they enter into when carrying out mobile payments, this may also cause problems.

The unclear division of responsibilities among the mobile network operator, the financial institution, and the provider of the good or service, experienced by consumers with mobile payments transactions, was frequently cited as problematic by ICPEN survey respondents.

Some respondents stated that these consumer challenges can be solved by legally requiring the mobile network operators to give consumers the same level of protection granted to them by credit card issuers. Given that the means of different payments essentially offers the same service to consumers, some respondents stated that consumers should enjoy the same level of protection for all types of payment services.

(3) Consumer protection – policy and law Few of the responding countries have specific laws aimed at regulating mobile payments, although some agencies are using their general consumer protection authority to develop policies and enforcement measures in this area.

Whether consumers have the same rights when purchasing goods and services with mobile payments instead of traditional means of payment or not varies among the ICPEN member countries. In some countries, mobile payments charged on the mobile phone bill are considered as credit card transactions, with consumers therefore enjoying the same level of protection when purchasing with their mobile phone or with their credit card. In most countries, however, consumers often have less protection when paying with mobile payments in comparison to traditional means of payment that are regulated by specific laws or regulations, such as debit or credit cards. For the main part, consumers are usually provided with the same legal protections that apply to credit and debit card transactions when they use mobile payment mechanisms that rely on debit or credit cards. However, the consumers' legal protections may vary when mobile payment transactions are carried out through alternative payment mechanisms.

In a number of jurisdictions, policymakers require that all mobile payments are subject to a double opt-in procedure with a Personal Identification Number (PIN)-code or similar security procedure. In other countries, no specific security procedures for mobile payments have been adopted, or if they have, there is a mixed approach where some payments are protected with security procedures while others are not. In some cases, security procedures such as double opt-in are implemented by mobile payment providers through adherence to a self-regulatory code, as discussed in further detail, below.

Some authorities point out that mobile phones have limited security measures to prevent unauthorized transactions. This concern is amplified in cases of theft of the mobile phone or other situations where misuse can occur.

Some authorities assert that mobile payments must be regulated by law to create a free and competitive market with low barriers for market entry, which in turn will secure fair and cost effective services for the consumers.

(4) Enforcement

Most ICPEN authorities can enforce consumer laws regarding misleading and deceptive marketing practices. Protections against such practices are indispensable in building consumer confidence and trust between businesses and consumers in online and offline commercial transactions.

Although some authorities can apply this general consumer protection enforcement authority to mobile payments-related practices, some authorities may require more specific legislation. Some authorities assert that such protections are needed for mobile payment transactions because the information supplied to consumers may not be disclosed properly in the mobile context or such information may lack the necessary transparency for consumers to make an informed decision. Others suggest that the prevalence of fraudulent and misleading practices, such as negative options billing scams that take advantage of mobile payment mechanisms, may require additional protections.

To date, not many ICPEN authorities have taken enforcement action regarding consumer problems with mobile payments. There is no clear reason for the low number of enforcement actions. One possibility is that these are fairly new services so existing laws may be inadequate to deal with mobile payments. Another reason is that these services span different markets and are often co-regulated by various authorities. Other authorities may be constrained by their lack of relevant enforcement authority. For example, only a few agencies state that they have the authority to initiate or intervene in civil disputes. Accordingly, mobile payment issues may be outside of the jurisdiction of many consumer protection agencies. Even fewer agencies state that they have the ability to initiate collective redress proceedings on behalf of the consumers. Consequently, most of the responding agencies must cooperate with other governmental and non-governmental organizations to assist consumers.

Recently, some authorities have begun to bring or consider enforcement actions relating to mobile payments. For example, in 2012, the Canadian Competition Bureau initiated legal proceedings against Bell Canada, Rogers Communications, Inc., TELUS Corporation, and the Canadian Wireless Telecommunications Association (CRTC), requiring them to stop misleading advertising that promotes costly "premium texting services," and to compensate consumers.

In 2014, the US Federal Trade Commission (FTC) brought an enforcement action against Apple, Inc. alleging that the company billed consumers for millions of dollars of charges incurred by children in kids' mobile apps without their parents' consent.⁶ To settle the charges, Apple agreed to pay a minimum of \$32.5 million to consumers and change its billing practices. In a significant effort to end mobile cramming, the FTC has also filed several lawsuits against alleged mobile cramming operations, including Jesta Digital, Wise Media, and Tato Inc., T-Mobile USA Inc.⁷ and, more recently, issued a Mobile Cramming Staff Report giving industry guidance.⁸ Elsewhere globally, in 2013, the

⁶ U.S. Federal Trade Commission, Press Release, *Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent*, January 15, 2014, available at: <http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million>.

⁷ U.S. Federal Trade Commission, Press Release, *FTC Alleges T-Mobile Crammed Bogus Charges onto Customers' Phone Bills*, July 1, 2014, available at: <http://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-t-mobile-crammed-bogus-charges-customers-phone-bills>.

⁸ U.S. Federal Trade Commission, Press Release, *FTC Recommends Mobile Industry Changes to Combat Mobile Cramming*, July 28, 2014, available at: <http://www.ftc.gov/news-events/press-releases/2014/07/ftc-recommends-mobile-industry-changes>.

UK's former Office of Fair Trading⁹ released final principles relating to payments for online and in-app games and warned games producers that they must comply with consumer protection laws or face enforcement action.

(5) Initiatives from industry associations and others

There are quite a few initiatives by other stakeholders besides consumer protection authorities that reportedly aim to increase consumer protection with mobile payments. The majority of these initiatives are concerned with establishing codes of conduct or similar guidelines that various players will employ in the mobile payment services market.

Some responding authorities also report on specific efforts by industry associations and others, such as implementing specific security mechanisms or providing alternative dispute resolution systems ("ADR") and consumer education. Most initiatives seem to have originated from consumer protection authorities, while others are more directly attributable to the industry or non-governmental organizations (NGOs).

Conclusions

The emergence of mobile payment mechanisms has provided consumers with new opportunities to engage in e-commerce, but has also provided them with new challenges, which consumer protection authorities are beginning to address. The main issue that emerged from the ICPE questionnaire is the difference in the levels of consumer protections between mobile payments and more traditional payment mechanisms. In the view of many consumer protection agencies, consumers should enjoy the same high level of protection regardless of the type of payment services they use. The types of protections consumer authorities have recommended include, adequate authentication and authorization procedures for consumer transactions, limitations on the consumers' total liability when using mobile payment mechanisms service, and limitations on consumers' liability for unauthorized charges or costs occurred after the theft of a mobile device or SIM card.

These types of issues are already being considered domestically and internationally. The OECD has recommended that "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."¹⁰ Some consumer authorities have already implemented these protections while others are in the process of developing regulatory and self-regulatory solutions. The information contained in this report is intended to aid that process.

⁹ The UK Office of Fair Trading was responsible for protecting consumer interests throughout the UK. It closed on April 1, 2014 with its responsibilities passing to a number of different organizations including the Competition and Markets Authority (CMA) and the Financial Conduct Authority (FCA).

¹⁰ The Organization for Economic Development and Cooperation (OECD), *Consumer Policy Guidance on Mobile and Online Payments*, April 4, 2014:17, available at: http://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-mobile-and-online-payments_5jz432cl1ns7-en .

1. Market analysis

Mobile payments are a small but growing financial service in most ICPEN countries. For this reason, there is limited statistical information from official sources about the use and prevalence of mobile payments in the payment services market. Nonetheless, some ICPEN countries have begun to collect this information.

