Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Mistaken identity, identity theft and problems of remote authentication in e-commerce

Eliza Mik

Singapore Management University, Singapore

Keywords:
Identity theft
e-commerce
Authentication
Digital signatures

ABSTRACT

The problem of mistaken identity in e-commerce transactions brings together seemingly unrelated issues: privacy, network security, digital signatures – and classic contract law. Combining an academic exercise with the practical implications of the insecurity of the Internet, this paper draws some unexpected conclusions regarding cases of mistaken identity and exposes flaws in popular legal arguments on the subject. Problems of mistaken identity must be analysed afresh with a number of factors in mind: the more widespread use of fictitious identities in on-line transactions, the higher incidence of identity theft and the greater difficulty of authenticating the other transacting party. The trend to preserve the privacy of Internet users indirectly clashes with efforts to ensure transactional security in e-commerce. An indispensable prerequisite of the latter is the ability to identify the other party to the contract. The problem of mistaken identity is not new – but it assumes a different scale in e-commerce transactions.

> … *commerce, on a large scale, can prosper only when people can deal confidently with people they have never met and have no reason to trust.*[1]

1. Introduction

The choice to contract with a specific individual is often based on her special skill(s) or characteristics. Contractual intention may therefore be directed at a *particular* person. The resulting legal problems can be evaluated as part of the offer and acceptance model or from the perspective of the doctrine of mistake.[2] Offer and acceptance relate to contract formation; mistake is generally considered a factor affecting the validity of a contract. This paper focuses on mistake, in particular, on the technological aspects of mistakes pertaining to the identity of the other contracting party. In e-commerce, identities are embodied in information, not flesh.[3] Transactions occur over an open and inherently insecure network. It is therefore necessary to re-evaluate existing approaches to cases of mistaken identity. It becomes unavoidable to account for the fact that identifying the actual, physical person behind a click or an email may be next to impossible. Problems of identification are traditionally discussed alongside attribution, not intention. Attribution focuses on accountability for an act, intention relates to the existence of a contract. Both attribution and the intention to contract with a specific person require the ability to identify this person. As it is the recipient

[1] W Diffie, S Landau, Privacy on the Line: the Politics of Wiretapping and Encryption, 48 (1998).
[2] S Smith, Atiyah's An Introduction to the Law of Contract 76–77 (2006).
[3] Lucy Cradduck, Adrian McCullagh, *Identifying the Identity Thief: is it time for a (smart) Australia Card?* I.J.L. & I.T. (16) 2, 125, at 127 (2008).

0267-3649/$ – see front matter © 2012 Eliza Mik. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.03.009

who must prove that the (alleged) sender dispatched the message, attribution is predominantly a question of proof.[4] Before asking who is accountable for the transaction, it must be established whether a contract exists. The presence and effect of a vitiating factor must be taken into account prior to – or at least in parallel with – any discussions of contractual liability.

A mistake as to identity is a unilateral mistake: one party is mistaken, the other knows of the mistake or caused it. Generally, a mistake as to the identity of the other party renders a contract voidable.[5] In some circumstances, however, such mistake may render the contract void *ab initio*. It is these circumstances that require revision in light of the characteristics of e-commerce transactions.

1.1. *The problem*

In the classic scenario crook (C) fraudulently represents to the owner of goods (O) that he is another person (X) and on that basis O parts with goods to C by way of sale. Is there a contract between O and C? If a contract exists but is voidable, C passes good title to an innocent purchaser. If the contract is void, such purchaser cannot obtain valid title. The protection of third parties plays a prominent role in all mistaken identity cases. The issue is less relevant between O and C, as the mistaken party can rescind for misrepresentation. Little attention is usually devoted to the carelessness of O or to X, the person C purports to be. This problem has recently been revisited in *Shogun Finance Ltd v Hudson*.[6] The majority in *Shogun* held that no contract was formed between O and C. The decision was predominantly based on the construction of the written contract between O and X, the person named in the contract.

While difficulties of identification arise in all first time transactions between strangers, e-commerce transactions seem to exacerbate these difficulties and shed new light on the aforementioned legal problem. The possibility of holding a contract void (i.e. non-existent) due to a mistaken belief as to the other party's identity must be re-analysed with two factors in mind: *first*, a more widespread use of fictitious identities in on-line transactions than in the real world and a higher incidence of identity theft; *second*, the practical problems of remote authentication over insecure networks such as the Internet.

