Fall 2010

Known and Unknown, Property and Contract: Comments on Hoofnagle and Moringiello

James Grimmelmann
Cornell Law School, james.grimmelmann@cornell.edu

KNOWN AND UNKNOWN, PROPERTY AND CONTRACT: COMMENTS ON HOOFNAGLE AND MORINGIELLO

James Grimmelmann[*]

In addition to gerund-noun-noun titles and a concern with the misaligned incentives of businesses that handle consumers' financial data, Chris Hoofnagle's *Internalizing Identity Theft*[1] and Juliet Moringiello's *Warranting Data Security*[2] share something else: hidden themes. Hoofnagle's paper is officially about an empirical study of identity theft, but behind the scenes it's also an exploration of where we draw the line between public information shared freely and secret information used to authenticate individuals. Moringiello's paper is officially a proposal for a new warranty of secure handling of payment information, but under the surface, it invites us to think about the relationship between property and contract in the payment system. Parts I and II, respectively, of this brief essay will explore these hidden themes in Hoofnagle's and Moringiello's articles. I hope the exercise will tell us something interesting about these two papers, and also about the problems of privacy and security in the payment system. A brief conclusion will add a personal note to the mix.

I. INTERNALIZING IDENTITY THEFT: KNOWN AND UNKNOWN

Chris Hoofnagle's *Internalizing Identity Theft* is built around a clever, if obscure, provision in the federal Fair and Accurate Credit Transactions Act of 2003 (FACTA).[3] A victim of identity theft is entitled to obtain any "application and business transaction records" relating to the theft from the entity that did business with the identity thief.[4] This remedy helps victims recover from identity theft,[5] but Hoofnagle realized it could also be used to study the problem. He convinced identity-theft victims to request their files and share them with him, allowing him to sketch a portrait of how new-account fraud happens in the real world.[6]

---

[*] Associate Professor of Law, New York Law School. My thanks to the participants in the Data Security and Data Privacy in the Payment System Symposium, particularly Ted Janger, Chris Hoofnagle, and Juliet Moringiello. Aislinn Black and Caucus also provided helpful comments.

1. Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & TECH. 1 (2009).

2. Juliet Moringiello, *Warranting Data Security*, 5 BROOKLYN J. CORP. FIN. & COMM. L. 63 (2010).

3. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1953 (amending the Fair Credit Reporting Act and codified with it at 15 U.S.C. §§ 1681–1681x).

4. 15 U.S.C. § 1681g(e)(1) (2006).

5. Hoofnagle, *supra* note 1, at 4–7.

6. *Id.* at 6–8.

Running through *Internalizing Identity Theft* is a recurring question: how much information about us should be well-known and public, and how much should be unknown and private? In the first place, identity theft itself depends on what is known and unknown about potential victims. Hoofnagle frames the issue in terms of a debate between Daniel Solove and Lynn LoPucki.[7] To Solove, identity theft is a crime of too much knowledge.[8] When an individual's identifying, personal information flows freely through computer systems, unscrupulous fraudsters can access that information and use it to impersonate her.[9] In contrast, LoPucki describes identity fraud as a crime of too little knowledge.[10] Identity thieves take advantage of the fact that all of the millions of differences between themselves and their victims are unknown to the credit-granting business.[11]

Despite this apparent tension, both stories are right in important ways. Identity theft is only possible when the fraudster knows enough about the victim to plausibly impersonate her *and* the credit grantor doesn't know enough to make the impersonation implausible again. That is, identity theft is a crime of differential knowledge; it requires the perpetrator to know at least as much about the victim as the credit grantor does. It's a kind of Turing Test: if the would-be thief can answer every question about the victim that the credit grantor knows how to ask, there is no way for the grantor to tell the two of them apart.[12] It follows that identity theft is not a monotonic function of the quantity of publicly available information about the victim. Putting more information in circulation helps thieves fool businesses and helps businesses catch thieves; which effect will dominate isn't something we can easily determine without getting our hands dirty.