For example, according to statistics from Germany, mobile payments are available to 40 percent of Germans, and 56 percent of Germans are interested in doing mobile payments. In the United States, the Board of Governors of the Federal Reserve System released two reports – one in March 2012 and one in March 2013 – which together provide a good snapshot of consumer usage of mobile payments in the United States.¹¹ According to the March 2012 report, only 12 percent of mobile phone users had made a mobile payment in the previous year; however, the number was higher for mobile banking (21 percent). By the March 2013 report, the percentage of mobile phone users that had made a mobile payment in the previous year was up to 15 percent, while the number of consumers that engaged in mobile banking grew even more rapidly. (Indeed, by 2013, 28 percent of all mobile phone users had used mobile banking in the past 12 months.) The most common use of mobile payments by consumers, according to the March 2013 report, was to pay bills online (42 percent of mobile payment users, down from 47 percent in 2011). Significantly, according to the March 2013 report, six percent of all smartphone users had made a point-of-sale payment using their phone in the past year, up from one percent in December 2011, and 22 percent of all mobile phone users expressed an interest in using their phones to buy things at the point of sale.

Despite the lack of official statistics, many industry observers expect that consumers' use of mobile payments will increase in the next few years. Gartner, Inc., a global information technology firm, recently predicted that worldwide mobile payment transaction values would increase from an estimated \$235.4 billion in 2013 to \$721 billion by 2017, with a corresponding increase in an estimated 245.2 million mobile payment users worldwide in 2013 to more than 450 million users by 2017.¹² Also, according to an April 2012 study by the Pew Internet and American Life Project, "The Future of Money in a Mobile Age," by 2020, most consumers will have embraced and fully adopted the use of smart-device swiping for purchases, nearly eliminating the need for cash or credit cards.¹³ This is also supported by public statements of former Chief Executive Officer and President of Visa Europe, Peter Ayliffe, who predicted that 50 percent of Visa's transactions would be carried out on a

¹¹ The U.S. Federal Reserve's findings are based on two online surveys, the first conducted in December 2011 and January 2012, and the second conducted in November 2012. Both surveys examined US consumers' use of mobile technology to access financial services and make financial decisions. They used a broader definition of mobile payments than the one used in this report with the inclusion of browser-based mobile payment services in each of the surveys. See Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services - March 2012*, available at: <http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf> and Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services 2013 - March 2013*, available at: <http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf>

¹² Gartner Research, Inc., Press Release, *Gartner Says Worldwide Mobile Payment Transaction Value to Surpass \$235 Billion in 2013 - Gartner Predicts That Asia/Pacific Will Overtake Africa to Become the Largest Region*, June 4, 2013, available at: <http://www.gartner.com/newsroom/id/2504915>.

¹³ Pew Research Internet Project, *The Future of Money in a Mobile Age*, April 2012, available at: <http://www.pewinternet.org/Reports/2012/Future-of-Money.aspx>

mobile device by 2020.¹⁴ The Pew study, however, cautioned that mobile payment adoption in the United States will unfold relatively slowly due to a combination of concerns over privacy, a desire for anonymous payments, demographic inertia, a lack of infrastructure to support widespread adoption, and resistance from those with a financial stake in the existing payment structure. Indeed, in the March 2013 report from the Federal Reserve, of the consumers who had not made a mobile payment in the past year, 38 percent (down from 42 percent in 2012) stated that they did not do so due to concerns about security; 36 percent reported that it is easier to pay with other methods, such as cash or credit card; and 35 percent reported that they did not see any benefit from using mobile payments. Only 30 percent said they did not have the necessary features on their phones. Based on the survey responses to the ICPEN questionnaire, it is clear that consumers in ICPEN countries share these concerns.

The survey responses showed that the most common mobile payment mechanism in ICPEN countries are payments associated with SMS premium services that are charged to a consumer's mobile carrier phone bill. Nonetheless, new mobile payments mechanisms are emerging. In several ICPEN countries, pilot projects are being conducted at retail outlets with Near Field Communication (NFC)¹⁵ payments. In most countries, the mobile network operators appear to be driving these pilot projects, sometimes together with a bank or other financial institution. By contrast, in other countries, third party companies are pushing the evolution of mobile payments. An example of such a company is Paybox, which delivers payment services in Austria and several other countries. In July 2012, the Association of Hotels, Restaurants and Similar Services of Portugal announced its pilot project that mobile payments would be made available to all of its consumers by 2013. Interestingly, this strategy was marketed as a response to high fees on credit and debit card payments.

Because there are many different organizations and governments trying different pilot projects, the mobile payments market is fragmented and diverse in most countries. As a result, in some countries, such as Norway, Sweden, and the United States, the major mobile network operators have formed joint ventures with outside companies, which handle a large percentage of mobile payment transactions.

The survey responses note that mobile network operators play a larger role in the market for digital services than in the market for tangible goods and services, thereby acting at the same time as the service provider, financial instrument provider, and payment collector. The fact that mobile network operators can play all of these roles in the market can create some difficulties and confusion for consumers, as discussed below.

¹⁴ See http://www.visaeurope.com/en/newsroom/news/articles/2012/visa_europe_backs_mmn.aspx. On August 7, 2013, Visa Europe announced the appointment of Nicolas Huss as its next President and CEO, beginning on October 1st. See: http://www.visaeurope.com/en/newsroom/news/articles/2013/new_ceo_appointed.aspx

¹⁵ Using electromagnetic radio fields, Near Field Communication (NFC) technology lets smartphones and other enabled devices communicate with other devices containing a NFC tag. See <http://www.nearfieldcommunication.org/>

a. Types of transactions

When mobile payments are used to pay for tangible goods and services, there may be a credit card or another financial instrument that carries the transaction. In these transactions, the mobile device is usually seen as a carrier for the financial instrument performing the transaction. Many of these transactions use NFC or other technologies. The most common services that have introduced NFC-enabled mobile payments are small purchases at grocery stores, kiosks, and gas stations; and ticketing purchases like the cinema, parking, or public transport.

On the other hand, when digital services such as ringtones, movies, music, and digital subscriptions to magazines and newspapers are purchased using mobile payments, the purchase tends to be charged directly to the consumers' phone bill as a premium SMS service.

An exception to the divide between tangible and digital goods and services is the purchase of goods from vending machines or other automated sales points. Here the majority of non-cash transactions are carried out through premium SMS services and charged directly on the consumer's phone bill.

However, as the market for mobile payments continues to evolve, alternative payment systems may emerge. For example, on Apple iOS devices, purchases of digital content such as apps, music, and movies are made through the consumer's iTunes account, which may be billed via some other mechanism.

The market for app-based payments has been around since Apple Inc. released its second generation of iPhone, the 3G, and the App Store opened in 2008. Today, the use of smartphones and apps is common among most consumers. For example, 90 percent of the mobile phones sold today in Norway are smartphones, and the total penetration of smartphones is over 50 percent. According to the March 2013 Federal Reserve Report, mobile phones and mobile Internet access are in widespread use by Americans. Eighty-seven percent of the US adult population has a mobile phone, and 52 percent of these are smartphones (Internet-enabled).¹⁶ Norwegian consumer authorities report that over one-half of consumers in their country are equipped to do app-based transactions. One growing trend is the marketplace for app-based payments is a move from a business model offering consumers both pure "free" and paid premium apps to one based on "free" apps with in-app purchases (so called "freemium" apps). These freemium apps can be used for services such as new editions of newspapers and magazines, additional levels in games, and for the payment of offline goods and services, including parking and movie theatre tickets.

b. Consumer Risks

Consumers are generally more at risk when using mobile payment mechanisms to obtain premium SMS services, rather than credit cards or other financial instruments. This is because, in most countries, there are generally:

¹⁶ Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services – March 2013*, available at: <http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf>

- No laws or regulations that apply directly to premium SMS transactions or that protect consumers from fraudulent and unauthorized charges on mobile carriers bills, and
- Less security mechanisms in place; in most countries, there is:
 - no requirement of authorization of the transaction,
 - no authentication of the payer, and
 - no limitation on the consumer's liability if the device is stolen.