1.2. *Terminology*

Some terminological clarifications are necessary. "Identification" is the process of distinguishing one entity from another. "Authentication" has multiple meanings: to "establish as genuine" or to "associate oneself" with a document, as in "to sign."[7] For present purposes, "authentication" refers to the verification of an identity.[8] Authenticating documents differs from authenticating persons: senders authenticate *messages*; recipients authenticate the *senders* of messages. Authentication involves the presentation of authentication information that confirms the association between a person and an identifier. Authentication information consists in something a person *knows* (password, PIN), *possesses* (token, smartcard, passport) or *is* (biometric data). Access to authentication information enables the assumption of the identity verified by this information. In this sense, the term "identity *theft*" denotes the unauthorized use of authentication information relating to an existing person. Knowledge or possession of authentication information does not automatically imply that the person with such knowledge or possession *is* the person to whom the information rightfully belongs.[9] Lastly, as all e-commerce transactions are conducted at a distance, it seems more correct to speak of "remote authentication."

1.3. *Broader context*

Legal problems never exist in a vacuum. Mistaken identity and difficulties of authentication intersect with general privacy and security concerns posed by the Internet. The process of authentication requires the disclosure of authentication information. Privacy protection, on the other hand, aims at hiding the real identities of persons and preventing any association between them and their on-line activities.[10] Privacy protection requires the limitation of both the collection and the disclosure of authentication information. The more such information is revealed and the easier the access to such information, the greater the risk of its unauthorized use.[11] After all, "personal information" may serve as "authentication information."[12] Authentication information can be used to create *and* to verify an identity. In practice, using the authentication information of another person amounts to assuming the identity of such person. Accordingly, there is an inherent tension between privacy and the need to authenticate the other party in an e-commerce transaction. Privacy requires anonymity; e-commerce requires the disclosure of real identities. While being a tool to achieve privacy, anonymity is also a means of avoiding accountability. Privacy preservation measures may prevent effective authentication, whereas authentication attempts may violate privacy laws.

Additional complications arise from the fact that the Internet is an inherently insecure network. Practically every computer, or device, connected to the Internet can be

[4] W Ford, M S Baum, Secure Electronic Commerce, Building the Infrastructure for Digital Signatures and Encryption 336 (2001) ("*Ford & Baum*") p 336; another term used in legal literature is "non-repudiation."

[5] *Lewis v Averay* [1972] 1 QB 198.

[6] [2004] 1 AC 919 ("*Shogun*").

[7] Oxford English Dictionary; S Mason, *Validating Identity for the Electronic Environment*, 20 CLSR 3 at 166 (2004).

[8] R Shirey, RFC 2828, *Internet Security Glossary*, 13 (2000).

[9] Nicholas Bohm & Stephen Mason, *Identity and its Verification*, [2010] 26 CLSR 43–51, at 44.

[10] For a discussion of anonymity on the Internet see: A M Froomkin, *Flood Control on The Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 15 J L & Com 395 at 422 (1996).

[11] Holly K Towle, *Identity Theft: Myths, Methods, and New Law*, 30 Rutger's Comp & Tech L J 237 at 262 (2004) on the "Collision between Identity Theft and Privacy;" A Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 Yale J L & Tech 123 (2004–2005).

[12] J Grijpink, *Biometrics and Identity Fraud Protection*, [2005] 21 CLSR 254.

compromised and accessed without authorization. Hardly a week goes by without news about network security breaches in organizations with seemingly impenetrable information systems.[13] Experts speak of "rampant exploitation of compromised end-user systems."[14] Storing personal information on an insecure network leads to possible misuses of such information due to security breaches.[15] Such breaches frequently result in the misappropriation of personal information and lead to identity theft. While identity theft is not a new phenomenon, its occurrence has risen dramatically since the advent of the Internet. Identity theft aside, the inherent insecurity of the Internet also affects the ability to establish the identity of the other party: a person may appear to be the originator of a message – but he is just a victim of a security flaw in his machine.[16] It is against this background that the existing approaches to mistaken identity must be re-examined.

