Journal of Monetary Economics 56 (2009) 918–929

Contents lists available at ScienceDirect

Journal of Monetary Economics

journal homepage: www.elsevier.com/locate/jme

Data breaches and identity theft ☆

William Roberds [a,*], Stacey L. Schreft [b]

[a] Federal Reserve Bank of Atlanta, 1000 Peachtree Street, N.E., Atlanta, GA 30309-4470, USA
[b] The Mutual Fund Research Center, LLC, 7301 College Blvd., Suite 220, Overland Park, KS 66210, USA

ARTICLE INFO

Article history:
Received 15 September 2008
Received in revised form
15 September 2009
Accepted 18 September 2009
Available online 26 September 2009

JEL classification:
D83
E42
G28

Keywords:
Identity theft
Identity fraud
Data breach
Fraud
Money
Search

ABSTRACT

An environment is analyzed in which agents join clubs (payment networks) in order to facilitate trade. The networks compile personal identifying data (PID) so as to match transactors to transactions histories. Technological limitations cause the networks' data management practices to impact each other's incidence and costs of identity theft. Too much data collection and too little security arise in equilibrium with noncooperative networks compared to the efficient allocation. A number of potential remedies are analyzed: (1) reallocations of data-breach costs, (2) mandated security levels, and (3) mandated limits on the amount of data collected.

Published by Elsevier B.V.

1. Introduction

Modern information technology enables the collection and storage of large amounts of personal data. While these activities undoubtedly provide economic benefits, it has proved impossible to keep data completely secure against criminal misuse. Survey data suggest that in 2006 identity thieves obtained about $49.3 billion from US consumer victims. Add in the time and out-of-pocket costs incurred to resolve the crime, and identity theft may have cost the US economy as much as $61 billion in 2006 (Schreft, 2007).

This looks like a large cost – equivalent to two Bear Stearns rescues in a year – but the central policy question is whether the size of these losses indicates a market failure (Anderson et al., 2008). In the mind of the general public, the answer seems to be a resounding "yes." Press accounts routinely suggest that too much personal identifying data (PID)[1] is being collected and that this data is being stolen too often, leading to excessive identity theft.[2] This view is echoed in the legal

☆ Helpful comments were provided by an anonymous referee and by participants in presentations at the Federal Reserve Bank of Chicago and Kansas City, the 2008 Payments Workshop at the Bank of Canada, the 2008 LAEF Conference on Payments and Networks at UC Santa Barbara, and the 2009 Workshop on the Economics of Information Security at the University of London. The views expressed in this paper are not necessarily those of the Federal Reserve Bank of Atlanta, the Federal Reserve System, or The Mutual Fund Research Center, LLC.

* Corresponding author. Tel.: +1 404 498 8970.
E-mail addresses: william.roberds@atl.frb.org (W. Roberds), sschreft@mutualfundstore.com (S.L. Schreft).

[1] A.k.a. "personally identifiable information" (PII).

[2] See, e.g., Swartz and Acohido (2007), Caruso (2007), and Dow Jones and Company Inc. (2008a, b).

0304-3932/$ - see front matter Published by Elsevier B.V.
doi:10.1016/j.jmoneco.2009.09.003

literature on identity theft and data confidentiality,[3] where a recurring message is that the credit industry has failed to deliver "efficient confidentiality" of personal data (Swire, 2003). Negative popular sentiment has also contributed to the passage of legislation designed to improve data security practices.[4]

Government reports[5] and industry sources[6] have argued against the market failure hypothesis. These arguments often emphasize two stylized facts. First, losses from identity theft are small relative to overall usage of payments and credit in today's economy (e.g., over $3 trillion in card transactions in the US each year). Second, much identity theft does not result from any compromise of data stored by businesses, but from opportunistic, low-tech criminal activity (e.g., stolen wallets). Because this type of fraud can be effectively deterred through intensive data analysis (Greene, 2009), the implication is that any problem with identity theft could be best addressed by compiling more (e.g., biometric) data on individuals, not less.