Hence the importance of studies like Hoofnagle's. The remarkably consistent pattern in his results is that credit grantors aren't making effective use of the information they already have access to. *Every single fraudulent application in the study* got basic, easily checked information wrong: the wrong address, the wrong date of birth, even the wrong spelling

---

7. *Id.* at 1–3.

8. Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003).

9. *Id.* at 1229–39.

10. *See* Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003) [hereinafter LoPucki, *Privacy*]; *see also* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89 (2001) [hereinafter LoPucki, *Human Identification Theory*].

11. Hoofnagle, *supra* note 1, at 2.

12. *See* Alan M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433 (1950), *reprinted in* THE TURING TEST: VERBAL BEHAVIOR AS THE HALLMARK OF INTELLIGENCE 67 (Stuart Shieber ed., 2004) (arguing that claims of artificial intelligence might be evaluated using an "imitation game" in which a person and a computer both attempt to convince a questioner, who can communicate with them only via typewritten messages, that they are the person).

of the victim's name.[13] Identity thieves are dumb, and the companies who offer them credit are even dumber.

While this may be a depressing comment on the sloppiness of American business practices, it's actually an encouraging finding from a policy perspective. We're not caught between Solove's rock and LoPucki's hard place; there's information readily available to businesses that fraudsters don't have.[14] This means there may well be money lying on the table; if businesses had cleaner credit-granting procedures, they'd get more cases right.[15] Hoofnagle suggests that credit grantors be subject to strict liability for the harms they cause when they grant credit to the wrong person.[16] He's not asking them to do the impossible.

The tension between known and unknown also crops up in the FACTA file-access process Hoofnagle's study relies on. There's an obvious security benefit from procedures like it, which give consumers the right to find out the details when someone applies for credit in their names. Not only does it help them fix mistakes after the fact; it helps them detect and prevent impersonation attempts in the first place.[17]

But there's a catch. There's always a catch. A credit grantor who receives a FACTA request cannot simply assume that the requester really is the person whose name appears in the file. Structurally, this is a hard problem for exactly the same reasons that identification during the credit-granting process is hard. The credit grantor has no personal history with the requester, is dealing with him or her at arm's (or more likely, wire's) length, has few outside sources of identifying information it can consult, and may even have incorrect data in its own files.[18]

FACTA takes a cut at this dilemma by requiring identity verification before the business releases its records to the requester.[19] Indeed, the business may decline to release the records if it "does not have a high degree of confidence in knowing the true identity of the individual requesting the information."[20] There are similar processes in the Fair Credit Reporting Act,[21] the Health Insurance Portability and Accountability Act,[22]

---

13. Hoofnagle, *supra* note 1, at 8–13.

14. *Id.* at 13.

15. *Id.* at 15–17.

16. *Id.* at 29–34.

17. *See* Solove, *supra* note 8, at 1264–66; *see also* LoPucki, *Human Identification Theory*, *supra* note 10, at 119.

18. LoPucki, *Privacy*, *supra* note 10, at 1284.

19. 15 U.S.C. § 1681g(e)(2)(A) (2006). The business may also require proof of identity theft in the form of a police report, a threshold that can act as a deterrent to would-be impostors. *Id.* § 1681g(e)(2)(B)(i).

20. *Id.* § 1681g(e)(5)(B).

21. *See id.* § 1681g(a) (giving consumers a right of access to files on them held by consumer (credit) reporting agencies); *id.* § 1681h(a)(1) (requiring "proper identification" as a condition of access).

and the Privacy Act,[23] among other places. Any measure designed to give individuals control over the distribution of their personal information—that is, to limit knowledge about them—requires, as a practical matter, some kind of identity-verification system.