2. Method of communication: face-to-face and "by correspondence"

The case law on mistaken identity distinguishes between dealings face-to-face[17] and dealings by correspondence.[18] In the first scenario, O is presumed to intend to deal with the person in front of him, in the latter, the parties are named in the document. When O intends to deal with the physical person in front of him it is more difficult to raise the argument that the identity of such person was of fundamental importance, i.e. the mistake itself cannot be regarded as "essential." Where O and C deal by correspondence, identity assumes greater weight and there is a theoretical possibility of holding the contract void. The principles are not applied consistently, the "blurring" factors being the protection of innocent purchasers, the exact moment the representation is made, and the actual intention of the mistaken party. In practical terms, the division is between making a contract with the person one *intends* to deal with or the person one *actually* deals with. In Shogun, the minority expressed the view that "new means of communication render the distinction untenable."[19] The majority, however, whilst recognizing the problem, did not address its undesirable side effects and re-affirmed the distinction.

Two arguments can be raised against its continued use in legal arguments. *Firstly*, even conventional transactions are often a mixture of face-to-face dealings and correspondence. Written documents frequently follow oral negotiations. The mistake is identical in both situations: O deals with one person but intends to deal with another.[20] O deals with the writer of the email, the person in front of him or on the other end of the telephone line. Whatever the mode of communication, O agrees to sell his goods to the person with whom he is dealing.[21] The presence or absence of "writing" should not constitute a ground for distinction. The essence of the transaction is the same, irrespective of how the parties communicate. Accordingly, the law should be the same. *Secondly*, the majority of e-commerce transactions cannot be easily placed in either category. Are interactions via instant messengers face-to-face or by correspondence? What category does a video conference fall under? Is it the text-based character of a particular method or its real-time quality that is decisive? Does the use of a text-based method of communication imply that an e-commerce transaction tainted by a mistake as to the identity of the other party is always void? The antecedent question is whether such text-based method renders the e-commerce contract "in writing." It is easy to devise more examples demonstrating the futility of the distinction. Both arguments converge on one conclusion: the effect of the mistake – which ultimately determines whether a contract exists – should not depend on the communication method used in the transaction.[22]

It must, however, be acknowledged that the communication method affects the quality and quantity of authentication information available to O.[23] In *Phillips v Brooks*, the face-to-face scenario is described as enabling the *identification* of the other party by sight and hearing.[24] When dealing via email or on a website, O is limited to validating the digital certificate of the purported sender, if any, or verifying the address information. Frequently, all that is available is the IP address or the HTTP referrer – both of which can be hidden or manipulated. The information about the other party is scarce and unreliable.[25] Accordingly, the method of communication may bear on the difficulty of authenticating C and the authentication mechanisms available to O.

3. Fundamental importance: identity or attribute(s)

Mistake as to identity is traditionally distinguished from mistake as to attribute(s). The prevalent view is that the former renders a contract void, the latter "only" voidable. Certain attributes are, however, perceived as so important that they form part of a person's identity and a mistake as to them can render the contract void.[26] Notably, creditworthiness is not one of them. The identity-attribute distinction has

[13] See for example: http://www.ibtimes.co.uk/articles/156908/20110603/china-google-u-s-white-house-hack-security-gmail-email-clinton-government.htm and http://www.guardian.co.uk/local-government-network/2011/sep/16/data-security-breaches-local-government.

[14] David D. Clerk & Marjory S. Blumenthal, *The End-to-end Argument and Application Design: The Role of Trust*, 63 Fed. Comm. L.J. 357 at 369 (2011).

[15] Bert-Jaaps Koop, *Law, Technology and Shifting Power Relations*, 25 Berkeley Tech. L.J. 973 at 1016 (2010).

[16] David D. Clark & Susan Landau, *Untangling Attribution*, 2 Harv. Nat'l Sec. J. 323, at 335 (2011).

[17] *Lake v Simmons* [1927] ACN 487; *Ingram v Little* [1961] 1 QB 31; *Phillips v Brooks Ltd* [1919] 2 KB 243; *Lewis v Averay* [1972] 1 QB 198.

[18] *Cundy v Lindsay* (1878) 2 App Cas 459.

[19] *Shogun* at 950.

[20] D W McLauchlan, *Parol Evidence and Contract Formation*, 121 LQR 9 at 9 (2005).

[21] *Shogun* at 937.

[22] S Smith, above at note 4, at 84.

[23] B Schneier, above at note 26, at 191.

[24] *Philips v Brooks* [1919] 2 KB 243 at 247.

