Summary

This study looks into the question which new forms of fraud can emerge in consequence of technological developments and market trends in mobile telecommunications (especially in effecting mobile payments), and whether today’s legislative instruments are adequate to satisfactorily combat these (new) forms of fraud. In order to answer these questions (and the derivative sub-questions) we have taken four lines of approach: desk research, interviews, framing variants of mobile payment, and a meeting of experts. The report itself comprises three sections:

(I) Developments in mobile payment;
(II) Fraud with mobile payments
(III) The legal framework and instruments.

I. Developments in mobile payment

The mobile payments market is very diverse. In the Netherlands, mobile payments are made on a considerably large scale and include the use of premium rate SMS services. While several new, more advanced forms of effecting mobile payments are on the horizon, expectations in the Netherlands regarding this form of payment are modest. The financial sector argues that mobile payment has no credible advantage above the current alternatives. The costs and complexity are considerable. Mobile payment will have a hard time winning the market in the Netherlands because the (over-the-counter) payments market here is highly advanced. After having made a false start, payment by chip card is now starting to achieve significant scale. Furthermore, the payments market has a strongly national character. Advanced forms of mobile payment do however require large, international scale if they are to be introduced cost-effectively. Most market parties anticipate that mobile payment will initially expand in the national dimension. Growth of the various sub-markets for mobile payment will be spread out over the course of years. The expectation is that the market for mobile payments will initially develop in the form of services for making micro payments for online content or online services. And yet it is in this market that there are very few alternatives for effecting mobile payments. There is, however, also a direct benefit for telecommunications operators from such forms of payment; only in the case of adequately developed forms of online payments will the substantial costs incurred for UMTS licences and networks be able to be recovered. Only later will the sub-markets for local micro payments, remote macro payments (also international) and local macro payments follow. Developments in mobile payment are still enshrouded in uncertainties. These uncertainties are not primarily of a technical nature, but are rather the consequence of the lack of a sound business case for mobile payment.

Numerous initiatives are taken both by existing parties and new entrants to the market. These initiatives (in the Netherlands and in other countries) are to be seen in Internet payments and mobile payments. Nevertheless, many initiatives fail to achieve adequate scale, and some are even withdrawn from the market not long after their introduction. New entrants are then faced with bankruptcy. The (numerous) international standardisation

---

1 Fraud with mobile payments relates to acts that (1) are intended for the purpose of procuring (personal) financial gain; (2) are carried out with intent; (3) contain an element of deception; and (4) make use of a mobile payment system.
initiatives are not regarded by the market parties as significant. They are far distanced from reality and take very little advantage of the national context.

Four variants of mobile payment are worked out in detail in this report. They differ in terms of intended use, technical structure, the roles and responsibilities of the parties concerned, and the link with existing payment systems. These variants concern (1) the further development of mobile debit transactions via the Internet; (2) the next generation of prepaid payments; (3) mobile credit card payments and (4) mobile digital cash via wallets. The main players in these variants are banks, the providers of mobile telecommunications, credit card companies, and (for mobile digital cash via wallets) new entrants and/or banks. Given the major uncertainties involved it is too early to say which of these variants has or have the highest chance of success.

II. Fraud with mobile payments

A distinction can be drawn between so-called relational fraud (including using a false identity) and technical fraud (where use is made of technical imperfections in the system). Relational fraud is currently the main category of fraud in both telecommunications services and payment services. Nevertheless we anticipate that technical fraud will (for some time) gain the upper hand with the introduction of new mobile payment services. Although market parties are putting efforts into mapping out the ex-ante fraud risks and in protecting their systems from misuse, not all the technical and non-technical risks can be predicted. Providers will therefore to a large extent have to rely on a reactive fraud policy. It is a fact that the situation will to some extent continue to be overtaken by events. The current fraud detection systems, both of telecommunications providers and financial parties, can bring certain types of fraud to light by using advanced methods of pattern recognition and other systems, yet they are often unsuccessful in detecting advanced, unexpected forms of technical fraud.