Economists (economic theorists in particular) have remained relatively quiet on issues regarding identity theft and data breaches.[7] This paper offers an initial exploration, using a model derived from contemporary monetary theory. Monetary theory is informative for this analysis, as it focuses on two key market frictions that may be counteracted through the use of PID: (1) displacement of agents' consumption demands over time, and (2) a limited ability to force agents to repay debts. The benefit of a multilateral recordkeeping arrangement – a credit-based payment system – derives from its ability to overcome these frictions, and knowledge of agents' identities helps provide this benefit. Credit is impossible without knowing who the debtor is.

The environment studied below extends the model of identity theft developed in Kahn and Roberds (2008) to allow for identity theft through data breaches. The paper begins by presenting a game-theoretic model of multiple payment card networks. Payment networks are modeled as club arrangements for the sharing of information for intertemporal trade. Each club must decide how much data on its members to assemble into a database, and each also must choose how thoroughly to secure its database. Collecting more PID imposes costs on card-network participants, but as industry sources assert, yields a benefit in terms of deterring attacks on the network. On the other hand, collecting such data can have negative spillover effects, because one network's data can be stolen and used to open an account with another network. A network can reduce data theft (and therefore suppress identity fraud) by better securing its database, but it might be cheaper to suppress fraud by increasing the amount of PID compiled.

Using the model environment, we then compare networks' noncooperative data and security decisions to the decisions that a planner would implement. This comparison supports some facets of the "popular wisdom": divergences in social and private incentives cause data to inefficiently overcollected and undersecured. However, the net effect of these practices is shown to be an inefficiently *low* rate of identity theft at the expense of privacy, irrespective of the division of identity theft between its low-tech and high-tech forms. In other words, the model shows how inefficiency of equilibrium can be consistent with the facts emphasized in the "industry view." A final section of the paper considers some policy remedies for this inefficiency.

In summary, the model developed here allows for calculation of the efficient levels of data accumulation and data security, and for evaluation of policies meant to attain efficiency. More generally, it illustrates how any such calculation should balance the costs of data misuse against the substantial gains afforded by the relaxation of anonymity.

2. Institutional background

This section provides a brief overview of the phenomenon of identity theft and its relationship to data security. Recent surveys are given in Schreft (2007) and Anderson et al. (2008).

We begin by defining terms. Identity theft can take many forms in practice. The Federal Trade Commission (Synovate, 2007) divides identity theft into two broad categories: *existing-account fraud* and *new-account fraud*. Existing-account fraud occurs when a thief steals an existing payment card or similar account information (e.g., a checking account number) and uses these to purchase goods and services. Traditionally, new-account fraud occurs when a thief uses someone else's PID to open a new account. As will be clear below, new-account fraud is the type of identity fraud that occurs in the model.[8]

There are no comprehensive statistics on the prevalence of identity theft, or definitive estimates of its cost. In a widely cited survey, the Federal Trade Commission (FTC) estimated that in 2006, 3.7% of the US adult population fell victim to some form of identity theft, at a cost of roughly $16 billion (Anderson et al., 2008). These figures are likely underestimates, however, because they omit certain forms of identity theft as well as many of its indirect costs. Adjusting for some of these effects easily quadruples the cost estimate (Schreft, 2007).

A data breach occurs when an unauthorized party is able to access personal data that has been collected by an organization (e.g., business or payment service provider). Data breaches can facilitate either existing-account fraud (as

[3] See, e.g., LoPucki (2001, 2003), Solove (2003, 2004), Swire (2003), and Chandler (2008).

[4] Including the 2003 US Fair and Accurate Credit Transactions Act (with 30+ pages of implementing regulations) and laws in at least 36 US states.

[5] See, e.g., Synovate (2007) and United States Government Accountability Office (2007).

[6] See, e.g., Cheney (2004), Experian (2006), Kirshbaum (2006), McGrath and Kjos (2006), and Javelin Research (2008).

[7] Some relevant literature is discussed in Section 6.

[8] The term "new-account fraud" includes an increasingly prevalent type of fraud, which is *fictitious* or *synthetic identity fraud*. In this type of fraud, a thief combines information taken from a variety of sources with invented information to create a new, fictitious identity. By one recent estimate, more than 80% of all new-account identity theft has occurred using synthetic identities (Coggeshall, 2007).