Nevertheless, several countries are the exception to this general rule. In the Dominican Republic, premium SMS transactions must be authorized by consumers using a PIN-code. In Finland, an interoperable multi-operator Mobile ID was launched in March of 2011. In the future, this method can be used to establish more secure mobile payments, but, to date, the service has not been applied for such purpose. In Germany, the mpass¹⁷ payments service, launched in 2013, connects the consumer's mobile number with the consumer's bank account, allowing premium SMS transactions to be charged directly on the account. In case of theft, an SMS/TAN procedure¹⁸ is in place that allows the SIM card to be blocked to avoid the misuse.

In the United States, most of the major mobile carriers entered into an agreement at the end of November 2013 with forty-five of the states' attorneys general to end premium SMS billing by the end of January 2014 in an effort to end mobile cramming.¹⁹ Premium SMS billing had accounted for the majority of third-party charges on cell phones and for the overwhelming majority of cramming complaints by consumers in the United States. On July 1, 2014, the FTC announced that mobile phone service provider T-Mobile USA Inc. had been charged with making hundreds of millions of dollars by placing charges on mobile phone bills for purported "premium" SMS subscriptions that, in

¹⁷ Telefonica, Press Release, *DLD Conference 2013: Telefonica introduces mobile-to-mobile money transfers and digital wallet*, January 21, 2013, available at: <http://blog.digital.telefonica.com/?press-release=telefonica-mobile-digital-wallet>

¹⁸ TAN stands for Transaction Authentication Number. This service is used by some online and mobile banking services to authorize financial transactions. TANs are series of one-time passwords used as a second layer of security above and beyond the traditional single-password authentication (or PIN)-code.

¹⁹ The settlement, which was spearheaded by the Attorney General of Vermont, is with AT&T Mobility, Sprint and T-Mobile US. AT&T, Sprint, and T-Mobile are the second, third and fourth largest providers of mobile telephone services nationwide. See Press Release, Office of the Attorney General of Vermont, *AT&T Mobility, Sprint and T-Mobile Will Stop Billing Problematic Third-Party Charges* (Nov. 21, 2013), available at: <http://www.atg.state.vt.us/news/att-mobility-sprint-and-t-mobile-will-stop-billing-problematic-third-party-charges.php>. Some of the companies will still support text-to-donate for charitable programs and text-to-contribute for political campaigns. The largest wireless carrier in the U.S., Verizon Wireless, not part of the settlement, has discontinued the practice with the exception of charitable donations. See Verizon Wireless, Premium Messaging FAQs, available at: http://support.verizonwireless.com/support/faqs/Premium_TXT_and_MMS/fag_premium_txt_and_mms.html. Industry observers expect most of the major carriers to move to a "direct carrier billing" (also known as "direct operator billing") business models, in part, to better monetize the value of mobile payments; however, there are potential consumer problems with this model as well.

many cases, were bogus charges never authorized by its customers.²⁰ And on July 28, 2014, the FTC issued a Mobile Cramming Staff Report giving industry guidance.²¹

However, most countries fall under the general category in which consumers are more at risk when using premium SMS services rather than credit cards or other similar financial instruments because of a lack of applicable law and mechanism in place. In Europe, there has also been some uncertainty as to whether mobile network operators are offering regulated payment services or issuing e-money, which requires them to be authorized or registered with the relevant competent authority, as there is room to interpret the relevant EU legislation in different ways.²² Based on the responses to the ICPEN questionnaire, only one of the mobile operators in Europe has registered or applied for authorization as a payment service provider or e-money issuer, while the remaining mobile operators have instead partnered with credit institutions that can provide payment services or issue e-money to the mobile network operator's customers or their own customers through the mobile device. In contrast, as mentioned above, in some countries, the major mobile network operators have formed joint ventures, which handle the mobile payment transactions on their behalf. These joint ventures will require, at least under European law, authorization from the relevant competent authority if providing regulated payment services or issuing e-money.

Other countries are attempting to bridge the gap and implement similar solutions. In Mexico, the financial and telecommunications authorities have been the driving force, together with the industry, behind an initiative to link bank account details with telephone numbers, allowing mobile phones to be used as a regular credit or debit card. The regulation in Mexico is specifically designed to allow for various arrangements of market players to offer mobile payment services and to ease implementation of new technology. So far, the regulation has paved the way for the service platform "Transfer," launched in Mexico in 2012.²³ This payments system is similar to Germany's mpass service mentioned earlier. A similar initiative is on its way in the United Kingdom, where the UK Payments Council is working on facilitating the development of mobile payment services by UK banks and building societies by establishing a central database that links account details to telephone numbers.

Some ICPEN responding countries reported specific consumer challenges with in-app purchases, especially in relation to cost as these are usually greater than those of traditional free or premium apps. Two reasons for these concerns include: (1) the reduced security mechanisms and in-app

²⁰ U.S. Federal Trade Commission, Press Release, *FTC Alleges T-Mobile Crammed Bogus Charges onto Customers' Phone Bills*, July 1, 2014, available at: <http://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-t-mobile-crammed-bogus-charges-customers-phone-bills>

²¹ US Federal Trade Commission, Press Release, *FTC Recommends Mobile Industry Changes to Combat Mobile Cramming*, July 28, 2014, available at: <http://www.ftc.gov/news-events/press-releases/2014/07/ftc-recommends-mobile-industry-changes>.

²² Some but not all mobile payment services are regulated payment services as defined in the Payment Services Directive (2007/64/EC), See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF>

²³ "Transfer" is a mobile money service, in Mexico, launched by Latin American operator group América Móvil on a joint basis with its banking partners, Citibank's Mexican unit Banmex and Banco Inbursa. It was designed to enable consumers to make financial transactions in real time from a mobile device through SMS messaging. See <http://www.telecoms.com/42967/mobile-money-service-to-serve-unbanked-in-mexico/>

purchases that are often used in games, and (2) other apps that are marketed towards children who do not understand the binding nature of the purchases. However, payment for apps and in-app purchases is usually completed with a credit card, which means that consumers tend to be fairly well protected by law for these transactions. Moreover, some authorities have taken steps to address these issues as described elsewhere in this report.

2. Consumer challenges related to mobile payments

a. Information and disclosure

Almost all respondents to the ICPEN questionnaire reported high numbers of consumer complaints regarding mobile payments, particularly with premium SMS services. A keyword phrase that appears in most complaints is “insufficient disclosure and information.” This issue is addressed at length in the OECD Consumer Policy Guidance on Mobile and Online Payments, cited earlier in this report, that includes recommendations that consumers could benefit from better information on mobile payments. These recommendations include the need for guidance on the clarity, transparency, completeness, and timeliness of information for consumers regarding the terms and conditions and costs of transactions, as well as guidance on providing consumers with information about the level of consumer protection and dispute resolution and redress procedures.

Insufficient disclosure and information can lead consumers to pay for services they thought were free, or subscribe to services with recurring charges that they thought were free or a one-off charge service. Several authorities also found that consumers struggle to end services with recurring charges.²⁴

For instance, in Korea, it is possible to purchase digital content just by clicking on an image of the service. Hence, the Korean Consumer Agency found insufficient authorization procedures together with equally insufficient information about pricing and the main characteristics of the product are a major problem.

