Summary

The Dutch Ministry of Justice requires more insight into the nature and magnitude of telecommunications fraud in The Netherlands. A recent analysis of organized and heavy crime, performed by the Dutch police, classified this problem area as void. As a consequence, the Ministry of Justice is unable to determine the exact threat that emanates from this phenomenon. TNO was commissioned to clear away this gap, by investigating the following issues:

- The current nature and magnitude of telecoms fraud in The Netherlands as well as expectations for the next two to three years
- Characterization of telecoms fraud victims and perpetrators, including the manner in which groups of perpetrators are organized
- Effectiveness of the fraud fighting chain, including current bottlenecks and the extent to which foreseen developments will pose new requirements on this chain
- The extent to which the current set of legal instruments suffices to combat present and future manifestations of telecoms fraud.

This new knowledge shall serve as a basis for determining the threat that telecoms fraud presently constitutes for Dutch society. In addition, the Ministry aims to improve the effectiveness of the fraud management chain where possible.

As a first step in addressing the issues described above, the problem area telecoms fraud was thoroughly characterized and demarcated. Here, a detailed taxonomy of telecoms fraud methods was devised. This taxonomy characterizes and rates individual fraud methods, but also explicitly addresses relationships that exist between the various forms of telecoms fraud. Subsequently, to gain insight into the national status quo with respect to telecoms fraud, an extensive set of expert interviews was convened. Among parties interviewed were telecoms providers, criminal investigation units and various governmental bodies. In order to place the results of said interviews into a meaningful perspective, these were examined against and complemented with international reference material. The latter included quantitative data with regard to the magnitude of telecoms fraud on a Western-European and global scale.

Note that the emphasis of this investigation was on detailing the nature and magnitude of telecoms fraud and the effectiveness of current fraud fighting provisions. In close agreement with the contractor, it was decided to explore the other research topics more globally.

The investigation resulted in the following conclusions:

- Possibilities to commit telecoms fraud primarily exist within fixed and mobile telephony services. Large-scale exploitation often involves abuse of (international) Premium Rate Service numbers.
- For the greater part, the financial damage due to telecoms fraud seems to be caused by a very limited number of criminal organizations, operating on an international scale. The layered structure of such organizations contributes to the fact that chief offenders usually remain untouchable.
- Perpetrators of telecoms fraud appear to also be involved in various other forms of crime, such as handling of stolen goods, narcotics trade and money laundering. Although various experts suggested that telecoms fraud also serves as a means of financing terrorism, this investigation was unable to substantiate this claim with hard facts.

- Although only EUR 20 million worth of damage can be demonstrated undeniably, the absolute financial magnitude of telecoms fraud in The Netherlands probably amounts to at least EUR 40 million (2005). International reference data shows that this damage might also come close to EUR 90 million. The damage is for the most part (over 98%) suffered by Dutch telecoms providers. Based on conservative estimates, the damage suffered by end users seems to amount to EUR 650.000 per year (2005).
- The financial impact of telecoms fraud on both providers and end users is presently limited. As a consequence, most Dutch telecoms providers do not possess a clear view of the exact damage they suffer. There does not seem to be a direct business interest to improve the registration of telecoms fraud.
- The dynamic nature of the telecoms fraud phenomenon poses limitations on the extent to which preventive measures can be taken. New manifestations of telecoms fraud can only be predicted to a very limited extent. As a consequence, fighting telecoms fraud will, to a certain extent, always be of a reactive nature. This does not alter the fact that, especially for fraud with Premium Rate Service numbers, preventive improvements are feasible. Here, the recent expansion of OPTA jurisdictions is regarded as a valuable step forward. In addition, a structural dialogue between government and providers might yield an additional basis for improved control. Further investigation should reveal whether and in which form this might be effective.
- Investigation and prosecution within the context of telecoms fraud may be improved in variety of ways. Among other things, the process of reporting incidents to law enforcement agencies as well as the subsequent follow-up both seem ineffective. In addition, investigative capacity at law enforcement agencies presently seems too limited to adequately address all relevant incidents of telecoms fraud.
- Existing penalty clauses for the most part seem sufficient for the purpose of prosecuting and adjudging perpetrators of telecoms fraud. In addition, recently embraced adjustments to the Dutch Telecommunications Law seem to form a solid basis to take faster and more effective action against telecoms fraud by means of Premium Rate Service numbers.
- Within the period 2006-2009, telecoms fraud will also primarily manifest itself within telephony services. The emergence of Voice over IP will enlarge and simplify the palette of gathering methods. No substantial shift is foreseen regarding the nature of perpetrators, although the number of occasional fraudsters will probably increase. In this period, the magnitude of damage suffered will at least remain equal to the present values, but probably increase. A realistic quantitative estimate can not be made at present.