Any such system, in essence, allows someone who presents the right kind of credentials to see certain information. As the very existence of the FACTA file-access remedy itself demonstrates, however, not everyone presenting credentials is who they claim to be. Sarah Palin's Yahoo! email account was hacked, in "an attack that any 17-year-old in America could have mounted," by an intruder who spent 45 minutes of Internet research looking up Wasilla, Alaska's two zip codes and confirming that Palin and her husband had met in high school.[24] Moreover, rules designed to filter out fraudsters almost certainly also filter out some legitimate requests from victims of identity theft. These victims thus find themselves trapped in the Kafkaesque position of being unable to prove that they really are themselves, to the satisfaction of a business that has already shown itself incapable of correctly telling who they are.

Worse, identification measures designed to *limit* information flows also necessarily *create* them. Information used to authenticate in one context can be used to defraud in another. When multiple web sites use the same security questions—*What is the name of your pet? What is your mother's maiden name?*—they become security risks for each other. Even systems that use sophisticated, interactive, multi-step authentication technologies are vulnerable to being snookered by phishers who first impersonate a business to its customer, and then, having talked the customer out of the critical identifying information, impersonate the customer to the business.[25] The continual slow leakage of "private" information used to authenticate individuals has a hydraulic effect; as this information becomes increasingly public, the threshold of information required for reliable authentication rises.

---

22. *See* 45 C.F.R. § 164.524(a)(1) (2009) (giving individuals a right of access to "protected health information about the individual"); *id.* § 164.524(b)(1) (allowing entities to require that such requests be "in writing").

23. *See* 5 U.S.C. § 552a(d) (2006) (giving individuals a right of access to records pertaining to them held by federal agencies); *id.* § 552a(f)(2) (allowing agencies to establish "reasonable . . . requirements for identifying an individual who requests his record").

24. Kate Pickert, *Those Crazy Internet Security Questions*, TIME, Sept. 24, 2008, http://www.time.com/time/business/article/0,8599,1843984,00.html.

25. *See* Stuart E. Schechter et al., *The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies* (2007 IEEE Symposium on Security and Privacy, Working Draft, 2007), *available at* http://usablesecurity.org/emperor/emperor.pdf; Christopher Soghoian & Markus Jakobsson, *A Deceit-Augmented Man In The Middle Attack Against Bank of America's SiteKey ® Service*, SLIGHT PARANOIA BLOG (Apr. 10, 2007, 3:46 PM), http://paranoia.dubfire.net/2007/04/deceit-augmented-man-in-middle-attack.html.

In a final twist, the problem of the known and the unknown also appears in the difficulty Hoofnagle had finding subjects to participate in the FACTA study, even after posting ads on the heavily-read Craigslist site.[26] For understandable reasons, victims of identity theft often prefer not to talk publicly about the experience.[27] But this means there is no simple way to find a list of identity theft victims and call them up. Ultimately, only six subjects completed the study, and five of them were recruited through ID Watchdog, a company that helps victims of identity theft.[28] They, in other words, had already stepped forward to identify themselves. This is how you end up with an N=6 study.

For similar reasons, Hoofnagle's study identifies the subjects only as X1 through X6. It's a common social-science precaution to protect study participants, and one obviously of particular concern to identity-theft victims. Even with confidentiality, two participants found the subject too "upsetting" and dropped out of the study after learning what it would entail.[29] For a study about the problem of identification, the results are a bit incongruous. At one point, Hoofnagle writes, "It is difficult to visualize this case without illustration, but such a description would breach confidentiality."[30] One shudders to think what the process of obtaining IRB approval must have been like.[31]

Amusingly, Hoofnagle also had to deal with would-be fraudsters himself. The study provided gift cards to participants to compensate them for their time and effort.[32] Multiple people called in response to the initial Craigslist ads, "with dubious tales of fraud, in transparent attempts to get a gift card."[33] They were, in other words, fraudsters pretending to be people whom fraudsters had pretended to be—taking advantage of the fact that there is no public listing of actual victims. This secondary deception illustrates, yet again, the obscurity that suffuses the subject of identity theft; *Internalizing Identity Theft* sheds some rare, but valuable light on it.

