# Identity theft, identity fraud and/or identity-related crime

**ARTICLE** *in* DATENSCHUTZ UND DATENSICHERHEIT - DUD · SEPTEMBER 2006

DOI: 10.1007/s11623-006-0141-2



**2 AUTHORS:**

Bert-Jaap Koops
Tilburg University
**55** PUBLICATIONS **112** CITATIONS
SEE PROFILE

Ronald E. Leenes
Tilburg University
**94** PUBLICATIONS **246** CITATIONS
SEE PROFILE

[Bert-Jaap Koops & Ronald Leenes (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter', *Datenschutz und Datensicherheit* 2006 (9), pp. 553-556.]

# ID Theft, ID Fraud and/or ID-related Crime. Definitions matter

Bert-Jaap Koops[1] & Ronald Leenes[2]

**Abstract**
Identity theft is often perceived as one of the major upcoming threats in crime. However, there is no commonly accepted definition of 'identity theft' or 'identity fraud', and it is impossible to study the real threat of this phenomenon without conceptual clarity. In this article, we attempt to provide a starting point for policy and research by proposing some definitions. We indicate that what is usually called 'identity theft' (defined as fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent) is part of the larger issue of 'identity fraud'. This, in turn, is a subset of the umbrella term 'identity-related crime', which we define as all punishable activities that have identity as a target or a principal tool. We argue that it is relevant to look at this broader picture, since not only identity 'theft', but also consensual yet unlawful identity changes as well as unlawful identity deletion should receive the attention of policy-makers and legislatures.

## Introduction

'Identity thieves make thousands of victims!' is a typical headline of current e-zines. One pictures thousands of people panicking and pursuing thieves running away with their identities. Reality is different, of course. Identity criminals do no steal identities: they use identity as a tool to steal money. And the typical victim does not notice the crime until long after the criminal has booked a one-way ticket to the tropics. A good reason to have a look at the terminology of ID 'theft', ID fraud, and ID-related crime.

The threat of identity theft is increasingly felt, not only in the United States, where reports present shocking figures and ring alarm bells loudly (see for instance [FTC06]), but also in Europe[3]. However, what is called 'identity theft' – or 'identity fraud' – in these reports is not clearly delineated. In fact, there is no commonly accepted definition of 'identity theft' or 'identity fraud', and it is impossible to study the real threat of this phenomenon when the prevalent literature can only compare apples and oranges. It is therefore necessary to delineate exactly what is meant by these terms. This article, building on [Le06], attempts to suggest definitions for the notions of 'identity theft' and 'identity fraud', and proposes the term 'identity-related crime' as a useful umbrella term.

## 1 Some existing definitions

'Identity theft' and 'identity fraud' are rarely defined in a precise way. Rather, much of the literature provides descriptions or working definitions. A fairly precise definition of 'identity theft', however, can be found in the US Identity Theft and Assumption Deterrence Act (title 18, s. 1028(a)(7) U.S.C.), one of the few laws to specifically criminalise ID theft. Punishable is s/he who:

> 'knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.'

Identity theft is here primarily defined as a subsidiary crime, where an ID is abused to commit another crime.

---

[1] Professor of Regulation & Technology, Tilburg Institute for Law, Technology, and Society (TILT). E-Mail: e.j.koops@uvt.nl.

[2] Associate Professor of Law & Technology, Tilburg Institute for Law, Technology, and Society (TILT). E-Mail: r.e.leenes@uvt.nl.

[3] See, e.g., http://news.bbc.co.uk/1/hi/business/2999694.stm.

In Europe, Mitchison et al. [Mi04] describe it rather narrowly:

> 'Identity theft, in what in this paper is called its 'paradigm' form, occurs when one person – in this study a "rogue" – obtains data or documents belonging to another – the victim – and then passes himself off as the victim.'

This description, like the former, covers only the unlawful use of identifying data from another person. This is a rather narrow view, since credit-card fraud, for example, can also be committed by generating a non-existing credit-card number. In other words, one can equally – or perhaps not quite equally – well commit identity fraud without 'stealing' someone else's identity.
Therefore, 'identity fraud' can be conceived of as a broader term than 'identity theft'. In a study by the UK Cabinet Office [UK02: 9], this is described functionally:

> 'ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.'

