Journal of Banking & Finance 33 (2009) 347–357

Contents lists available at ScienceDirect

Journal of Banking & Finance

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

Determinants of banks' risk exposure to new account fraud – Evidence from Germany

Thomas Hartmann-Wendels, Thomas Mählmann *, Tobias Versen

Department of Banking, University of Cologne, Albertus-Magnus-Platz, 50923 Köln, Germany

ARTICLE INFO

Article history:
Received 29 March 2008
Accepted 17 August 2008
Available online 27 August 2008

JEL classification:
G21
K42

Keywords:
Account fraud
Internet banking
Demographics
Socio-economic factors

ABSTRACT

This paper studies empirically the determinants of new account fraud risk within two dimensions: the probability of fraud, and the expected and unexpected (monetary) loss-per-account due to fraud. By fraud risk, we mean the risk that a bank fails to enforce a debt because the identity of the person incurring the debt cannot be ascertained. Using a unique and rich data set of account applicants, provided by a German Internet-only bank, we find that fraud risk is highly sensitive to demographic and socio-economic variables like nationality, gender, marital status, age, occupation, and urbanisation. For example, foreigners are 22.25 times more likely to commit account fraud than Germans, and men are 2.5 times more risky than women.

1. Introduction

New account fraud, which involves the criminal using a false identity, made-up or stolen, to open a new account, typically to obtain a credit card or loan, is becoming a serious concern in our information-based economy. According to official statistics from the German Federal Criminal Police Office, the total costs to banks of new account fraud increased from €13 million in 1999 to over €35 million in 2006. Furthermore, a recent survey conducted by the US Federal Trade Commission (FTC, 2007) studies the prevalence of identity theft (i.e., the misuse of another individual's personal information to commit fraud). Besides existing account fraud, in which a thief takes over or appropriates an existing account or credit relationship (e.g., credit card fraud), the other major subcategory of identity theft is new account fraud, in which a thief uses personal information to open new accounts and credit relationships in the victim's name. Among other things, the survey found that 0.8% of survey participants, representing 1.8 million American adults, reported that in 2005 they had discovered that their personal information had been misused to open new accounts or to engage in types of fraud other than the misuse of existing accounts in the victim's name. In addition, the survey indicates that new account fraud is typically much more costly than existing account fraud. Where the identity thieves opened new accounts, the median value of goods and services obtained by the thieves was $1350, with 10% of the victims reporting that the thief obtained $15,000 or more. In contrast, where the ID theft was limited to the misuse of existing accounts – either credit card or non-credit card – the median value of goods and services obtained was less than $500.

In this paper, we study empirically the factors that determine the extent of new account fraud risk. We define fraud risk as the risk that a debt cannot be enforced because the identity of the person incurring the debt cannot be ascertained. This is distinct from credit risk, which is the risk that an identified debtor cannot or will not discharge his debt. Our empirical exercise is based on a unique data set containing information (e.g., gender, age, employment, marital status, etc.) for more than 203,000 individuals that applied for a checking account by a major German Internet-only bank. In particular, we have information on whether the applicant subsequently (after account opening) turned out to be a fraudster or not, and on the total loss to the bank caused by each fraudster. We use this information to study fraud risk within two dimensions: first in terms of fraud probabilities, and second in terms of monetary fraud losses.[1]

[1] Although we can rely on a rich data set, our findings are subject to one caveat. Since we have no information about rejected applicants, the resulting sample selection effect can possibly bias our estimates of fraud risk determinants. However, we expect any such bias, if even existing, to be far less prevalent within an Internet-only bank applying formalized and automated customer selection procedures, compared to a traditional brick-and-mortar bank relying more on "soft" information to establish a credit relationship.

* Corresponding author. Tel.: +49 221 4702628; fax: +49 221 4702305.
E-mail address: maehlmann@wiso.uni-koeln.de (T. Mählmann).

0378-4266/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jbankfin.2008.08.005

In the first exercise, we employ binary response regressions to find characteristics that measure an individuals' propensity or probability to commit account fraud. Among our explanatory variables are both, a deterrence variable (the previous average account fraud clear-up rate measured on the German state-level) and economic/socio-demographic factors, predicted by the economic theory of crime (Becker, 1968; Ehrlich, 1973) to be related to the supply of offenses. Our results indicate that foreigners are 22.25 times more likely to commit account fraud than Germans. Far less extreme than this, men are 2.5 times more risky than women, and compared to married persons, singles are 1.3 times more risky. A high (low) propensity for fraud can also be observed for blue-collar workers (students/apprentices), and contemporaneously with the new account, fraudsters more often apply for an overdraft facility. Among several age categories, people aged between 36 and 45 years are associated with the highest fraud risk, as well as people noting only their cell-phone number on the application form, compared to people noting only their network number, both numbers, or no number at all. Whereas we find a significantly higher fraud propensity for people living in highly populated states, our results do not support the deterrence theory of crime, put forth in Becker (1968), since the coefficient for the natural logarithm of the average, state-level account fraud clear-up rate is insignificant.

