Available online at www.sciencedirect.com
ScienceDirect
Journal of Business Research 61 (2008) 1160–1172
JOURNAL OF BUSINESS RESEARCH

Identity theft: An exploratory study with implications for marketers ☆

Eric M. Eisenstein

The Johnson Graduate School of Business, Cornell University, 321 Sage Hall, Ithaca, New York 14853 USA

Received 1 March 2007; received in revised form 1 August 2007; accepted 1 November 2007

Abstract

Identity theft is the fastest growing crime in America, and millions of people become victims each year. Furthermore, identity theft costs corporations over $20 billion per year, and consumers are forced to spend over $2 billion and 100 million hours of time to deal with the aftermath. This paper uses a system dynamics model to explore policy options dealing with identity theft and to provide implications for marketers. The results indicate that the current approach to combating identity theft will not work. However, inexpensive security freezes could be effective, because they result in a nonlinear reduction in identity theft that is similar to the "herd immunity" seen in epidemiology. Thus, identity theft can be addressed by protecting just a fraction of the total population.

Keywords: Identity theft; System dynamics; Security freezes

> "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."—Warren Buffet

The quote above is particularly true in our networked electronic age, in which information about any one of us can be transmitted around the world in a matter of seconds. Identity theft is a crime that compromises one's reputation in a few minutes, often without awareness of the victim, and with long term and possibly devastating consequences to the victim's financial position. In the last several years, consumers have been almost continuously exposed to heartrending stories of identity theft and recovery of the victims. Identity theft has been called *the* crime of the 21st century, both due to its rapid growth since 2000 and because it relies on the extensive computer networking and architectures that enable the U.S. economy to exist in its current form. Secretary of Treasury John Snow has called identity theft "the greatest threat to consumers today…" because identity theft "…destroys the trust in both people and financial institutions that is necessary to run an open, modern economy" (Snow, 2003). Because of the publicity surrounding identity theft, it also ranks as one of the most important worries among consumers (Consumers Reports WebWatch, 2005; Federal Trade Commission, 2007).

1. What is identity theft?

At the most general level, identity theft is "…the misuse of another individual's personal information to commit fraud" (Gonzales and Majoras, 2007). Most reporting agencies recognize two major subcategories of identity theft: existing account fraud, in which a thief takes over or appropriates an existing account or credit relationship, and new account fraud, in which a thief uses personal information to open new accounts and credit relationships in the victim's name. Existing account fraud is more prevalent and typically less costly than new account fraud (Anderson, 2006; Gonzales and Majoras, 2007; Javelin Strategy and Research, 2007b). Although existing account fraud may result in thousands of dollars of charges to a credit card, laws and corporate policy limit consumer liability for such fraudulent charges, and existing account fraud rarely affects an individual's credit rating. By contrast, new account fraud costs approximately $850 dollars and 80 h of time per

☆ I thank Charles Nicholson, Peter Otto, George Richardson, and the participants of the System Dynamics and Marketing Strategy workshop held at Cornell University in May of 2007 for their insightful comments, suggestions, and aid in model development. This research was funded by Cornell University.
E-mail address: eme23@cornell.edu.

0148-2963/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jbusres.2007.11.012

victim to correct when it is first discovered (Javelin Strategy and Research, 2007b). Moreover, whereas existing account theft is generally over at the time of detection (when the fraudulent account is closed), new account fraud is a symptom of a larger problem—that a thief has stolen one's identity. As a result, new account fraud can continue occurring for years before the thief is caught (as the thief continues to open new additional accounts), and the fraud can have a disastrous effect on the victim's credit rating (even if each occurrence is temporary). Because of the severity of the new account identity theft problem, this analysis focuses only on it.