Israeli authorities also noted that their biggest consumer challenges pertained to information disclosures, such as: (1) ensuring that consumers are aware that they are entering into a contract; (2) that the substantive information regarding the transaction is clear and conspicuous, including details as to the duration of the transaction, its cost, and information regarding the consumer's right to cancel the transaction; and (3) that the content providers act according to their obligations under Israel's Consumer Protection Law, including their obligation to enclose a disclosure document.

Some respondents favor stronger regulation of the traders' duty to adequately disclose and inform consumers who carry mobile payments transactions because the screen of the mobile device and the format in which the information is presented may be used to intentionally obscure the terms and conditions of a contract. The OECD Consumer Policy Guidance contains several recommendations for policy makers and industry stakeholders on information disclosure designed to remedy these problems, including a recommendation that consumers be provided with clear, easy-to-use procedures for preventing automatic renewals of contracts and for terminating recurring charges.

²⁴ See, for example, Federal Trade Commission, *FTC Reply Comment Before the Federal Communications Commission Concerning Placement of Unauthorized Charges on Wireless Bills, Otherwise Known as “Cramming”*, CG Docket Nos. 11-116, 09-158, and 98-170, Matter No. P104403, July 2012, available at: <http://www.ftc.gov/policy/policy-actions/advocacy-filings/2012/07/ftc-reply-comment-federal-communications-commission>

b. Authorization and authentication

Many other authorities report significant problems due to the lack of authorization and authentication protocols for certain types of mobile payment transactions. Some ICPEN respondents would like to see legislation that imposes an authorization scheme for mobile payment transactions similar to that used for payments with debit and credit cards. Such a scheme would ensure that relevant price information is disclosed to the consumer before the purchase is completed and that the contract is concluded with the correct person. It would also prevent fraudulent purchases made with mobile devices in cases of theft.

On the other hand, the implementation of authorization procedures for mobile payments has to be weighed against the usability of the payment service. Accordingly, some respondents, like the Danish Consumer Ombudsman, have suggested that low value transactions should not require authorization or authentication by the purchaser. However, the Danish Consumer Ombudsman does note the challenges that would still arise as consumers are often oblivious to the dangers connected with mobile payments without such security measures. There is also a concern on the part of some authorities that low value charges can add up and cause consumers financial detriment.

c. Billing issues

Some ICPEN authorities reported that unclear billing information from mobile network operators regarding mobile payments was problematic. A bill from a mobile operator will typically state “premium rate services” and a sum, but both the vendor of the service and the time of purchase are usually not included. This can make it difficult for consumers to fight unauthorized charges on their bill or prepaid credit.

The practice of “mobile carrier billing,” which offers service providers the ability to charge payments directly to a mobile phone bill, has been increasing in the United States and in other jurisdictions as a growing number of third-parties enter into agreements with carriers to place charges on mobile bills. Concurrently, the mobile carrier billing platform raises a unique challenge for authorities with regard to the third-parties’ practice of placing fraudulent or unauthorized charges on consumers’ mobile carrier bills (known as “cramming”). Some ICPEN respondents suggested strategies to ensure that cramming does not occur; these include: (1) permitting consumers to block all third-party charges on their mobile phone bills (including the ability to block third-party charges on individual accounts operated by minors in the household); (2) requiring mobile carriers to establish clear and consistent processes for consumers to dispute suspicious charges and obtain reimbursement; and (3) requiring mobile carriers to standardize and prominently highlight billing descriptions of third-party charges in a format that makes it clear why the consumer is being billed for a third-party charge, the provider or merchant that placed the charge, and the good or service provided.²⁵

²⁵ See *id.* and FTC Staff Report, *Paper, Plastic... or Mobile? And FTC Workshop on Mobile Payments*, March 2013, available at: <http://www.ftc.gov/sites/default/files/documents/one-stops/mobile-technology-issues/130306mobilereport.pdf>. See also the OECD Consumer Policy Guidance on Mobile and Online Payments April 4, 2014, available at: http://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-mobile-and-online-payments_5jz432cl1ns7-en

d. Children

There were also reports of problems with children purchasing goods and services with mobile payments from ICPEN respondents. Legislation in most jurisdictions typically does not allow children under a certain age to have credit cards, enter into binding contracts, or use other financial instruments. Nevertheless, many children have access to a mobile device that they can use to purchase goods and services. As children may not be aware of the binding nature of the transactions they enter into when doing mobile payments, this may cause problems.²⁶

e. Unclear division of responsibilities

The mobile payments ecosystem involves a large number of entities including mobile operators, mobile vendors, website operators, mobile aggregators, operating system developers, application developers, and payment card networks as well as traditional retailers. This large number of players can lead to an unclear division of responsibilities among the various entities and the vendor selling the good or service that, in turn, makes it more difficult for consumer dispute resolution and redress. This may cause problems for the consumer, particularly if the goods or services are defective, not delivered, or acquired based on deceptive marketing practices.

When several parties are involved in the supply of a service and the payment transaction, consumers have difficulties in determining their rights and the responsible parties. There is also a chance that the parties will start a “blame game” among themselves when consumers are complaining, which often will cause consumers to give up pursuing the answer. The result of this lack of clarity in responsibility is often a failure to refund overcharges and unlawful one-time charges to the consumers. Consumers need to know who is responsible for what and whom to turn to if things go wrong.

To solve this problem, some ICPEN authorities have proposed that mobile operators should bear the same kind of responsibility as the issuers of credit cards, which would include responsibility for price information and charge backs, and other penalties imposed on the consumer. In addition, many countries have alternative dispute resolution systems (“ADR”) that can resolve the matter, but it may be unclear in some circumstances which ADR has the jurisdiction.

f. In-app purchases

Several respondents to the ICPEN questionnaire mentioned in-app purchases as a type of purchase that causes many complaints. This is often due to the fact that many applications for smartphones and devices are marketed as “free,” but the consumer actually has to purchase additional content in order to be able to enjoy the application to the fullest. Information about the cost of in-app purchases and the authorization procedures is often insufficient or incomplete.

As with premium SMS services, there are also problems with an unclear division of responsibility between the makers of the device’s operating system, the mobile operator, the issuer of the credit

²⁶ See FTC Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, December 2012, available at: <http://www.ftc.gov/reports/mobile-apps-kids-disclosures-still-not-making-grade> .

card to which the purchase is charged, and other relevant players vis-à-vis consumer dispute resolution and redress.

g. Unclear level of consumer protection

Sometimes when purchasing goods or services, the consumer may be faced with a wide variety of different payment options. Although the payment service is basically the same to the consumers, the different payment options will usually be regulated by different legislation or codes of conduct granting consumers different levels of rights and protection. As the different payment services may appear essentially the same to consumers, it may be difficult for them to understand the legal nature of the different services and the consequences of choosing a particular form of payment. This concern is also discussed in Section 3, Consumer Protection – policy and law.

h. Other concerns:

ICPEN authorities shared other issues that they see rising on the mobile payment landscape:

- For the Latvian Consumer Agency, the merging of different mobile payment solutions; namely, premium SMS services with apps and smartphones, is an area of concern.
- The digital divide and literacy is another area of concern for some authorities, as this may cause some segments of the population to not be able to reap the benefits of new technologies. In Zambia, a voice-based mobile payment service is envisioned as a potential solution to such problems. Voice-based operations would work with all handsets and can be used by everyone irrespective of one's comfort level with technology or literacy level.
- Issues regarding data protection and privacy are also high on ICPEN agencies and consumers' concerns list.²⁷
- Finally, there is also a risk that, when more and more services are tied or bundled to consumers' mobile phone subscriptions, competition between mobile network operators will be hampered making it more difficult for consumers to switch providers. Some countries hold that mobile payments must be regulated by law in order to create a free and competitive market with low barriers for market entry, which in turn will secure fair and cost effective services for the consumers.

