



## **Identity Theft: Making the Known Unknowns Known**

1. Introduction.....	3
2. The Known Knowns: Identity Theft.....	6
New Account Fraud.....	6
Account Takeovers and Credit Card Fraud .....	9
3. The Known Unknowns.....	10
Missing Data and Other Limits on Identity Theft Surveys.....	11
Law Enforcement Statistics Do Not Capture the Problem Either.....	13
4. Making the Unknown Knowns Known .....	15
Mandated Reporting of Identity Theft Incidences and Severity .....	15
a. Incidences Suffered or Avoided .....	16
b. The Form of Identity Theft Attempted and the Product Targeted.....	17
c. The Amount of Loss Suffered or Avoided.....	18
Who Reports and To Whom?.....	18
5. The Challenges of the Reporting Approach.....	20
Institutions Themselves Are Not Always Aware of Identity Theft .....	20
Reporting Could Enable Fraud.....	21
Reporting Will Pitch Lending Institutions Against Victims.....	21
The Market Will Solve the Identity Theft Problem .....	23
6. The Benefits of the Reporting Approach.....	25
Reporting Will Identify the Most Vulnerable Practices .....	25
Reporting Will Provide Metrics for Interventions .....	26
Reporting Will Eliminate Some Polling Mischief .....	27
Reporting Will Dramatically Reduce Identity Theft, As A True Market For Protecting Consumers Will Arise.....	29
7. Conclusion .....	31



CHRIS JAY HOOFNAGLE, IDENTITY THEFT: MAKING THE KNOWN UNKNOWNNS KNOWN, 21 HARV. J.L. TECH. \_\_\_\_ (FORTHCOMING FALL 2007).

We cannot tell whether consumers, regulators, and businesses are over or under reacting to the crime. We cannot determine whether identity theft is more or less prevalent, or more or less severe than a year ago. We cannot determine how the costs of the crime are being distributed back upon society.

These may seem like provocative and confusing statements. How could a crime that did not have a name just a decade ago now plague commerce, online and off? How can we know so little about it? How, despite its apparent prevalence and severity, can it not be measured properly by law enforcement, the public, industry, or policymakers?

The answer lies in the methods used to measure the problem. What we do know has been learned through telephone and internet surveys. While well-intentioned, and valuable for some purposes in the identity theft policy debate, these surveys cannot completely document the contours of the crime.

But more fundamentally, we are asking the wrong people about the crime. The surveys performed seek to obtain information about the crime from victims, individuals who have the most limited view of the problem. Victims often cannot tell how the crime occurred, how their information was stolen, or who stole it.

A solution can be found in gathering information from the entity that knows the most about the crime—the lending institution. If "lending institutions," used here to describe the entities that actually extend credit (such as banks and credit card companies) and control access to accounts (including payment companies such as Paypal and Western Union), were required to provide statistical data about the crime, a more complete and focused picture would emerge. Lending institutions have not provided this information because it could cause embarrassment and because it could attract unwanted

CHRIS JAY HOOFNAGLE, IDENTITY THEFT: MAKING THE KNOWN UNKNOWNNS KNOWN, 21 HARV. J.L. TECH. \_\_\_\_ (FORTHCOMING FALL 2007).

regulatory attention. Another important reason is the advent of "synthetic" identity theft. This new form of the crime, I argue below, has caused us to underestimate the prevalence and severity of identity theft greatly.

My proposal is to require lending institutions to disclose 1) how many identity theft incidences they suffered or avoided, 2) the form of identity theft attempted (i.e. new account fraud, credit card fraud, etc.) and the product targeted (mortgage loan, credit card, etc), and 3) the amount of loss suffered or avoided. As I will explain, these three categories of statistics can be elusive to lending institutions themselves, but even imperfect reporting of them by institutions will benefit public understanding of the crime.

My proposed intervention is relatively simple and does not require extensive regulatory mandates. While there are many challenges, practically and politically, to implementing it, it would result in great benefit to the public. It will enable benchmarking and the identification of additional consumer protections that work and those that do not. It will help regulators and law enforcement allocate the proper resources to fight the crime. It will help clear the air of suspicious polling mischief, the release of surveys that have used questionable assumptions to pin the blame of identity theft to the victims of the crime.