Note that this defines as fraud the mere act of assuming another identity, regardless of a subsequent unlawful act. One wonders what Eric Arthur Blair would have thought of this when he assumed the pseudonym of George Orwell. Jan Grijpink [Grij03] is more restricted in this respect, taking identity fraud to mean

> 'that someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person' [translation by the authors].

Some common factors can be noted among these definitions and descriptions. There must be a) some means of identity: a name, document, or other identifying data, b) which does not belong to the perpetrator herself, c) with an element of unlawfulness. However, there are significant differences in scope and emphasis, triggering the question just which activities should be regarded as 'identity theft' or 'identity fraud'. In order to answer this question, a typology of identity-related crime is useful.

# 2 Identity-related Crime

There are many things you can do with identities. Not only can you use someone else's or a non-existing identity, but people can also swap identities or destroy identities. Such things can also happen accidentally. It should be emphasised that these activities need not be unlawful: there are perfectly legitimate reasons for doing such things with identities. Only a subset of what Rost, Meints, and Hansen have termed 'the rearrangement of identity linkage' is unlawful. The typology developed by them, in [Le06: 50-57], is illuminating, since it offers a useful starting point to delineate the various forms of 'bad things you can do with identities'. For this overall category, we propose to use the term 'identity-related crime' as an umbrella term. This covers all punishable activities having identity as a target or a principal tool. (We use the term 'tool' here in the general sense of a means to achieve an end.)

Rost, Meints, and Hansen distinguish four – partly overlapping – types of modifying the link between an identifier and the person (or role) identified by this identifier:

- identity collision, e.g., when two people have the same name, or when a wrong e-mail address is used; this usually occurs unintentionally;
- identity change, when someone takes on another identity, usually intentionally;
- identity deletion, e.g., revoking a digital-signature certificate, or reporting the death of Mark Twain in a newspaper;
- identity restoration, i.e., restoring the link between identifier and person, e.g. when Mark Twain tells the world that reports of his death are grossly exaggerated.

What interests us here is when these acts constitute a crime, or should be considered a crime. For this purpose, the categories of identity change and identity deletion are the most interesting. Identity collision usually happens accidentally, and when it is done with intent, it likely falls into the category of identity change. Identity restoration is usually perfectly acceptable, except when conducted without the consent or knowledge of the person whose identity is being restored; in that case, however, it is again a matter of identity change.

Identity deletion is an interesting category from a criminal perspective. When someone has (part of) her identity deleted by someone else, this can have severe consequences, for instance, when a hacker destroys patient records in a hospital computer system. For such an act to fall within the scope of 'identity-related crime', however, the destroying of the patient record should be done with the goal of

destroying a patient's identity. Otherwise, it simply is a matter of data interference as mentioned in art. 4 of the Convention on Cybercrime[4]. Most instances of unlawful identity deletion will actually fall in traditional categories of crime (e.g., damage to property, data interference, slander). Nevertheless, it is useful for legislatures to analyse whether the intentional deletion of someone else's (partial) identity merits specific criminalisation, given that people can hardly function within (a sector of) society if their existence in (sectoral) files and computer systems is denied.

When someone destroys (part of) her own identity, this may well be considered unlawful; several countries, for instance, have criminalised destroying an official ID, and they consider it unacceptable when asylum seekers destroy their passport before arrival. However, as Rost, Meints, and Hansen rightly point out [Le06: 55], the latter could be seen as building up a new identity rather than merely destroying an old identity, and this could therefore be handled within the category of identity change.

Altogether, the category of identity deletion should not be overlooked when researching identity-related crime, but it can be thought of as an overseeable and perhaps minor phenomenon when compared to the category of identity change, which in its criminal guise can be conceived of as 'identity fraud'. It is this type of identity-related crime that is really the major issue.