II. *WARRANTING DATA SECURITY*: PROPERTY AND CONTRACT

Juliet Moringiello's *Warranting Data Security* investigates the rights of consumers whose payment information—such as credit card numbers—is

---

26. Hoofnagle, *supra* note 1, at 7.
27. *Id.*
28. *Id.* at 6–8.
29. *Id.* at 5.
30. *Id.* at 15.
31. *See generally* ZACHARY M. SCHRAG, ETHICAL IMPERIALISM: INSTITUTIONAL REVIEW BOARDS AND THE SOCIAL SCIENCES, 1965–2009 (2010) (describing the history of institutional review boards created to ensure that research does not harm human subjects, and expressing concern about overreaching by such boards).
32. Hoofnagle, *supra* note 1, at 5.
33. *Id.* at 5.

stolen in a data breach.[34] Although consumers typically face little if any liability for unauthorized charges[35] (at least the ones that they notice promptly[36]), they bear a number of other costs, both monetary and intangible: credit monitoring, replacement card fees, lost time and effort, and emotional distress, to name a few.[37] Moringiello argues that as between the consumer and the merchant whose sloppy security led to the data breach, it would be fairer and more efficient to let these costs fall on the merchant.[38] The heart of her paper is an attempt to map this normative argument onto the doctrines of payments law; she concludes that an implied warranty of a secure payment system would be a good fit.[39]

This time, the recurring motif is the uncertain boundary between property and contract. Moringiello's analysis jumps off from a classic question of contract law: whether the implied warranties in Article 2 of the Uniform Commercial Code (UCC) provide a basis for consumers to recover their indirect damages.[40] Unfortunately for consumer plaintiffs, contract law as reflected in the UCC doesn't offer suitable warranties.[41] Neither the warranty of merchantability nor the warranty of fitness for a particular purpose is a close fit for payment information security.[42] Worse, the UCC applies only in the sale of goods[43] (i.e. the sale of tangible movable *property*[44]), and both warranties can be disclaimed.[45]

This leads Moringiello to shift from contract law to property law, specifically to the law of residential leases.[46] Led by the Court of Appeals for the District of Columbia Circuit, American courts in many states read an implied warranty of habitability into most residential leases over the last half century.[47] A residential tenant is entitled to premises "fit for

---

34. Moringiello, *supra* note 2, at 63–72.

35. *See, e.g.*, 15 U.S.C. § 1693g (2006) (limiting the liability of a debit cardholder for unauthorized charges); 12 C.F.R. § 226.12(b) (2010) (limiting the liability of a credit cardholder for unauthorized charges).

36. *See, e.g.*, 12 C.F.R. 205.6(b)(2) (2009) (raising the liability limit when a credit cardholder "fails to notify the financial institution within two business days after learning of the loss or theft").

37. Moringiello, *supra* note 2, at 64, 68–69.

38. *Id.* at 65, 72–80.

39. *Id.* at 80–83.

40. *Id.* at 72–80 (drawing inspiration from a recent case, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108 (D. Me. 2009), in which the plaintiffs unsuccessfully argued that the defendant supermarket chain had implicitly warranted that it would keep their payment information secure).

41. *Id.* at 71.

42. *See id.* at 72–80.

43. U.C.C. § 2-102 (2009).

44. *Id.* § 2-103(k).

45. *See id.* § 2-316.

46. Moringiello, *supra* note 2, at 80–83.

47. *See* 2 POWELL ON REAL PROPERTY § 16B.04 n.37 (Michael Allan Wolf ed., Matthew Bender & Company, Inc. 2010) (listing states).

habitation";[48] an unsafe apartment is ipso facto a breach of the lease on the landlord's part.[49] Moringiello's proposal for an analogous, unwaivable implied warranty of payment information security is thus a conscious effort to make contract law more like property.[50]

Historically, however, courts and commentators described the implied warranty of habitability as a movement in the other direction, one in which property law became more like contract.[51] Common-law courts had treated a lease as a pair of "independent covenants": the landlord conveyed a leasehold estate to the tenant, and the tenant covenanted to pay rent.[52] Even if the land was uninhabitable, the tenant's independent obligation to pay rent continued.[53] As the court in *Paradine v. Jane* explained, "[T]hough the land be surrounded, or gained by the sea, or made barren by wildfire, yet the lessor shall have his whole rent."[54]