[25] Lawrence Lessig, Code and other Laws of Cyberspace 28, 30–31 (1999); Jane K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce* (1998) 72 Tul L Rev 1177 at 1213 (1998).

[26] Edwin Peel, Treitel, The Law of Contract 267, 277. (12ed., 2007).

important legal consequences: when C says "I am creditworthy" the mistake concerns an attribute and the contract is voidable; when C says "I am someone else who is creditworthy" the mistakes relates to identity and the contract is void. It is therefore in O's interest to prove the fundamental importance of the buyer's identity. If O succeeds, the contract is void and O retains title to the goods. In e-commerce transactions the identity-attribute distinction must, however, be approached with caution. It is not so much the distinction *per se*, but the "fundamental importance" of identity that may be difficult to maintain. The assumption of different identities for on-line transactions is more widespread than in the real world: people assume various identities due to privacy concerns or as an expression of personal freedom. A person may validly transact under an alias.[27] One person can have multiple identities; the same identity can be lawfully used by multiple persons. Not only is the concept of identity difficult to define but the on-line environment increasingly "commodifies" identity[28] and dilutes its original purpose – that of pinpointing a specific individual.

There is no prohibition to adopt a different identity as long as it is not designed to escape liability or impersonate another entity. If a person does not pretend to be X, the person *is* X.[29] To illustrate: when someone transacts under the pseudonym Pussycat, the other party cannot claim that: "I intended to contract with another Pussycat" or "There is no Pussycat" and therefore there is no contract. *There is a Pussycat*. It is the person who sent the message signed "Pussycat." Similarly, if one assumes the pseudonym John Smith, one is John Smith. Pussycat and John Smith are equally valid identities. The association between person and name occurs in O's mind only. O's accidental knowledge of a person bearing a particular name demonstrates that in many instances the importance of identity is purely subjective. And subjective elements are rarely taken into account in contract law.

Complications arise when someone uses an identity that happens to be the real identity of an existing person. The existence of such real person may be accidental and unknown to both transacting parties. Where a person assumed what she believed to be a fictitious identity, it can be questioned whether it is correct to speak of mistaken identity. The latter term seems more appropriate in instances of "identity theft", i.e. the use of somebody else's identifying information to engage in transactions *as* the person whose identifying information was "stolen."[30] In the leading case of *Cundy v Lindsay*[31] the contract was held void because O only intended to contract with the person *named* in the correspondence and *knew* of a company dealing under the name assumed by C. In *King's Norton Metal*,[32] O was held to intend to contract with the writer of the letter and there *existed* no other entity of the assumed name. The contract stayed intact. In both cases C pretended to be X but in the latter case – X did not exist.

The identity-attribute distinction is further complicated by the conceptual turmoil surrounding "identity" and the inconsistent use of the term in mistaken identity cases.[33] "Identity" is a concept shaped by its context. Moreover, only *persons* – not names or identities – become parties to a contract. "Persons" must therefore be distinguished from "identities." It is always a person who assumes an identity. It is always a person who enters a shop or sends an email. Persons are primarily identified by names.[34] Ideally, names should be uniquely attached to persons, pointing to the accountable individual. Names, however, are not unique.[35] Once used in an open environment, such as the Internet, they lose their association with persons. As persons cannot be distinguished by names alone, they must be co-defined by their attributes.

In other words, global uniqueness can only be achieved by combining names with attributes.[36] "Identity" can therefore be regarded as a construct of name and one or more attributes. The identity-attribute distinction becomes even harder to maintain when one takes into account that persons can be identified by their attributes only, e.g. the painter of the picture, the person in the room. Frequently – and especially in mistaken identity cases – "identity" is used interchangeably with "name." It is important to distinguish the two concepts. There are a numerous motivations to contract with a particular person. It is, however, illogical to assume that one intends to contract with a person because of her name. Names are labels used to identify an individual.[37] They constitute a pure reference, without regard to *any* attributes. At the same time, names may constitute a tool to confirm attributes. Some names (such as "Warren Buffet") automatically imply the existence of certain characteristics. Even in the latter scenario, however, it must be assumed that additional proof is required to confirm that the person actually is Warren Buffet.