# 3 Identity Fraud

## 3.1 A typology of ID change

Identity fraud can roughly be described as the unlawful changing of someone's identity. Rost, Meints, and Hansen [Le06:52-55, RoMe05] distinguish four closely related subcategories of identity change:

- identity takeover, when someone takes over the identity of another person without that person's consent;
- identity delegation, when someone uses someone else's identity with that person's consent;
- identity exchange, when two or more people, with mutual consent, use each other's identity;
- identity creation, when someone creates the identity of a non-existing person.

In all subtypes, the identity change can be perfectly lawful. For instance, a Tony Blair doppelgänger can walk the streets of London to see how the public reacts; a wife can lend her bank card to her husband to purchase something; the prince and the pauper can swap lives for a day; and Eric Arthur Blair may well choose a pseudonym to publish his books. Nevertheless, many cases of identity change can be considered unlawful. When the Tony Blair look-alike uses his doppelgängsterism to receive free services or goods, he commits fraud, and when a director gives the password to her digital signature to her secretary to sign documents he is not authorised to sign, she also commits fraud. Swapping loyalty cards to thwart a supermarket's profiling will not generally be considered fraud, but – depending on the terms and conditions – may well constitute tort. And using a self-generated credit-card number that fulfils the characteristics of credit-card numbers clearly is unlawful.

## 3.2 What is new?

As these examples already illustrate, the bulk of identity fraud cases will readily fall within the ambit of the traditional notion of fraud. This means that, from a strictly legal perspective, there is no need to pay specific attention to identity-related fraud: most if not all cases can be prosecuted as fraud.

Why, then, should we handle identity fraud as a separate category of crime? Although it is not a foregone conclusion that identity fraud is an intrinsic category in its own right, we feel that it merits special treatment, for several reasons. First and foremost, fraud occurs in forms and on a scale formerly unknown, because of the new role of identity management in the information society. Face-to-face transactions have increasingly given way to e-commerce and on-line service-provision, and the information society is based on an ever more complex web of interactions in intricately interwoven relationships. This implies that identifiers such as names and numbers have become much more important as essential entry points for social interactions: without ID, nothing happens – at least nothing much that is legally relevant. (We use 'ID' here in the sense of a partial identifier, which may also be pseudonymous.) And along with the new role of identity in the information society, identity fraud is emerging as an unavoidable consequence.

[4] See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

A comparison with computer-related crime may be instructive here. Although computer fraud can be conceived of as simply another means to commit fraud, it has been considered a category in its own right since the 1980s, when computers started fundamentally changing the way in which society functions. As a result, from the OECD's 1986 report *Computer-related Crime* to art. 8 of the 2001 Convention on Cybercrime, computer-related fraud has featured prominently in instruments to combat computer crime. This is not primarily because forms of computer fraud were not punishable under traditional criminal provisions such as fraud or forgery, although there certainly were some legislative gaps. Rather, specific attention and criminalisation was warranted because combating computer fraud requires special knowledge of computers. Investigation and prosecuting computer fraud implies that the police and judiciary know how to investigate and judge the technical odds and ends of computers and computer data. Moreover, successfully combating computer fraud is not only a matter of prosecution, but also – and perhaps even more – a matter of prevention. For this, awareness must be raised, since computers create specific vulnerabilities that organisations and individuals tend to disregard through ignorance.

The same is true now for identity fraud. The new forms and scale of identity management create new opportunities for fraudsters. Phishing (collecting personal data on-line for use in financial services) is a prime example of such a new phenomenon, which has been mushrooming since a few years. In order to combat these new forms of fraud effectively, it should not only be studied whether or not current legal provisions must be extended, but also, and more importantly, strategies should be developed tailored to the specifics of identity fraud. This requires adequate insight and understanding of the vulnerabilities of identification infrastructures, leading to a balanced mix of legal, technical, and socio-economic measures [Le06].