Finally, I believe that this approach will dramatically reduce identity theft. In providing more accurate identity theft numbers, identified by institution, a market will be born. Security will become a market differentiator, much like low interest rates and fee-free accounts. In this market, the carrots of consumer loyalty will be provided to institutions that provide the safest financial products.





CHRIS JAY HOOFNAGLE, *IDENTITY THEFT: MAKING THE KNOWN UNKNOWNNS KNOWN*, 21 HARV. J.L. TECH. \_\_\_\_ (FORTHCOMING FALL 2007).

men are charged with a variety of federal crimes for allegedly using real Social Security Numbers from credit reports combined with fabricated names to apply for credit cards.<sup>9</sup>

One of the men owned a small consumer reporting agency, and apparently has a high level of sophistication in credit practices.<sup>10</sup> The pair established credit histories for synthetic identities by reporting favorable payment information to consumer reporting agencies. In doing so, the synthetic identities appeared to be real people with a track record of paying bills. They then, it is alleged, obtained 250 credit cards from 15 banks, and charged \$760,000 to these synthetic identities.<sup>11</sup>

As will be explained more fully below, synthetic identity fraud cannot always be detected by the individual whose Social Security number was used. This is because the synthetic identity is an amalgam of false and real information, which is sufficient to obtain credit, but may never be attributed to a specific victim's credit record. For instance, in this case, the defendants used real Social Security numbers but wholly fabricated names.<sup>12</sup> Below, from the indictment, it can be seen that a Social Security number assigned to a real person ("Haqqani Saifullah") was used to apply for a credit card for a synthetic identity ("Hanna Curin").<sup>13</sup>

<b>Count</b>	<b>Date (on or about)</b>	<b>False Name</b>	<b>Amount of money obtained from use</b>	<b>Credit card #</b>
1	05/02/2002	Hanna Curin (SSN 7483 assigned to Haqqani Saifullah)	\$3,481.00	Fleet #0519

<sup>9</sup> *US v. Rose et al*, CR06-0787PHK-JAT (VAM) (D. Az. 2006), *indictment filed Aug. 22, 2006*.

<sup>10</sup> *Rose*, Indictment at 2.

<sup>11</sup> *Rose*, Indictment at 3-4.

<sup>12</sup> *Rose*, indictment at 5, 7-8.

<sup>13</sup> *Rose*, indictment at 5.

According to the U.S. Attorney's Office, "None of the individuals whose Social Security numbers were used suffered financial losses as a result of the scheme."<sup>14</sup>

### ***Account Takeovers and Credit Card Fraud***

Second, in "account takeovers," which we think most commonly occurs as credit card fraud, an impostor uses one of the victim's existing accounts. For instance, the impostor may steal a credit card number from the victim and use it without authorization. A variety of consumer protection laws and self-regulatory practices limit liability for financial account takeovers.<sup>15</sup> For example, consumers can dispute fraudulent charges and have them removed from a bill.

But account takeover is much broader than mere credit card fraud. For instance, "phishing" is the practice of tricking the victim into revealing passwords or other information so the thief can access or alter existing accounts.<sup>16</sup> In addition to credit cards, traditional checking and savings accounts are targeted by phishers, as are new payment systems and auction services, such as Paypal and eBay. Once the accountholder is tricked into revealing the password, the account can then be taken over by the thief, and emptied. In the case of credit accounts, consumers can dispute charges when they receive their bill. But when a non-credit account, such as a checking or savings account, is phished, the victim is left with no money and no ability to pay bills.

---

<sup>14</sup> William Carlile, *Two Indicted in Credit-Card Scheme That Used SSNs From Credit Reports*, 5 Privacy & Security Law Report 1257, Sept. 11, 2006

<sup>15</sup> See e.g. Regulation Z, 12 C.F.R. § 226; Regulation E, 12 C.F.R. § 205.

<sup>16</sup> FEDERAL TRADE COMMISSION, HOW NOT TO GET HOOKED BY A 'PHISHING' SCAM (Oct. 2006), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm>.













