The courts that created the implied warranty of habitability took inspiration from contract law, emphasizing instead the real-world purposes for which the lease was made.[55] On a contractual view of the world, an uninhabitable residence looks a lot like the subject matter of a contract whose essential purpose has failed, and thus, it becomes plausible to treat the tenant's promise to pay rent as dependent on the landlord's promise to deliver possession in a form the tenant can actually use.[56] Other doctrinal shifts in the landlord-tenant revolution, such as imposing a duty to mitigate damages on the landlord whose tenant moves out mid-lease, similarly drew

---

48. Javins v. First Nat'l Realty Corp., 428 F.2d 1071, 1079 (D.C. Cir. 1970).

49. *See* RESTATEMENT (SECOND) OF PROPERTY (LANDLORD AND TENANT) § 5.1 (1977) ("[T]here is a breach of the landlord's obligations if . . . the leased property . . . is not suitable for residential use."); *see also id.* § 5.4 (same, if condition arises after tenant's entry and landlord fails to make repairs within a reasonable period).

50. Moringiello, *supra* note 2, at 83–84.

51. *See, e.g.*, *Javins*, 428 F.2d at 1074–75; Hiram H. Lesar, *The Landlord-Tenant Relation in Perspective: From Status to Contract and Back in 900 Years?*, 9 U. KAN. L. REV. 369, 372–75 (1961).

52. *See, e.g.*, Wade v. Jobe, 818 P.2d 1006, 1011 (Utah 1991) ("Under traditional property law, a lessee's covenant to pay rent was viewed as independent of any covenants on the part of the landlord.").

53. *See, e.g.*, Lawler v. Capital City Life Ins. Co., 68 F.2d 438, 439 (D.C. Cir. 1933).

> [I]t is long established that upon the letting of a house there is no implied warranty by the landlord that the house is safe; or well built; or reasonably fit for the occupancy intended. The tenant is a purchaser of an estate in the property he rents, and he takes it under the gracious protection of caveat emptor.

Id.

54. Paradine v. Jane, (1647) 82 Eng. Rep. 897 (K.B.) 898.

55. *Javins*, 428 F.2d at 1079.

56. *See* Edward Chase & E. Hunter Taylor, Jr., *Landlord and Tenant: A Study in Property and Contract*, 30 VILL. L. REV. 571, 616–41 (1985) (discussing destruction-of-premises cases as propertarian or contractual).

on the idea that the lease was primarily a contract and only secondarily a transfer of a property interest.[57]

Still, as much as a lease is a contract, it is still *also* a property transaction, and as the habitability revolution took hold, it stopped drinking as deeply from the contractarian well. Concerned about oppressive landlords and unfortunate tenants, courts allowed tenants alleging a breach of the warranty to remain in possession while withholding rent, even when the most natural contractual remedy would have been recission.[58] Even more dramatically, they made the implied warranty of habitability non-waivable—a logical enough consumer-protection move, but not exactly one consistent with classical freedom of contract.[59] The modern implied warranty of habitability—a strong set of mandatory minima for residential houses and apartments—has less to do with the logic of contract, in which the parties are free to pick whatever rule they wish, and more to do with the logic of property, in which legal interests come only in a few standardized packages, and the parties must order one or another from the menu given them.[60]

On that note, return to Moringiello's proposed warranty—to be provided in any transaction that uses the payments system—that the retailer's payment system is secure, regardless of whether the transaction is for goods, services, intangibles, or what-have-you.[61] One way of thinking about this new warranty is that it would be incident to any transaction involving a payment (i.e. sales and leases), which would seem to locate it squarely in the contractual tradition. But perhaps "warranty" isn't the closest legal category. Focus on what the retailer actually promises: to protect the information given to it during the payment.[62] This promise focuses on the payment information, rather than on the nominal subject of the transaction. On this view, the retailer sounds more like a bailee, promising to keep consumers' property (i.e. their payment information) secure while in its possession. While bailments are technically a species of property relationship, like leases they sit on the border that property shares with contract.[63]

---

57. *See, e.g.*, Sommer v. Kridel, 378 A.2d 767, 768–69 (N.J. 1977).