A significant part of any identity-fraud combating strategy is awareness-raising. This is a second reason to treat identity fraud as a special category. Opportunities for identity fraud thrive as long as people develop and use identity-management technologies without heed of their potential for abuse. It is only when people are educated about the various risks of identity fraud, that the weakest link in identification vulnerabilities can be strengthened. In this respect, Europe can benefit from the example of the US, where through the Identity Theft and Assumption Deterrence Act, a complaint and education centre has been established with the Federal Trade Commission.[5] In Europe, the UK has a similar website.[6]

A third reason to look at identity fraud as a separate category is the victim's perspective. Unlawful identity takeover ('identity theft') differs from traditional fraud in two fundamental ways. First, it takes time for the victim to notice the crime, which may happen long after the identity 'thief' has fled to Vanuatu with his gains. Second, the victimisation of the victim may well continue long after the crime, since, contrary to most traditional cases of fraud, a feature of identity takeover is that the victim is blacklisted and has difficulty in regaining her credit history and trustworthy image. This difficulty is another characteristic of current identification infrastructures. It is therefore altogether important to study the specifics of identity fraud in order to support victims effectively.

## 3.3 Definition

The definitions of identity fraud given in section 1 stress the element of assuming a false identity. Perhaps surprisingly, the definitions do not go into the element of fraud as such. This means in effect that the act of taking on a false identity would constitute a criminal act in itself, if done with malicious intent. It is thus a subsidiary crime, resembling other forms of punishable preparatory acts.

It should be borne in mind that criminalisation of preparatory acts is an exception to the rule. Criminal law, at least in most current legal systems, penalises bad activities rather than bad intentions. There may be good reasons to criminalise the preparation of a crime apart from the crime itself; for instance, when the preparation necessarily leads to the crime, when it is much easier to detect and prove than the crime itself, or when the crime carries a particularly high risk for society.

Although we do not exclude the possibility that one or more of these reasons hold for identity fraud, we feel that defining identity fraud on the basis of false identity rather than on fraud lays a wrong emphasis. After all, there are legitimate reasons for assuming another identity, but none so for committing fraud. In other words, the core of identity fraud should be seen in fraud rather than in

[5] http://www.consumer.gov/idtheft/.

[6] http://www.identity-theft.org.uk/.

identity. What distinguishes identity fraud from fraud in general, however, is that it uses identity as a tool or, occasionally, as a target. The latter may be the case when, for example, the Tony Blair look-alike ostentatiously visits a prostitute in order to smudge Blair's identity.

At the same time, we should be careful not to call 'identity fraud' all cases of fraud in which some form of identity is used. If it concerns merely another instance of fraud, there is no need to call it identity fraud; on the contrary, we risk blurring the issue by tarring everything with the same brush. Rather, we should bear in mind the reasons mentioned in the previous section that identity fraud merits treatment as a special category. This implies that it is relevant to distinguish identity fraud from fraud in general when knowledge of identity or awareness of vulnerabilities in identity management is relevant in combating the type of fraud at issue. This is when the 'identity' tool is something more than merely accessory to the crime.

We therefore propose the following definition, based on our definition of identity-related crime.

> Identity fraud is fraud committed with identity as a target or principal tool.

'Fraud' in this definition need not necessarily be defined. It can be understood in terms of the existing legal definitions of fraud which prevail in different countries, or in terms of internationally used definitions such as the Convention on Cybercrime's definition in art. 8: 'procuring, without right, an economic benefit for oneself or for another person.'

# 4 Identity Theft

Having focused on identity fraud as a useful target of research, we have still the prevalent term of 'identity theft' to consider. What is usually meant with this term is the subcategory of unlawful identity takeover from the broader category of identity fraud.

'Identity theft' is a rather awkward term, since identity is not something that is typically stolen. A characteristic of theft, after all, is that the owner no longer possesses the stolen thing. With identity, this is usually not the case: the victim of identity takeover still retains her identity. We should therefore speak of 'identity "theft"' rather than of 'identity theft'. Another reason to be hesitant in using this term broadly, is that it invites overlooking the other forms of identity fraud. The consequences for third parties of identity takeover *with* consent (as in unlawful identity delegation or exchange) may be equally serious as those of identity takeover without consent (as in identity 'theft'). Policy-making and action plans should therefore not be confined to unconsensual identity takeover.