In sum, contracting partners are chosen based on their attributes, not their names or identities. Even when identity appears to be of fundamental importance, such as in contracts for specialized services, it is important because it points to a person with specific attributes.[38] The importance of "identity" must be limited to cases where contractual performance is limited to a unique individual.[39] In such instances, however, it is not a question of "identity" being more important than "attribute" but a question of the two terms becoming practically synonymous as the identity automatically implies the

[27] *Shogun* at 951.

[28] Dan Svantesson, *The Significance and Protection of Identity in the On-line World*, [2011] 27 CLSR 1–3, at 2.

[29] *Treitel*, above at note 26, at 274.

[30] H K Towle, above at note 11 at 238, 241; J Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 Berkeley Tech L J 259 at 260 (2005); "theft" is a misnomer, as the person whose identifying information was "stolen" can still use her identity.

[31] *Cundy v Lindsay* (1878) 2 App Cas 459.

[32] *King's Norton Metal Co Ltd v Edridge Merrett & Co Ltd* (1897) 14 TLR 98.

[33] The difficulty of defining "identity" is stressed by S Smith, who speaks of mistake as to *person* and mistake as to *identity*, above at note 4, at 76, 77.

[34] Niels Ferguson, Bruce Schneier, Practical Cryptography 323 (2003) ("*Ferguson & Schneier*").

[35] B Schneier, above at note 25, at184.

[36] Nicholas Bohm, Stephen Mason, above at note 9, at 45.

[37] *Shogun* at 969.

[38] Michael Furmston Cheshire, Fifoot and Furmston's Law of Contract 208 (2001).

[39] *Boulton v Jones* (1857) 2 H & N 564, 157 ER 232; *Said v Butt* [1920] 3 KB 497; *Sowler v Potter* [1940] 1 KB 271.

existence of unique attributes. The identity-attribute distinction must be approached with caution whenever the transaction is of a mass-market character, the seller is willing to contract with anybody and the contract can be performed by anybody.[40] In sum, the focus on "identity" introduces subjective elements into the discussion and taints the transaction with uncertainty. While the concept of "attribute" is relatively straightforward (the *good* singer, the *creditworthy* buyer), the concept of "identity" remains blurry (who *is* John Smith?). A contract's existence (i.e. void or voidable?) must not hinge on a distinction ridden with so many ambiguities.

The importance of identity and its potential impact on the existence of a contract must also be re-evaluated in light of the technical difficulties of establishing the identity of the other party in e-commerce transactions.

4. Remote authentication – digital signatures

The Internet is plagued by problems of establishing the person on the other end of the communication channel. It is possible to identify a machine on the network. It is difficult, however, to tie a *person* to a specific machine.[41] As information pointing to specific computers is easily hidden or manipulated,[42] one of the main challenges of Internet-based communications consists in establishing ways of authenticating (i.e. confirming the identity of) the other party. Digital signatures are often portrayed as the solution to these challenges. Their practical deployment, however, paints a different picture and illustrates the potential futility of authentication efforts on open, insecure networks. Digital signatures are usually discussed in the context of formal requirements or the functions of traditional signatures.[43] This line of argumentation is, however, of limited relevance. Determining *whether* a digital "signature" meets formal requirements is distinct from determining *who* signed the document. Assuring enforceability is pointless if it is unclear who to enforce the contract against. The same can be said about determining what intention a signature was made with. Moreover, as traditional signatures do not automatically link the name-holder to the signature, carry a presumption of authenticity or reverse the burden of proof – none of these functions can be performed by their digital equivalents. Comparing digital signatures to traditional signatures is therefore pointless. The term itself – digital *signatures* – must be regarded as a misnomer. One more point before proceeding: model regulations[44] and statutes[45] distinguish between "electronic" and "digital" signatures. The former relate to any electronic representation of a name, such as letters or digitised handwritten signatures, the latter rely on asymmetric cryptography. The regulations differ to the extent that some equate digital or electronic signatures with handwritten signatures, without reversing the burden of proof, while others create technology-dependent presumptions.