58. *See, e.g.*, Pugh v. Holmes, 405 A.2d 897, 907–08 (Pa. 1979). Indeed, from the tenant's point of view, the ability to remain in possession was the warranty's principal advantage over the common-law doctrine of constructive eviction—an early termination of the lease by a tenant who claimed the premises had become unusable and proved it by moving out. *See, e.g.*, Boston Hous. Auth. v. Hemingway, 293 N.E.2d 831, 837–38 (Mass. 1973).

59. *See, e.g.*, *Boston Hous. Auth.*, 293 N.E.2d at 843.

60. *See generally* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1, 3 (2000) (discussing "limited number of standard forms" in property law).

61. Moringiello, *supra* note 2, at 80–83.

62. *Id.*

63. Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 811–20 (2001).

Bailments doctrine turns out to be a surprisingly good fit for Moringiello's proposed warranty, even though bailments are most commonly created for tangible items: cars left in parking lots;[64] goods stored in warehouses.[65] Bailments can arise by implication, just like the warranty.[66] A bailee is strictly liable for misdelivery, which captures the core legal promise of the proposed warranty.[67] And a bailee's risk of liability ends when it returns the goods; presumably, a retailer who deletes its only remaining copy of a customer's payment information ought to be on safe ground from then on.[68] Given this close fit, Moringiello's bailment-like warranty may be a more workable borrowing from property law than more ambitious (but so far unsuccessful) attempts to create full-fledged property rights in personal information.[69]

Moringiello's proposed warranty points in yet another intriguing direction that mixes property and contract: the problem of privity. Privity is already one of the classic issues in payment systems law. A promise to pay is a contractual obligation; the genius of negotiability doctrines is that they synthesize freely transferrable *in rem* property rights from these *in personam* contractual obligations.[70] Warranties enter the picture to allocate liability. When something goes wrong due to fraud or carelessness, the various actors in the payment chain invoke their warranties to push the loss along the chain until it lands at the "right" place—the one whose mistake caused the loss.[71] Privity is thus both a problem to be overcome and a device to track legally significant relationships.

The same issues arise in a world with a warranty of safe payment information handling. If the warranty is a purely contractual affair—a promise made by a retailer to its customers—then it doesn't apply when the breach happens further upstream, say at the retailer's payment processor.[72] To work, the warranty seems to need to be a genuinely propertarian duty, one that runs with the personal data to which it is attached, no matter whose

---

64. *See, e.g.*, Allen v. Hyatt Regency-Nashville Hotel, 668 S.W.2d 286, 287 (Tenn. 1984) (treating a car left in hotel garage as a bailment).

65. *See* U.C.C. art. 7 (2004) (establishing rights and duties of bailees under warehouse receipts and bills of lading).

66. *See, e.g.*, Russell v. American Real Estate Corp., 89 S.W.3d 204, 210–11 (Tex. App. 2002).

67. *See* RESTATEMENT (SECOND) OF TORTS § 234.

68. *See id.*

69. *See, e.g.*, LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 160–61 (1999) (proposing "a kind of property right in privacy").

70. *See* U.C.C. § 3-203(b) (2010) ("Transfer of an instrument . . . vests in the transferee any right of the transferor to enforce the instrument."); *see also id.* §§ 3-202, 3-305, 3-306 (allowing the "holder in due course" of a negotiable instrument to enforce it free from various personal defenses that would otherwise apply).

71. *See id.* §§ 3-416, 3-417 (specifying warranties given by transferors and presenters of negotiable instruments).

72. Moringiello, *supra* note 2, at 78–79.

hands that data is in.[73] Or, perhaps, the retailer who let the data out of its control (by entrusting it to the untrustworthy payment processor) should be held liable for its subsequent misadventures.