Having said this, we admit that identity 'theft' is a major issue and probably the most important subset of identity fraud and identity-related crime at large. Giving a definition is, however, not straightforward. The definitions in section 1 focus on the assumption or use of the identity of another existing person. As in our discussion of identity fraud, it is questionable whether this strikes the right note. By focusing only on the element of another's identity, it is implied that the crime is targeted at the person whose identity is taken. Mitchison's description explicitly calls this person 'the victim' of the crime. However, from the perspective of the perpetrator, the target is not so much the identity bearer as the person or institution who is fooled by the false identity. The latter may equally truly be called a victim of the crime. Again, it seems a matter of focusing on the preparatory act of assuming a false identity as such versus focusing on committing a crime by using a false identity. The former has, almost by definition, the identity bearer as victim. In the latter approach, the victim of the crime is the one who bears the loss; depending on the allocation of liabilities in the legal system, this may be the shop or institution who provides goods or services to the wrong person, the bank accepting the means of payment, and/or the person in whose name the transaction is being done and who may be blacklisted as a result. This is context-dependent.

Since identity 'theft' is not primarily targeted at the person whose identity is used, and since the question who is the victim of the crime depends on the context of the modus operandi and the legal distribution of liabilities, we propose to stress the 'target crime' – usually fraud, and occasionally other crimes such as slander or extortion – rather than the subsidiary element of using another's identity. The latter element is nevertheless relevant, from the perspective of awareness and the grave consequences for identity bearers if they *are* victims. This leads to the following definition.

> Identity 'theft' is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent.

# Summary and Conclusions

Identity theft is often perceived as one of the major upcoming threats in crime. However, there is no commonly accepted definition of 'identity theft' or 'identity fraud', and it is impossible to study the real threat of this phenomenon without conceptual clarity. In this article, we have attempted to provide a starting point for policy and research by proposing some definitions.

We have indicated that what is usually called 'identity theft' is part of the larger issue of 'identity fraud'. This, in turn, is a subset of the umbrella term 'identity-related crime'. We have argued that it is relevant to look at this broader picture, since not only identity 'theft', but also consensual yet unlawful identity changes as well as unlawful identity deletion should receive the attention of policy-makers, legislatures, and others involved in identity management.

Identity-related crime merits treatment as a discrete category of crime, because in the current information society, identity management involves vulnerabilities and hence leads to abuse in ways that require special knowledge and understanding to prevent and combat. Moreover, people should be educated on these specific risks, and victims require special attention because of the potential consequences particular to identity-related crime, such as being blacklisted.

This has led us to propose the following, hierarchically ordered, definitions.

- '**Identity-related crime**' concerns all punishable activities that have identity as a target or a principal tool.
- '**Identity fraud**' is fraud committed with identity as a target or principal tool.
- '**Identity "theft"**' is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent.

We are aware that these definitions are not the final word. Elements such as 'identity', 'fraud', 'principal', and 'existing person' will need to be further delineated and defined, which will require extensive discussion. However, we hope that these definitions provide a shared, conceptually clear starting point on which further discussions can be based.

## Literature


FTC06 Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data. January – December 2005*, FTC, January 2006.

Grij03 Grijpink, J., 'Identiteitsfraude als uitdaging voor de rechtstaat' [Identity Fraud as a Challenge to the Rule of Law], *Privacy & Informatie*, Vol. VI, No 4, pp. 148-153, August 2003.

Le06 Ronald Leenes (ed.), *FIDIS deliverable 5.2b ID-related Crime: Towards a Common Ground for Interdisciplinary Research,* May 2006, available at http://www.fidis.net.

Mi04 Mitchison, N. et al., 'Identity Theft – A Discussion Paper', *Technical Report EUR 21098 EN*, European Commission - Joint Research Center, 2004.

RoMe06 Rost, M., Meints, M., 'Authentisierung in Sozialsystemen – Identitytheft strukturell betrachtet', *Datenschutz und Datensicherheit* 4/2005, pp. 216-218, Wiesbaden April 2005.

UK02 UK Cabinet Office, *Identity Fraud: a Study*, UK Cabinet Office, London, 2002.