²⁷ Note that the *OECD Policy Guidance on Mobile and Online Payments* contains a section addressing these issues.

3. Consumer protection – policy and law

General consumer protection laws, in some cases, can be applied to mobile payments. Because mobile payments are developing rapidly, only a few responding countries have specific consumer protection laws addressing mobile payment-related issues. For example, only a few responding ICPEN countries have specific laws aimed directly at protecting consumers when they purchase digital services using premium SMS services. Among the countries that do, the United Kingdom has legislation that regulates premium SMS services through the Communications Act 2003 (section 120). By contrast, many countries have soft law regulation of these services, including Denmark, Belgium, and Norway, while still others have general consumer protection laws that can be applied to new and emerging payment systems. Several of the countries surveyed are also working with government legislatures to increase the legal safety for consumers making purchases with premium SMS services. On the other hand, transactions with a credit card or other financial instruments are strictly regulated by law in all countries surveyed.

In Europe, most mobile payment transactions are covered by the Payment Services Directive²⁸ and the E-money Directive.²⁹ The Payment Services Directive requires, among other things, consumer authentication and authorization procedures before the individual transactions take place,³⁰ limitations on consumers' liability when using the service, and standard terms covering the parties' contractual duties and liabilities regarding the unauthorized use of financial services. However, there are exceptions to the application of these directives, and there is no other legislation or regulation for transactions that fall outside of the scope of these directives. This is seen as a problem by many European respondents that favor equal protection for mobile and card-based payments.

Whether consumers have different rights when purchasing goods and services with mobile payments instead of traditional means of payment varies among the ICPEN member countries. In some countries, mobile payments charged on mobile phone bills are considered the same as credit card transactions, so consumers enjoy the same level of protection when making purchases with their mobile phone as with their credit card. In other countries, mobile payments fall under the scope of the telecommunication legislation. However, most countries have implemented a solution in

²⁸ See The European Commission – The EU Single Market, *Directive 2007/64/EC of the European Parliament and the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC* available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007L0064&from=EN>

²⁹ See The European Commission – *The EU Single Market, 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 amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance)*, available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0110>

³⁰ On January 31, 2013, the European Central Bank also issued mandatory guidelines that require all “governance authorities of payment schemes and all payment service providers (PSPs) that provide internet payment services, such as: i) internet card payments, including virtual card payments, as well as the registration of card payment data for use in wallet solutions; ii) the execution of credit transfers on the internet; iii) the issuance and amendment of direct debit electronic mandates; and iv) transfers of electronic money between two e-money accounts via the internet” to adopt “strong customer authentication” by February 1, 2015. See European Central Bank, *ECB releases final Recommendations for the security of internet payments and starts public consultation on payment account access services*, Jan. 31, 2013, available at: http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

between these extremes where telecommunication and financial legislation regulate different aspects of the mobile payment transaction.

In most European countries, consumers enjoy a strong level of protection when making purchases with their credit and debit cards. The transaction is authenticated with the consumer's PIN-code, or personal password, and some vendors also offer two-factor authentication. In other instances, consumers can hold the issuer of the credit card jointly responsible with the merchant if something goes wrong with the transaction, or if there is a fault in the good or service purchased. As some mobile payments are regulated as payment services under the Payment Service Directive, they offer consumers the same level of protection as pure credit card transactions. Some mobile payment transactions, such as the purchase of digital content services may not, however, be a regulated payment service and consumers will consequently have much weaker protection for these purchases.

The wording of the Directive is ambiguous in some sections rendering it difficult for regulators to enforce its provisions. In the view of the Norwegian Consumer Ombudsman, this is unfortunate as the ambiguous text of the directive has created uncertainty in the market. Finland also mentions the ambiguity of the Payment Services Directive as an area of concern. Norwegian Consumer Ombudsman authorities believe it is difficult for consumers to understand when they are covered by the protection in the payment services directive, and when they are not. The Payment Services Directive and its interpretation was part of a larger government investigation into several issues regarding mobile payments in Sweden.³¹

On this basis, it is the view of Norwegian Consumer Ombudsman authorities that consumers should enjoy the same level of protection for all types of mobile payments, no matter the goods or services they purchase or the amount of the transaction. Assuming this approach, in Norway's view, will also be in the best interests of businesses as it will reduce consumer complaints and increase consumer trust in the payment systems which, in turn, will increase the use of mobile payments.

Some authorities also point out that the role of the parties in the transaction, including the merchant, payment service provider, mobile network operator, and aggregator, should be clearer. In Israel, for instance, mobile operators' licenses bar them from collecting money from consumers for mobile content services unless they have received the consumer's explicit consent and have documentation of the consumer's explicit request for the service. However, because the enforcement of the license terms carried out by the Israeli Ministry of Communications is only administrative and does not deal with consumer protection issues, the Israel Consumer Protection and Fair Trade Authority is working on a law that will address the need for license requirements to apply to all payments and all businesses (including mobile payments). Additionally, the Israeli Authority is in the process of examining the necessary adjustments to the Israeli debit card law so that its provisions will apply to mobile payments.

There are also several areas of concern and of advancement reported by the countries surveyed. First, cooperation with various sector organizations appears to be an area of policy development in

³¹ See European Commission, *Payment Services Directive: Frequently Asked Questions, Background to Payment Services Directive (PSD)*, available at: http://europa.eu/rapid/press-release_MEMO-07-152_en.htm?locale=en

several countries, where it is used not only to survey the market to take action in cases where harm to consumers occurs, but also to increase consumer safety to reduce the number of complaints.

Second, Danish authorities hold that the dynamic use of new technology and new media is difficult to regulate and that it is difficult for enforcement bodies to set up specific requirements for new technology and payment methods. For other respondents, such challenges are thought to be negated by regulations that are not specific to certain technologies or products. For their part, Mexican authorities emphasize that, when they created regulations for mobile payments, they avoided requirements tailored to specific business models or products. Similarly, Colombian authorities are applying existing consumer protection regulations to mobile payments in order to include consumer challenges from emerging payments services in the scope of already existing regulations. However successful this approach has been to date, Colombian authorities recognize the possibility that specific regulations of mobile payments may be needed as the Colombian market for mobile payments evolves.

Third, the Korea Consumer Agency has also recently established a protection system for mobile payments based on Korean financial laws and guidelines. The protection system requires, among other things, user authentication and transaction value authorization. The legislation in Korea has been expanded in correlation with the introduction of new payment services.

Fourth, legislation prohibiting false or misleading advertising or representations is in place in most countries and is enforceable for both online and offline advertising.

Finally, most ICPEN countries surveyed have legislation in place to deal with cross-border consumer issues in general. Mobile payments could therefore be an area for increased future international cooperation.

Annex III contains a list of sources with policy developments and sources of information.

Security

Some authorities point out that mobile phones have limited security measures to prevent unauthorized transactions. This is a concern in cases of mobile phone theft or other situations where misuse can occur. In some jurisdictions, mobile payments are subject to a double opt-in procedure, PIN-code, or similar security procedure; in others, there are no security procedures for mobile payments; and others who take a mixed approach where some payments (for example, those over a certain amount) are protected with security procedures while others are not.