Digital signatures rely on the mathematical correspondence between the private and the public key in asymmetric cryptosystems. A message encrypted with the public key can only be decrypted with the private one – and the other way round. The private key is tied to the message by means of a "hash function" and cannot be re-used. For the digital signature model to work, the public key must be accessible to everyone, the private key – exclusively to its authorized user. Absent any natural association between person and key-pair,[46] a trusted third party must guarantee that a given key belongs to a specific person. Consequently, digital signatures must be supported by a public key infrastructure ("PKI") or by a web of trust.[47]

The cornerstone of PKI is a Certification Authority ("CA"), which manages Digital Certificates ("DCs").[48] A DC contains information about the person it was issued to ("subscriber") and the public key. All potential subscribers are authenticated by the CA before obtaining a DC. The authentication processes ranges from simple verifications that an email belongs to a particular person, to elaborate procedures entailing notarised documents. The more comprehensive this process, the stronger the assurance that the subscriber is who he claims to be.[49] It must not be forgotten that the DC only associates a key-pair with an identity – not with a physical person. There is no natural link between the digital signature and the subscriber, comparable to the biometric link between a person and her handwritten signature or the mathematical correlation between the public and private keys. Digital signatures only guarantee that a specific message was transformed with a specific private key. *Anyone* who uses the private key produces a valid digital signature.[50] The strength of the cipher, the length of the key or the trustworthiness of the CA (including the authentication of potential subscribers) is *unrelated* to the relationship between the digital signature and the subscriber.

While the public key remains in a generally accessible repository managed by the CA, the private key is "at the mercy" of the subscriber – usually stored on a networked computer. The security of an individual computer depends on the security of the network it forms part of. The latter depends on the access control measures implemented to protect the network from unauthorized entry. Access control measures involve the presentation of authentication information. In sum: the security of private key depends on the robustness of the access control measures protecting it. The computationally intensive discovery of the private key is usually

[40] Hugh Beale, Chitty on Contracts (vol. 1, 26th ed., 1989) para 356.

[41] David D. Clark & Susan Landau, above at note 16, at 324.

[42] *Compuserve Inc v Cyber Promotions Inc* 962 F Supp 1015, 1020 (1997).

[43] Sharon Christensen, *The Statute of Frauds in the Digital Age – Maintaining the Integrity of Signatures*, 10 MurUELJ 4 (2003); Chris Reed, *What is a Signature?* J. Info. L. Tech. (3) (2000).

[44] E.g.: UNCITRAL Model Law on Electronic Signatures; American Bar Association Digital Signature Guidelines.

[45] E.g.: Electronic Signatures in Global and National Commerce Act (Public Law 106–229).

[46] Ch Sundt, *PKI – Panacea or Silver Bullet?*, 5 ISTR at 54 (2005).

[47] *Ford & Baum* at 251, 275.

[48] *Ferguson & Schneier* at 29.

[49] See generally: D S Anderson, *What Trust is in These Times? Examining the Foundation of On-line Trust*, 54 Emory L J 1441 (2005).

[50] S Matthews, *Authorization Models – PKI versus the Real World*, 5 ISTR 66 at 66 (2005); A Srivastava, *Is Internet Security a major issue with respect to the slow acceptance rate of digital signatures?* [2005] 21 CLSR 392 at 397.

unnecessary if access to the key is protected by a password or PIN, which can be hacked with little effort. It is often forgotten that digital signatures are not forged but private keys are used without authorization. The key's security – and therefore the reliability of digital signatures as a method of remote authentication – is a function of the security of the authentication information that enables its use. Digital signatures can be a reliable method of remote authentication only if the private key is secure – or undeniably tied to the subscriber. While digital signature technologies were designed to counterbalance the insecurity of the Internet, they cannot function on an insecure network.[51] In light of the above it becomes apparent that contracting parties have limited means of reliably identifying the other transacting party. That is – unless they are willing to engage in computer and network forensics. The practical difficulties in authenticating the other transacting party have a direct bearing on some arguments made in mistaken identity cases.

5. Carelessness of O

A closer look at the cases on mistaken identity reveals that C is not the only person responsible for the mistake. C misrepresented who he is, but it is O who relied on this misrepresentation. Mistaken identity scenarios are frequently characterized by *some* carelessness on O's side. It can be assumed that being concerned with risk allocation, today's courts may consider whether O has been negligent.[52] After all, holding the contract void rewards the careless O and punishes an innocent third party. As the intention to contract with a specific person is evaluated objectively, O (the party pleading mistake) should take reasonable steps to authenticate the other party. "[I]f a party takes the risk that the facts are not as he supposed them to be, or if he is simply indifferent as to the matter to which the mistake relates, the validity of the contract cannot be affected."[53] If O claims that he would not have contracted with C, had O not believed C to be X, O should have verified *who* he was dealing with, i.e. establish that the person *is* X. If O intended to contract *exclusively* with X,[54] there should be objective indicia of such intention, e.g. efforts to authenticate X. Otherwise, O's intention to contract with X *only*, injects a subjective element into the discussion.