There are many views regarding the extent of fraud and the importance of combating it. New entrants run a higher risk of loss from fraud. Out of sheer necessity these players devote less attention to fraud and effectively combating it than established players. Individuals frauds will take advantage of this weakness and focus on this group in particular. Fraud by criminal organisations poses a serious threat. Especially in telecommunications networks do we see highly organised fraud being committed by gangs with international branches who are able to gain access to advanced cryptographic knowledge, for instance by calling in unemployed East-European experts. A value chain which is gradually becoming more complex entails a higher risk of fraud by companies in the value chain too. Even now do we see numerous, more or less fraudulent parties active on premium rate numbers. This trend will probably continue and intensify as the value chain becomes more complex and if there is an increase in the diversity of services (and the relevant possibilities). The techniques used by frauds are constantly becoming more advanced and man is increasingly becoming the weak link in the chain. An appropriate example of this is the rise in phishing; a year ago the experts laughed about end-users that fell for this ruse, but they now admit that it is virtually impossible today for even a very cautious end-user to determine whether a certain service or application is bona fide or not.

III. Legal framework and instruments

One of the study’s main conclusions is that at the present time there is insufficient reason to validate large-scale changes/supplements to the legal framework. There is too little
insight into new forms of fraud, and the market parties generally expect that the current legal framework will be adequate to cope with future developments. Nevertheless, this does not alter the fact that it is still wise to keep a finger on the pulse. We shall deal with several specific legal aspects in the following. Apart from that, all parties point out the desirability of more scope for the Public Prosecutor (to take legal action) in connection with this subject matter.

**Penalization**

As was indicated in the above, there is still more or less too little necessity to make provisions for penalization. This point of departure calls for an explanation in two cases. We feel that penalization could be considered in the one, but not in the other.

Special penalization could be considered for phishing. Phishing should be made a punishable offence as a special form of fraud. Obtaining authentication data by any form of deception is a major preparatory act of unadulterated fraud. However, it is still uncertain whether phishing – as a preparatory act – is covered by the current fraud provisions, which are strongly geared towards property crime (and not so much towards obtaining authentication data). While making phishing a punishable offence would not be unique for mobile payment systems, it is characteristic of a general form of computer crime.

Registration under a false name need not be made a separate punishable offence. A preparatory act of quite a different nature is registering for telecommunication or financial services under a false name. Nevertheless, it is still doubtful whether there is the need to create a new punishable offence. It is already punishable as forgery in cases where the name is intended as proof, and this will indeed often be the case. Furthermore it restricts the possibilities open to persons who do not wish to disclose their name for good reasons.

**The status of mobile payment system providers**

The current status quo is unstable; there is absolutely no prudential supervision over telecommunications providers. Today, prepaid phone credit (*beltegoed*) is not regarded as electronic money within the meaning of Directive 2000/46/EG and the WTK 1992 (Credit System (Supervision) Act) (in which the directive is implemented). Therefore the telecommunications providers in question do not fall within the terms of the so-called Electronic Money Institutions (EMI) regime. The financial sector sees this as unjustified preferential treatment of telecommunications providers. Telecommunications providers fear that they are unable to meet some of the requirements imposed on EMIs, such as solvability and liquidity. A sui generis regime for prudential supervision over telecommunications providers is coming more distinctly into view. The key to the discussion on prudential supervision over telecommunications providers lies in Europe. The European Commission recently concluded a public debate on this subject. The expectation now is that the issue of prepaid phone credit will inevitably be governed by management regulations geared towards financial activities and regulations on prudential supervision.

**Consumer protection**

The EMI discussion also has consequences for consumer protection. Regarding the provision of financial services it is felt that there is already an adequately worked out regulatory system to protect consumers. If telecommunications providers are seen as EMI then it is only obvious that besides regulations on prudential supervision, the Compulsory Identification Act (*WID*) and the Disclosure of Unusual Transactions (Financial Services) Act (*WMOT*), other relevant regulations concerning consumer protection in terms of financial services (Recommendation 97/489/EG and the future implementation of Directive 2002/65/EG) could be applicable to telecommunications providers in as far as how they
deal with prepaid phone credit. Considering the interests of consumers that are at stake, this would indeed be desirable.

**Prevention and self-regulation**

Privacy legislation does not stand in the way of using black-lists. Market parties see the drawing up of black-lists as a major tool to combat fraud. Nevertheless, they still feel restricted by privacy regulations when setting up relevant databases, particularly those with an international character. Privacy legislation does not prohibit blacklisting, but it does impose certain conditions on the management and composition of such lists.

The Agreement to Counteract the Improper Use of Information Numbers is one example of a reasonably successful form of self-regulation that makes provision for coordination and collaboration between the relevant parties in the telecommunications value chain. In (the lack of) self-regulation for mobile payments it is up to the government to safeguard the interests of the weaker parties.