In many countries, mobile network operators take no responsibility for unauthorized charges for mobile payments on mobile phone bills. There is also a growing trend in other ICPEN jurisdictions where consumers have to authorize subscriptions or one-off charges on their mobile phone bill via the double opt-in or similar authorization mechanisms. Such security mechanisms may mitigate some of the risks with mobile payments. The Finnish Consumer Agency is pushing this agenda further by working on a change to their country's legislation that will make mobile network operators assume the same responsibility for transactions as credit card providers.

4. Enforcement

Consumer protection authorities face several structural challenges in relation to the enforcement of mobile payments. In many jurisdictions, ICPEN consumer protection authorities share responsibility for mobile payment issues with other regulators. Given that mobile payments often involve many different market players and span several different markets, some respondents reported that it was sometimes difficult to determine which authority should enforce the consumer protection laws in a given circumstance as a breach could violate the laws of several authorities. Also, civil disputes are outside the authority of many consumer protection agencies. Moreover, even if a collective consumer redress system exists in their country, many agencies state that the possibility to seek collective redress on behalf of the consumers generally sits outside their ambit. Finally, in many countries the enforcement of individual consumer rights is outsourced to private complaint boards run by the industry.

As a result, few of the respondent authorities have taken any enforcement action against mobile payment service providers. Some of the authorities stated that its country's laws are too ambiguous, and this may hamper enforcement actions. Others stated that the laws its country have are insufficient to deal with the new technology of mobile payments and that the laws need to be evaluated and possibly amended. In contrast, some countries have seen very few complaints and thus have no real need for taking action. Finally, in countries where the market for mobile payments is developing, but still relatively small, enforcement actions against mobile payments providers may not yet be of priority.

Overall, most of the responding authorities are able to handle consumer complaints regarding deceptive and unfair commercial practices, including false or misleading representations. Breaches of these standards may, depending on the applicable law, be reprimanded by securing undertakings from the business in question or by prohibiting the business with a court order. In addition, deceptive and unfair commercial practices are usually punishable by an administrative fine.

In addition, some ICPEN authorities actually have good experiences cooperating with other public authorities and relevant business organizations, and achieving voluntary compliance. Some of these voluntary compliances have furthermore developed into codes of conduct.

Nonetheless, some ICPEN agencies are using their general consumer protection authority to bring or consider enforcement actions involving mobile payment systems. For example, Apple agreed to pay a minimum of \$32.5 million to consumers and change their billing practices to settle charges by the U.S. Federal Trade Commission that the company billed consumers for millions of dollars of charges incurred by children in kids' mobile apps without their parents' consent.³² The Canadian Competition Bureau also initiated legal proceedings against Bell Canada, Rogers Communications, Inc., TELUS Corporation, and the Canadian Wireless Telecommunications Association (CRTC), requiring them to

³² U.S. Federal Trade Commission, Press Release, *Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases without Parental Consent: Company Also Will Modify its Billing Practices Under FTC Settlement.*, Jan. 15, 2014, available at: <http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million> .

stop misleading advertising that promotes costly "premium texting services," and to compensate consumers. The Competition Bureau is seeking full customer refunds and administrative monetary penalties in its legal action.

In further actions by an ICPEN Member, the UK's Office of Fair Trading (now the Competition and Markets Authority) released principles relating to payments for online and in-app games and warned games producers that they must comply with consumer protection laws or face enforcement action.³³

Finally, some jurisdictions do have specific legislation. In Israel, the Consumer Protection and Fair Trade Authority can take criminal enforcement actions against providers of mobile content services. However, in some cases it is difficult, if not impossible, to locate the content provider since the telephone and mobile companies charge the consumer without revealing to whom the money is transferred. The Consumer Protection Authority has therefore initiated a proposal to amend the Consumer Protection law prohibiting all businesses from charging consumers without their explicit consent. Once enacted, this provision would specifically prohibit operators from collecting money from consumers for mobile content provided through content providers, unless the content providers present a signed contract to the mobile operator with the explicit consumer consent to the transaction prior to charging the consumer.

³³ UK Office of Fair Trading, Press Release, *Online games industry given two months to get house in order following OFT investigation*, Jan. 30, 2014, available at: <http://www.tradingstandards.gov.uk/extra/news-item.cfm/newsid/1394>. The OFT principles state that consumers should be told upfront about costs associated with a game or about in-game advertising, and any important information such as whether their personal data is to be shared with other parties for marketing purposes. The principles also make clear that in-game payments are not authorized, and should not be taken, unless the payment account holder, such as a parent, has given his or her express, informed consent. Available at: http://webarchive.nationalarchives.gov.uk/20140402142426/http://www.of.gov.uk/shared_of/consumer-enforcement/oft1519.pdf

5. Initiatives for mobile payments from industry associations and others

According to the ICPEN responses received, there are quite a few initiatives by consumer protection authorities and other players. These initiatives vary but all reportedly aim at increasing consumer protection in mobile payments.

The majority of the initiatives are concerned with establishing codes of conduct or similar guidelines to be employed by various players in the mobile payment services market. Most seem to have originated from consumer protection authorities, while others are more directly attributable to the industry or NGOs or some combination of the industry and authorities.

The questionnaire results generated several examples of initiatives that originated from industry participants. In Belgium, the mobile network operators have organized themselves in the GSM Operator Forum and issued a self-regulatory code of conduct. The members of the GOF meet weekly to discuss, *inter alia*, issues regarding specific service providers. In New Zealand, mobile phone operators in the Telecommunication Forum have agreed to a framework that will make it possible for customers to purchase applications and digital content through a safe payment environment on their phone and have the charge added to their phone bill. In the UK, mobile network operators request content providers to use the "Payforit" scheme for mobile payments. The scheme employs a red and yellow card system, where cards are issued for services that forfeit their obligations under the scheme. A red card issued means that the service will be taken out of action immediately and remain out of action for a minimum of 10 days and only return to service when its compliance is confirmed. In Canada, the Canadian Radio-television and Telecommunications Commission's (CRTC) established a mandatory code of conduct for wireless service providers to address clarity and content in service agreements.

In other responding countries, specific security measures are in place as a result of negotiations between authorities and the industry. In Finland, for instance, negotiations between the authorities and the Finnish Ethical Committee for Premium Rate Services have resulted in a requirement for a double opt-in regime. When subscribing for recurring charges via premium SMS, Finnish consumers now need to authorize the subscription by replying "OK" to a separate confirmation message in order to start a subscription. Similarly, after negotiations with the Danish Consumer Ombudsman, mobile network operators in Denmark have taken on the obligation to send warnings to customers when the charge for premium rate services exceeds 250 DKR in one month.

Other types of industry initiatives include ADRs for payment services, as in Korea, and efforts to educate consumers, as in Mexico. In April 2012, in conjunction with the launch of the "Transfer" mobile payments platform, the Association of Banks of Mexico launched the ad campaign "Ponte buzo" which warned consumers about possible fraud in electronic banking. The two main banks in the country, Banamex and BBVA Bancomer, give courses and workshops on financial education, including the issue of Internet fraud.

The Working Group is also aware of two global consortia that are working on the development of mobile payments.³⁴

³⁴ Mobey Forum, www.mobeyforum.org, 2014. Global Platform, www.globalplatform.org, 2014.

Conclusions

The emergence of mobile payment mechanisms has provided consumers with new opportunities to engage in commerce, but has also provided them with new challenges that consumer protection authorities are beginning to address. The first version of mobile payments – premium SMS services – has been around for some years, and many consumer agencies have become acquainted with this service due to high numbers of consumer complaints. These complaints are usually based on the poor or non-existent user authentication or authorization of transactions, fraudulent and unauthorized charges on consumers’ mobile bills (a practice known as “cramming”), and little or no limitations on consumer liability for unauthorized charges or charges incurred should a consumer’s device become stolen or lost. This has led to consumers paying for services that they did not want or did not intend to purchase or for services purchased by thieves or unauthorized users. In countries where the system for premium SMS services is open and can be accessed by many traders, consumers can also fall victim to rogue traders who can charge a consumer’s phone bill without there ever being any sort of contact between the two parties. With the decline of premium SMS billing in some countries, and the emergence of direct carrier billing (also known as “direct operator billing”), some of these issues may be ameliorated; however, there may still be gaps in consumer protections.