Either way, however, the property/contract logic of payments law shows the way forward. The commercial entities that process payments information are linked to each other by chains of contracts: merchant to payment processor to acquiring bank to association to issuing bank. Those contracts can come with warranties, express or implied or statutory, and losses can be pushed along the chain until they stop at the "right" place—usually (but perhaps not always) the entity whose lax security caused the breach. By framing the issue as a problem of handling information (property) safely during a transaction (contract), Moringiello's proposal enables us to focus on the essential risk-allocation question at the heart of payment data security.

III. I AM X6

And now for the twist ending: *I am X6.* One evening in the spring of 2007, someone walked into a Kohl's in Trumbull, Connecticut and claimed to be me. (I have an alibi; I was at a conference in Germany on the day I was allegedly shopping in Connecticut.) The identity thief applied for a Kohl's credit card, was approved, and promptly charged a $400 mixer and $150 cutlery set to the card. Thoughtfully, if somewhat bafflingly, he or she also signed me up for the Account Ease plan, which would forgive up to $10,000 of debt were I to die or be seriously hospitalized.

I first heard about it when "my" new credit card showed up in the mail; I promptly called up Kohl's to inquire, and the friendly Upper Midwesterners who answered the phone walked me through the process of submitting an affidavit that my identity had been stolen. Within two days, they agreed that I was the victim of identity theft and released me from all charges. And there the matter sat, or would have, had I not offhandedly mentioned the incident to Chris Hoofnagle, a year and a half later, and been recruited into his FACTA study.

What came back in response to my FACTA request of Kohl's was unimpressive.[74] There was an application, on which my last name was spelled "Grimmalan" in the space reserved for the first name. The signature looked nothing like mine—and not very much like the signature on the charge slip, either. The charge slip did have my social security number (listed as my "Cust ID") and my name—this time, misspelled only to the extent of "Grimmelman." The clerk who took the application had clearly

---

73. *See generally* Molly Schaffer Van Houweling, *The New Servitudes*, 96 GEO. L.J. 885 (2008) (discussing servitudes in intangible property).

74. *See* Brad Stone, *How Lenders Overlook the Warning Signs of ID Theft*, N.Y. TIMES BITS BLOG (Apr. 7, 2010, 2:21 PM), http://bits.blogs.nytimes.com/2010/04/07/how-lenders-overlook-the-warning-signs-of-id-theft.

been sloppy, too: the store number and date were missing from the form. There was nothing else in the file. Even though the application specifically stated, "You MUST have a state issued picture ID and a current charge card to apply," Kohl's apparently hadn't kept copies of either on file—leading one to ask whether the fraudster provided them in the first place. Kohl's did know my mailing address—that's how they sent me the credit card and bill—but it didn't appear in the application.

All in all, the application was transparently slipshod. Looking over the file, it was obvious why the nice Upper Midwesterners on the phone at Kohl's had been so nice. One even remotely skeptical look at the application would have been enough to show that it was fraudulent.

No one looked, though, and as a result, Kohl's lost a mixer and some kitchenwares. That sort of thing happens all the time; mistaken seller-financed credit is just another source of shrinkage, along with clumsy stockroom clerks and five-finger discounts. The difference is that with identity theft there's another victim, even when the fraud is detected and admitted by the store. Kohl's is out a mixer, but I lost time, and could have lost some of my creditworthiness. I didn't lose much of either, but other victims aren't so lucky.

Most importantly, *there was nothing I could have done to prevent the identity theft.* To this day, I still don't know where the fraudster got the information about me that he or she gave to Kohl's. Nor was I present at Kohl's when the deal went down; by the time I could wave my arms and say, "Wait! That's not me!" the mixer was long gone. That's why Hoofnagle and Moringiello appropriately focus on assigning responsibility within the payment *system.* Until we fix the systematic flaws that made stealing my identity feasible and profitable, it could happen to you too.