1.1. How does new account theft occur?

The first step in becoming a victim of identity theft is that a criminal must obtain the victim's identity information, either through low-tech methods such as "dumpster diving" (i.e., rooting through garbage for personal information) or stealing mail, or by using higher-tech methods such as hacking into a corporate computer system, stealing a laptop containing identity information, "phishing" (i.e., fooling a customer into revealing information through a fake website or email), or using malicious computer code to obtain the information (Gonzales and Majoras, 2007). Once identity information is obtained, the criminal either uses it directly (if it is account information in the case of existing account fraud), or applies for credit by posing as the victim (in the case of new account fraud). After an application for credit, almost all potential lenders check applicants' credit scores with one of the three major credit bureaus (i.e., Experian, Equifax, and TransUnion). The bureau reports back a credit score, and, based on that score, the lender chooses whether to extend credit. If the fraud is successful, the lender and the bureau are deceived as to the true identity of the applicant, and the thief obtains credit in the name of the victim. At some point in the future, either the victim or a lender notices the theft, and the resolution process begins by closing the fraudulent account.

1.2. Combating identity theft

Based on how identity thieves exploit the system, there are two overarching approaches to controlling identity theft, which I term *control of information* and *control of use*. Control of information refers to efforts to reduce criminal access to social security numbers and other identifying information about individuals. Control of use refers to tightening procedures surrounding validation of submitted identity information once an application for credit has taken place, in order to control the usefulness of personal identifying information. Using control of information to combat identity theft is important, but is unlikely to significantly reduce the rate of identity theft. The reasons are that (a) identity information is very widely distributed (particularly social security numbers), which means that there are many potential sites of attack; (b) would-be thieves are diligent and resourceful in stealing or obtaining needed information; (c) previous laws that increased penalties for theft have had little or no impact on identity theft rates. A more realistic approach would be to assume that identity information will fall into malicious hands and to reduce the usefulness of such information (i.e., a control of use strategy). One way of reducing the usefulness of information is to use electronic monitoring services to inform consumers of changes to their credit files (Javelin Strategy and Research, 2004, 2007a). Monitoring services are fundamentally reactive, as they inform the account owner of a change only after it has occurred. Furthermore, monitoring systems rely on the account owner's continual vigilance, which is a shaky foundation, because people go on vacation, "spam" filters block email, servers crash, and other things interfere with notification. What monitoring does best is to substantially reduce the time from theft to detection, but monitoring does not prevent a significant amount of identity theft. A second means to reduce the usefulness of information is to create or exploit information bottlenecks in the system, breaking the credit-granting chain of events. There is a natural bottleneck when a credit score is requested from one of the three credit bureaus, because it is almost impossible to open a new credit line without checking with one of the three major bureaus. Thus, the bureaus serve as a natural focal point for preventative measures. One possibility would be to restrict access to credit bureau information about individuals, and a so-called "security freeze" is the legal implementation of this concept. When someone "freezes" their credit bureau file, it means that that the file cannot be shared with potential creditors, which essentially shuts down the possibility of opening a new account. In order for a consumer to open new legitimate lines of credit, she must "thaw" the file, either for a specified period of time, or for a given lender. There is currently no uniform national right to a security freeze; all legislation is at the state level.

2. Identity theft and marketing

Identity theft results in between $17 and $35 billion in losses to retailers and lenders each year, which makes it a major source of loss for companies that market to consumers (Gartner Inc., 2007; Javelin Strategy and Research, 2007b). However, the implications of identity theft for marketing are more serious than the direct monetary cost. For example, identity theft costs corporations substantial amounts of money in the form of preventative services that must used to insulate the business against fraud. More importantly, it is not an exaggeration to say that identity thieves have been enabled by our current marketing practices, and continued concern over identity fraud risks a consumer and legislative backlash against critical marketing activities. It is insightful to compare Europe and America to see how much things could change for American marketers. Identity theft rates are so low in Europe that there are few surveys or statistics to report. In the highest incidence country (Britain) the total identity theft rate is over twenty times lower than in America, with the incidence estimated to be 0.17% of the population in Britain vs. 3.9% per year in America (Weston, 2005). The reasons for this disparity are telling: Europe has almost no access to instant credit, companies are largely forbidden from sharing or selling personal data, credit bureaus