The classic cases on mistaken identity, however, do not always appreciate the importance of O's efforts to establish that X is in fact X. The reasonableness of O's belief in C's statement rarely seems to be a decisive factor. In *Cundy v Lindsay*,[55] O verified neither the signature nor the actual address of C. As C did not forge X's signature and gave his own address, a simple inquiry could have revealed the fraud. Similarly, in *Ingram v Little*,[56] O verified that X lived at the stated address but did not verify whether C was X, i.e. failed to authenticate C. Such authentication was performed in *Lewis v Averay*,[57] where C produced an "impressive looking pass" describing him as X. Unfortunately, O failed to authenticate (verify the genuineness of) the pass. In *Shogun*, C produced the driving license of X. Assuming that it contained a photo of the real X, C must have resembled him or replaced the picture with his own. C also forged the signature on the licence. O confirmed the creditworthiness of X on the basis of a fax copy of X's drivers licence. O never verified, however, whether the person presenting the licence was X.[58]

In other words, no *authentication* of C and no validation of the document took place. The claim that the identity of the purchaser was "fundamentally" important should only have been upheld if steps were taken to verify this identity, alternatively, if the reliance on C's representations was reasonable. By verifying the creditworthiness of X, without confirming that C is X, O's actions indicated that *identity* was in fact irrelevant. Identity was only a means of verifying the *attribute* of creditworthiness. The question remains: under what circumstances is O's belief in C's representation reasonable?[59] Transposed into an e-commerce scenario: what efforts should O undertake to authenticate the other party? How high is the standard of reasonableness in on-line transactions given the inherent difficulties of remote authentication?

6. Accountability of X

Mistaken identity cases never mention the potential liability of X: the person whose identity was "stolen." It must be assumed that the outcome of many cases would differ if the transaction involved digital signatures, i.e. X was the subscriber named in a DC and C used the digital signature without X's authorization. If the classic scenario was decided in line with UNCITRAL's Model Law on Electronic Signatures ("MLES"), O's reliance on the authentication information provided by C would have to be "reasonable." More importantly, X would be obliged to safeguard the information enabling the replication of his identity and inform a third party of any compromise of such information. Modified attribution rules would burden X with the risk of unauthorized use of his authentication information.

Solutions such as those contained in the MLES, are not without drawbacks. In traditional transactions, a name-holder is not automatically liable only because an imposter used his name. Similarly, a person is not liable for her forged signature. It is not for her to prove that she did not sign or authorize a particular transaction. Once digital signatures are deployed, however, some regulations protect the recipient of a digitally signed message and "punish" the person whose "signature" was used. One example is MLES Art 8, which obliges the subscriber to protect the private key and notify the relying party and the CA, if any, of its compromise.[60] The relying party

[51] Absent a complex legal regime of risk allocation.
[52] Michael Furmston et al., The Law of Contract para [4.108] (2010), see also: H M Howard, *The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim*, 54 Duke L J 1263 at 1271–1276 (2005).
[53] Michael Furmston, above at note 51, para [4.79].
[54] *Taylor v Johnson* [1932] AC 161 at 217.
[55] *Cundy v Lindsay* (1878) 2 App Cas 459.
[56] *Ingram v Little* [1961] 1 QB 31.
[57] *Lewis v Averay* [1972] 1 QB 198.
[58] C Elliot, *No Justice for Innocent Purchasers of Dishonestly Obtained Goods: Shogun Finance v Hudson*, 5 JBL 381 at 386 (2004).
[59] *Associated Japanese Bank (International) Ltd v Credit du Nord SA* [1988] 3 All ER 902 at 913.
[60] MLES Art 8 ("Conduct of the Signatory").

(O, in our example) must take reasonable steps to verify the reliability of a digital signature, and, where a certificate supports such signature, verify the validity of such certificate.[61]

It is often forgotten, however, that neither a thorough examination of the certificate nor the reliability of the algorithm underlying the digital signature reveals whether the subscriber used the private key. For the subscriber (X), the challenge lies in protecting the private key from unauthorized use, for the relying party (O) – establishing whether the subscriber used the private key. In practice, the subscriber is entirely dependent on the skill of his network administrator whereas the relying party has virtually no means of establishing who used the private key.