Indeed, the main issue that emerged from the ICPEN questionnaire is the difference in the level of consumer protections between mobile payments and more traditional payment mechanisms. In the view of many consumer protection agencies, consumers should enjoy the same high level of protection regardless of the type of payment services they use. The types of protections consumer authorities have recommended include: adequate authentication and authorization procedures for consumer transactions; limitations on consumers’ total liability when using mobile payment mechanisms service; and limitations on consumers’ liability for unauthorized charges or costs incurred after the theft or loss of a mobile device or SIM card.

The next generation of mobile payments is launching around the world. Whereas the first generation of mobile payments only allowed for the purchase of digital services and simple offline goods, the next generation of mobile payments will allow for larger and more complex purchases in both traditional stores and more automated sales. Furthermore, while the first generation of mobile payments was fairly uniform around the world, the next generation of mobile payments seems to be more diverse. In some countries, the credit card issuers and financial institutions are mainly driving the development, whereas in others, it is the mobile network operators, as was the case with first generation mobile payments. The technology and business models for mobile payments are evolving rapidly, so the market situation around the world can change at a faster pace than it did with first generation payments.

Due to the fact that the development of mobile payments is being driven by different market players, consumers’ mobile payment transactions in many countries will be covered by differing legal frameworks. For example, mobile payments with credit cards will be covered by financial legislation, while mobile payments supported by the device’s SIM card or similar technology will be covered by telecommunications law. In other countries, SIM cards are regarded the same as credit cards, which means that consumers can enjoy the same high level of protection as with credit cards when they purchase goods or services charged on their mobile network bill.

Although it was not covered in the questionnaire, from the consumers' point of view, it appears that it makes no difference who provides the service of transferring money from them to the provider of the goods and services. The consumer may be aware that the transaction is carried out by a credit card versus a SIM card, but it is likely that very few consumers are aware of the fact that the transaction may be covered by different legislation and entail different levels of consumer protection based on the technology providing the service.

These types of issues are already being considered domestically and internationally. Most notably, the OECD has recommended that "governments and payment providers should work together to develop minimum levels of consumer protection for mobile and online payment transactions, regardless of the payment mechanism used."³⁵ Some consumer authorities have already implemented these types of protections while others are in the process of developing regulatory and self-regulatory solutions.

The information and conclusions from this report can help ICPEN members, partners, and other consumer and governmental policymakers develop better consumer protections in the area of mobile payment systems. Findings from this report have already been used by the OECD Committee on Consumer Policy to help them formulate recommendations for best practices in consumer protection and mobile payments.

To discourage deceptive business practices involving mobile payment services and encourage the provision of sufficient information to enable informed consumer choice in the marketplace, ICPEN recognizes the need to constantly adapt to the new reality of a more global marketplace and rapidly evolving telecommunications and information technologies. By diversifying the realm of our respective consumer protection, outreach, and enforcement activities, and by building partnerships, domestic and international, with other levels of government, private industry, academia, financial services, and industry associations, ICPEN will be well positioned for a rich and transparent dialogue in the days ahead on mobile payments issues impacting consumers. At a later stage, ICPEN may consider further initiatives in this area, including developing a training manual for enforcement and regulatory agencies on mobile payment issues. More importantly, ICPEN recognizes that, by working together, we will achieve more, to the benefit of consumers, businesses, and the global economy.

³⁵ The Organization for Economic Development and Cooperation (OECD), *Consumer Policy Guidance on Mobile and Online Payments*, April 4, 2014:17, available at: http://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-mobile-and-online-payments_5jz432cl1ns7-en

Annex I – ICPEN questionnaire on mobile payments

The objective of the ICPEN project on consumer protection in mobile payments is to identify consumer issues relating to mobile payments and to produce a report (from ICPEN members) of problematic situations reported by consumers and authorities regarding these issues. To assist with the production of the report, we need you to answer the questions in this questionnaire.

The Working Group is mainly seeking information about:

- types of mobile payment you have in your country,
- consumer challenges regarding mobile payments you are aware of, and
- recent actions (enforcement, consumer education, surveys) that you or other relevant authorities have undertaken in respect of these consumer challenges.

Definition

The Working Group has defined mobile payment as any sort of payment for goods or digital/regular services done on or with a mobile phone, either billed by a mobile network operator, a card company/bank, or other. However, payment done via the mobile phone's browser as a part of traditional e-commerce, e.g. shopping and paying on eBay, is not within the scope of this questionnaire.

A few examples of mobile payment:

- paying for mobile content charged on the phone bill
- paying for a drink at a vending machine charged on the phone bill
- paying for parking your car charged on the phone bill
- paying for an app charged on the credit card
- paying within an app for "Smurf berries" (or similar) charged on the debit card
- paying for a bus-fare using an app or sending a SMS charged on the phone bill/the credit card
- paying for a bus-fare by NFC transaction charged on the phone bill/credit card
- paying for groceries at the local supermarket by NFC transaction charged on the phone bill/ credit card
- paying for other traditional goods and services by NFC transaction charged on the phone bill/ credit card
- other low value payments for goods and services paid through the interface of the mobile phone (e.g. person to person, iZettle, PayPal here)
- etc.

This list of different mobile payments is not exhaustive, and provides just a few examples that might help you when answering the first question.

QUESTIONS

A. *Mobile payment – market analysis*

1. What types of mobile payments are in use in your country?
 - a. Credit card based? If so, please specify the different types.
 - b. Phone bill based? If so, please specify the different types.
 - c. Other? If so, please specify the different types.
2. Describe the mobile payment market structure in your country. Who are the market players? What is their role?
3. What role do the mobile payment providers or mobile network operators play? What protection is offered by mobile payment service providers or mobile network operators in your country?
4. Are there any statistics regarding the use of mobile payments in your country? If so, please indicate the relevant market players, number of total market players, market share, turnover, type of payment providers (mobile network operators, banks, retailers, etc.), type of mobile payments, etc.

B. *Consumer challenges related to mobile payment*

5. Have you, or other relevant authorities/complaints boards, received any complaints from consumers related to mobile payments? If so, please specify the number of complaints and the most frequent consumer complaints issues.
6. Are there any specific types of mobile payment service that seem to cause more consumer problems than others?
7. What complaint handling mechanisms are in place in your country? Who handles complaints relating to mobile payments? How are they resolved?
8. From your perspective, what are the biggest consumer challenges with mobile payments?

C. *Enforcement*

9. In your country, do you have legislation that allows for any enforcement actions against the providers of mobile payment services or network operators when problems arise?
10. Have you or other relevant bodies taken any actions (contested, voluntarily compliance, and/or enforcement) against the providers of mobile payment services in your country? If so, please specify.

11. What were the results of actions taken? How was the process? What was the outcome?

Have any actions been supported by or required the assistance of other ICPEN members? If so, please specify.

D. Consumer Protection (policy and law)

12. Do you have any legislation in your country related to mobile payments? (If you do not, please skip to question number 14.)

a. Is there any requirement for any sort of authentication when the consumer makes a payment (e.g. double opt-in for mobile content)? If so, please specify.

b. Is the legislation in place satisfactory to deal with the current use of mobile payments in your country, and the likely future increased use of the services?

