A Workable Definition for Identity Related Crime

Ricardo M. Mata y Martín 1/ Alfonso Galán Muñoz 2

Identity fraud

"Whosoever possesses, obtains, transmits, sells or transports third-party payment instruments in an unauthorised manner which are generally accepted on the market place, and which are especially protected against counterfeiting or fraudulent use, or does so with the data that they contain, to such an extent that their fraudulent use might affect the patrimony of an indeterminate group of persons, will be punished by a sentence of ..."

Identity theft

"Whosoever by any technological or conventional means obtains identifying information on another or other persons without the consent of the persons concerned and with such information, undertakes any relevant action in which they assume the identity they have appropriated will be punished by a sentence of..."

Background

Over recent years, there has been a dramatic increase in events where personal information is fraudulently obtained, especially by computerised means, in order subsequently to carry out actions or operations with the aforementioned information, principally economic in nature, falsely attributing these to the legitimate owners of the information. Although behaviour of this type varies greatly in practice, it normally follows a dual sequence. There is firstly an appropriation of the information which allows the usurper to assume another identity, whether by conventional means (loss of documentation, dumpster diving, surreptitiously observing somebody entering their PIN number when using a cash machine etc.) or by digital or electronic means (skimming, phishing, pretexting, pharming, the use of sniffers or smishing). Secondly, the external facts refer to the use of information or identifying details obtained, using the aforesaid characteristics or information (the identity), in order to attribute certain actions and their legal consequences to another person.

The consequences that arise from this misappropriation of another’s identity can have direct and indirect effects. Although identity theft is generally carried out with the intention of obtaining financial gain, this behaviour also pursues other ends than those of a purely economic nature, such as illegal entry into a country, contacting third persons with a view to committing sexual crimes, avoiding the imposition of fines etc. The objective ends directly pursued by the person responsible for the identity theft tend to give rise to other crimes that are often of greater severity, such as the possible arrest of the affected person, loss of commercial reputation or peace of mind. Identity theft likewise affects supra-individual interests including economic and commercial transactions, veracity in social and legal relations, loss of confidence in documents for personal identification etc. The use of technological innovation by those responsible for such behaviour has meant that these interests are massively and especially intensely affected, thereby rapidly multiplying transactions and the appropriation of personal information.

In view of the scope of protected legal interests affected by identity theft, it is clear that in the most serious cases there is an evident need to apply criminal law. It should, nevertheless, be borne in mind that identity theft also takes advantage of the inherent weaknesses of identification processes. Specialy, in sectors in which the simplicity of the pro-

1 Coordinator of the New Technology and Computer Crime Law Consolidated Research Group (University of Valladolid, Spain).
2 Professor of Criminal Law (University Pablo de Olavide, Spain).
procedure represents a competitive benefit and there is no wish to assume the corresponding economic cost of greater rigor in the confirmation of information, which results in inefficient processes to verify the identity of the contracting parties.

The majority of countries have no specific criminal categories to deal with this type of behaviour. For this reason, the various behaviours related to misappropriation or identity theft are only partially sanctioned, insofar as they are only limited to certain points under consideration, and in a somewhat incoherent fashion. It is true that economic benefits are sought in the majority of cases, such that the existing offences of fraud and criminal deception may be reasonably applied. Nonetheless, even in cases where the pursuit of financial gain is foremost in the perpetrator's mind, there are still other interests in play to which the legislator must attend. The situation is hardly any different in an international context. The Council of Europe Convention on Cyber–Crime only punishes certain forms of identity theft through computer fraud, which entail the creation of false computer data to be subsequently used in a computerised system. Similarly, certain cases of identity fraud of a financial nature may come under the offence of computer fraud. In any event, given the character of this Convention, only circumstances relating to computer networks and systems would be included.

Due to the multiplicity of affected interests which may be fundamentally linked to an attack on economic–property interests and an attack on a person's identity, it is expedient to propose two complementary proposals for incrimination which allow us to cover two of the relevant interests at stake: (a) fraudulent identity theft and (b) generic identity theft.

(a) Fraudulent identity theft
So–called “fraudulent identity theft” is usually undertaken by employing various types of documents or information which identify the person concerned in the market, such as bank account numbers and, above all, instruments and data, which may be used to perform commercial operations. This is especially so for credit and debit cards and the information that they contain, which may then be used in what has become known as e–commerce. Within this context, as we have indicated, in the majority of countries there are criminal offences in place which may be used where financial loss occurs. Thus, over and above any extension to existing protection against the effective use or abuse of these instruments, a reform of the current criminal law should be carried out in order to adapt them to the new realities of the market place (e.g. to include non–magnetic means of payment such as smart cards) and to establish a more coherent and well–proportioned system to combat the great variety of existing suppositions of fact.

Related to fraudulent identity theft, and as set out in the European Council Framework Decision on combating fraud and counterfeiting of non–cash means of payment, there is also the need to create legal instruments which allow the pursuit and punishment of criminal behaviour of this kind in the Euro–zone. These range from obtaining or falsifying third–party payment instruments to their actual fraudulent usage. Actual events demonstrate that in the majority of cases, when a person or persons are detained in possession of one or more falsified or stolen payment instruments, or ones which have been lost by their legitimate holders, it is very difficult or well nigh impossible to demonstrate that the person or persons in illegal possession of the aforesaid instrument was or were involved in its misappropriation or falsification, nor that they had any intention whatsoever of using it to defraud its rightful owner.

Any modification of the protective barriers of criminal law should be justified in terms of due attention to principles of proportionality and ultima ratio. Thus, the criminal offence that has been proposed only covers those behaviours that as a result
of their scope or importance, might influence the market in a particularly intense manner, affecting a specific number of people and it likewise provides protection solely for those payment instruments that are generally accepted on the market and that are also especially protected against and possible fraudulent and/or abusive behaviour. Thus the aforementioned criminal offence would constitute an efficient legal instrument in the fight against the increasingly international, organised and dangerous illicit markets in means of payment which are nowadays emerging, but which in turn respects the principle of ultima ratio.

The proposal also signifies important advantages of a technical nature:

– By placing market protection at the fore, the proposed criminal act does not overlap with other criminal offences which safeguard individual patrimony, thereby avoiding concurrent infractions relating to the same facts.

– The proposed offence is based on the objective risk found in typical behaviours, wherein there is no need for a specific subjective element to concur, such as intention to use or to traffic in the instruments. This bypasses numerous problems relating to evidence.

– The proposed offence covers both physical payment instruments and others of an immaterial nature used when undertaking electronic operations (e.g. PAN, credit card expiry date, CCV etc.)

– The proposed legal offence neither refers to nor enumerates the measures or behaviours by which the perpetrator may have obtained the payment instruments in question or the information contained therein. It therefore permits punishment not only of the acts arising from the possession or distribution of falsified cards or of stolen or otherwise misappropriated originals, but also of any others in which the aforementioned instruments or information may have been obtained through deceitful acts or social engineering which may not always be criminal acts _per se_ (e.g. phishing or pharming).

(b) Generic identity theft

The severity of the conduct and the plurality of interests harmed by identity theft mean that the application of criminal law should not be restricted to the protection of patrimonial interests. Thus, the proposed creation of a criminal offence, which would be categorized within what certain countries refer to as personal falsification and which consists of the non-consensual gathering by either conventional or electronic means, of information which is relevant to others (the appropriation of another person’s identity), the fraudulent use of such third-party information (the use of another’s identity), as well as the pursuit of economic or other ends. In the typical organization of the criminal offence, possible aggravating circumstances may be established due to the high quantity of losses occasioned and the use of large-scale communication mediums in the execution of the acts.

---

65