Despite these challenges, the MLES directs member states to establish a presumption or substantive rule based on the technical characteristics of the signature and attach consequences to the signatory's failure to fulfil its obligations under Art 8. These range from the alleged signatory being liable for damages or estopped from denying the signature's binding effect.[62] In sum, the MLES disregards the practical difficulties of deploying digital signatures in an insecure network and encourages the creation of legal mechanisms that burden the subscriber with the risk of their unauthorized use. Some credit should, however, be given for recognizing that the party whose digital signature was used must not idly await its unauthorized use. Unfortunately, it is difficult to transpose this approach into transactions not involving digital signatures: a person will normally not know that her authentication information was compromised or that her identity was misappropriated. The MLES must also be praised for attempting to establish a minimal standard of reasonableness when evaluating the authentication information presented by the other party – a factor that is generally absent in mistaken identity cases.

7. Conclusions

On a technical level, it must be accepted that as long as the Internet remains insecure, it is virtually impossible to authenticate the other party to the transaction. While no popular technological solution currently exists (short of requiring biometric access to all network end-nodes) the problem can be partially alleviated by prior agreements between network users (e.g. terms and conditions of use frequently found on websites) or by regulatory intervention. Neither prior agreement nor regulation, however, constitutes methods of authentication. What they can achieve is the risk allocation for the unauthorized use of authentication information. It may not be possible to establish *who used* an email account. It may be, however, possible to determine *who is liable* for any activity originating from this account. On a conceptual level, it must be appreciated how the on-line environment affects the concept of "identity." The distinctions traditionally drawn in mistaken identity cases have accumulated critique even before the emergence of e-commerce. Evaluated against the background of the new transacting environment, they seem to be losing any of their remaining justifications.

It seems incorrect to debate the possibility of holding a contract void *ab initio* in cases of mistaken identity if the value of "identity" as a means of distinguishing between persons appears questionable in the first place. The fundamental importance of "identity" can only be entertained if the party seeking to invoke the mistake has undertaken objectively reasonable efforts to authenticate the other party. As Internet-based methods of communication affect the quality and quantity of authentication information, the reasonableness of such efforts becomes difficult to evaluate. While O is theoretically in the best position to uncover the fraud or misrepresentation regarding the other party's identity, it must also be acknowledged that technically O may have no reliable means of verifying such.

O's intention does not change depending on whether the contract is embodied on paper or concluded face-to-face. Neither does it change depending whether the parties used instant messengers or email. Objectively, a person should be treated as intending to contract with the person she is dealing with. If an offer is addressed to X, then it is intended for X – irrespective of X's name or identity and irrespective of the manner of communication. O wants to contract with someone who will perform the contract, be it due to his creditworthiness or specific skill.

While it is relatively easy to criticize the distinctions made in mistaken identity cases, it is difficult to suggest even simple answers to questions pertaining to reasonableness of the authentication efforts expected from the contracting parties. It is one thing to say: authentication on an insecure network is impossible, it is yet another to absolve the transacting parties from the implied obligation to do whatever is within their reach to establish the identity of the other party. For the time being, we must resign ourselves to the fact that e-commerce transactions, more than their real world counterparts, will remain contaminated with uncertainty. The simple principle stating that the whenever one of two innocent persons (O or third party purchaser) must suffer because of the acts of a third, "he who has enabled such third person to occasion the loss must sustain it"[63] becomes almost impossible to apply.

Eliza Mik (*elizamik@smu.edu.sg*) *School of Law, Singapore Management University*.

[61] MLES Art 11 ("Conduct of relying party") para 73; see also: See: MLEC Art 13 (3) (b), (4) (b), Guide to Enactment para 83; similarly (5) precludes the sender from disavowing the message, unless the addressee knew or should have known that the message was not that of the sender; see further: S Mason, *Electronic Signatures – Evidence*, [2000] 18 CLSR 242, at 243.

[62] MLES Guide to Enactment para 141.

[63] Lickbarrow v Mason (1787) 2 Term Rep 63 at 70; see also Lord Millet in *Shogun* at 82.1.