13. If you do not have any legislation in your country related to mobile payments: Do you see a need for such legislation, and if so, in your opinion which rules would need to be included in satisfactory legislation?

14. Have you or other relevant bodies taken any other specific action to address consumer problems regarding mobile payments (policy guidance, law initiatives, or other)? If so, please specify.

15. Under your legislation, are consumers' rights different when they purchase goods or services using mobile payments instead of traditional means of payment (e.g. cash or credit/debit card)? If so, please indicate the differences.

16. Does the legislation in your country relating to mobile payment deal specifically with domestic commerce, or are there mechanisms to deal with cross-border consumer problems (referrals from other agencies, etc.) associated with the borderless nature of the Internet and mobile commerce (e.g. a voucher or gift card obtained in one jurisdiction and used in another)? If so, please specify.

17. Are you aware of consumer policy developments or other developments with relevance to mobile payments that may be of interest to other enforcers in the ICPEN network? If so, please specify.

18. Are you aware of any existing relevant reports, recommendations, or other documents that will be beneficial to other enforcers in the ICPEN Network? If so, please specify.

E. *Industry initiatives*

19. Have any industry organizations or associations (NGOs, consumer, or industry associations) for mobile payment service providers or mobile network operators in your country taken any steps to increase consumer protection in mobile payments? If so, please specify.

Annex II – Websites of responding authorities

Austria	http://www.bmask.gv.at/site/
Belgium	http://economie.fgov.be/
Canada	http://www.competitionbureau.gc.ca
Chile	http://www.sernac.cl/sernac2011/
Colombia	http://www.sic.gov.co/es/
Denmark	http://www.consumerombudsman.dk/
Dominican Republic	http://www.proconsumidor.gob.do/
Estonia	http://www.tarbijakaitseamet.ee/en
Finland	http://www.kuluttajavirasto.fi/
France	http://www.economie.gouv.fr/dgccrf
Germany	http://www.vzbv.de/
Hungary	http://www.nfh.hu/en/
Israel	http://moital.gov.il/
Italy	http://www.agcm.it/
Republic of Korea	http://www.kca.go.kr/
Latvia	http://www.ptac.gov.lv/page/104
Lithuania	http://www.vvtat.lt/
Mexico	http://www.profeco.gob.mx/
New Zealand	http://www.consumeraffairs.govt.nz/
Norway	http://www.forbrukerombudet.no/
Philippines	http://www.dti.gov.ph/splash.php
Portugal	http://www.consumidor.pt/
Spain	http://www.consumo-inc.gob.es/
Sweden	http://www.konsumentverket.se/
United Kingdom	http://www.oft.gov.uk/
United States	http://www.ftc.gov/
Zambia	http://www.ccpc.org.zm/

Annex III – Policy developments and references

A. Policy developments

- OECD policy guidance on mobile and online payments: www.oecd.org/sti/consumer-policy/mobilepayments
- PhonepayPlus guidance on application-based payments: <http://www.code.phonepayplus.org.uk/pdf/guidance-notes/application-based-payments.pdf>
- The FTC in the United States held a workshop, *Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments*, on April 26, 2012. Information on the workshop, including archived videos of the presentations, is available at: <http://www.ftc.gov/bcp/workshops/mobilepayments/>. See also: *FTC Workshop, Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments – Staff Report*, March 8, 2013, available at: www.ftc.gov/os/2013/03/130306mobilereport.pdf
- The FTC also hosted a workshop, *In Short: Advertising & Privacy Disclosures in a Digital World*, on May 30, 2012 to consider the need for new guidance concerning advertising and privacy disclosures in today's online and mobile environments. A description of the workshop and archived webcasts of the panelist presentations are available at: www.ftc.gov/bcp/workshops/inshort/index.shtml
- FTC Report – *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), available at: <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>
- The International Standardization Organization's (ISO) committee on consumer policy has a Working Group on consumer protection in the global marketplace which works on financial services, including work towards an international standard for mobile payments. See http://www.iso.org/iso/iso_technical_committee.html?commid=55000
- The UK Payments Council's new database, Paym, (pronounced "Pay Em") launched by April 29, 2014, designed to be an easy, secure way for consumers to send and receive payments directly to a current account, using just a mobile number: http://www.paymentscouncil.org.uk/media_centre/press_releases/-/page/2878/
The Payments Council also published the report *The Mobile Way To Pay*, March 2014, which forecasts 1 billion payments could be made through Paym by the end of 2018, available at: http://www.paymentscouncil.org.uk/files/payments_council/paym/paym_white_paper_final.pdf

B. Other reports, recommendations and documents

- Belgian GOF-Guidelines: <http://www.gofguidelines.be/>
- The Guardian, Press Release, *Boku mobile payments look to crack contactless market*, February 23, 2012, describing how Near Field payments technology will use the Mastercard PayPass system to enable users to make purchases via their mobile phones, available at: <http://www.guardian.co.uk/money/2012/feb/23/boku-mobile-payments-contactless>
- Canadian Radio-Television and Telecommunications Commission (CRTC) consultation regarding the development of a national wireless services consumer code: <http://crtc.gc.ca/eng/archive/2012/2012-206.htm>
- Canadian Wireless Telecommunications Association (CWTA) code of conduct: <http://cwta.ca/for-consumers/code-of-conduct/>
- Chapter 5 of the book “ICTs for Development: Improving Policy Coherence,” Regulatory issues around mobile banking: http://www.oecd-ilibrary.org/development/icts-for-development/regulatory-issues-around-mobile-banking_9789264077409-7-en
- European Commission Green Paper, *Green Paper – Towards an integrated European market for card, internet and mobile payments*, November 1, 2012: http://ec.europa.eu/internal_market/consultations/2012/card_internet_mobile_payments_en.htm
- European Payments Council on the Single Euro Payments Area (SEPA) and mobile payments: <http://www.europeanpaymentscouncil.eu/index.cfm/sepa-for-mobile/>
- OECD Report from the Committee for Information, Computer and Communications Policy on *Online Payment Systems for E-commerce*, April 18, 2006: <http://www.oecd.org/dataoecd/37/19/36736056.pdf>
- Report on Innovations in Retail Payments of May 2012 by the Bank for International Settlements: <http://www.bis.org/publ/cpss102.htm>
- Final Report from Analysys Mason, *The marketplace for and regulation of micropayment services in the UK*, December 2010, commissioned by PhonepayPlus, available at: http://www.phonepayplus.org.uk/For-Business/~/_media/Files/PhonepayPlus/Research/Analysys_Mason_The_marketplace_for_and_regulation_of_micropayment_services_in_the_UK.pdf

- PhonePayPlus premium rate service annual review 2011:
<http://www.phonepayplus.org.uk/News-And-Events/News/2012/5/Promotion-of-premium-rate-services-on-social-networks-up-by-575-percent.aspx>
- Studies by The US Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services*, March 2012, available at:
<http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf> ; and *Consumers and Mobile Financial Services 2013*, March 2013, available at:
<http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf>
- Study of April 2012 conducted by the Pew Internet and American Life Project, *The Future of Money in a Mobile Age*, available at: <http://www.pewinternet.org/Reports/2012/Future-of-Money.aspx>
- Visa Europe's Press Release, *Vodafone and Visa announce world's largest mobile payments partnership* , February 27, 2012, available at:
http://www.visaeurope.com/en/newsroom/news/articles/2012/vodafone_vis_a_partnership.aspx.
- The Norwegian Consumer Ombudsman's *Guidelines on Mobile Content Services*, March 2009:
http://www.forbrukerombudet.no/asset/3219/1/3219_1.pdf