Our second exercise is intended to further highlight the economic significance of our previous results. In particular, we study for a variety of portfolios, composed according to specified applicant characteristics, the amount of equity (i.e., the economic capital) a bank needs to absorb fraud losses up to some probability cut-off (e.g., 99.0%). To derive the implied portfolio fraud loss distribution, we apply the non-parametric bootstrap technique that randomly draws, with replacement, portfolios from the original portfolio. The results are revealing and helpful in assessing the monetary impact of our fraud risk determinants. For example, whereas a portfolio composed completely of German account holders induces an expected loss of €3.5 per account, each account of a foreigner costs the bank €97.8 in expected loss, and additional €29.6 in unexpected loss (calculated as the loss-per-account at the 99.0th percentile minus the expected loss).[2] In sum, to cover all fraud losses in the foreigner portfolio up to a probability of 99.0%, the bank has to back up each account with €127.4 of equity, compared to only €4.3 for the "German" portfolio. Furthermore, to cover fraud losses up to a probability cut-off of 99.0% in the safest portfolio examined, the bank has to support each account with €3.3 of equity. By contrast, to absorb fraud losses up to the 0.99 probability level in the riskiest portfolio, the required amount of equity explodes to €4430.7 per account. These findings further illustrate the discriminatory power of the identified fraud risk determinants.

The literature on new account fraud and identity theft, both conceptual and empirical, is in its infancy. A recent theoretical paper by Kahn and Roberds (2008) develops a model in which identity theft – both the misuse of existing accounts and the opening of new accounts – exists in equilibrium. All identity theft is not eliminated because the investigation needed to verify a person's identity more completely is too costly and involves excessive inconvenience and invasion of individual privacy. To the best of our knowledge, our paper is the first that empirically studies the factors determining a bank's risk exposure to new account fraud.

The remainder of the paper is organized as follows. Section 2 presents some background information on the course of new account fraud and its prevalence in Germany. Section 3 introduces our data and the explanatory variable selection process. Empirical results on fraud risk determinants are described in Section 4, starting first with an analysis of fraud probabilities (Section 4.1), and turning afterwards to monetary fraud losses (Sections 4.2 and 4.3). The paper concludes with Section 5.

2. Background information on new account fraud

2.1. New account fraud within an Internet-only bank

In general terms, a viable payment system must be able to associate debts with debtors, i.e., banks should have adequate controls and procedures in place so that they know the customers with whom they are dealing.[3] Adequate due diligence on new and existing customers is a key part of these controls. The importance of customer identification or "know-your-customer" (KYC) policies has also been recognized by the Basel Committee on Banking Supervision (see BIS, 2001). As a reaction to deficiencies in a large number of countries' KYC policies, as identified by an internal survey of cross-border banking in 1999, the Committee issued a KYC framework in 2001, intended to become a worldwide benchmark for supervisors to establish national practices and for banks to design their own programmes. As a general rule, the framework requires banks to refrain from establishing a banking relationship until the identity of a new customer is satisfactorily verified. Banks need to obtain all information necessary to establish customer identity, especially those documents most difficult to obtain illicitly and to counterfeit. Furthermore, in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview.

However, the customer base of a typical Internet-only bank[4] is exclusively composed of non-face-to-face customers who wish to conduct banking via the Internet or similar technology, and who do not present themselves for personal interview. The impersonal and borderless nature of internet or "pure-play" banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. Even though the same documentation can be provided by face-to-face and non-face-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers, leading to a higher risk of fraudulent misrepresentation. One way to address the issue of an effective identification procedure for non-face-to-face customers consists of independent verification by a reputable third party, a possibility also noted by the Basel Committee. In Germany, almost every Internet-only bank relies on the PostIdent service, offered by the Deutsche Post AG, the German postal services operator and former state monopolist.

To use PostIdent, a bank first has to create a letter for its new customer. This customer letter contains the documents that the bank wants to have delivered to the addressee, as well as a self-addressed return envelope and a coupon, which the customer will then present at his Deutsche Post retail outlet for identification purposes. In the next step, the new customer brings the coupon,

[2] As a comparative value, the expected loss-per-account for the overall portfolio amounts to €5.3, with an unexpected loss (at the 99.0% level) of €0.91.

[3] See Scholnick et al. (2008) for a recent survey of the literature on the economics of important payment mechanisms like credit cards, debit cards and ATMs.

[4] The internet banking distribution channel can be applied in either of two ways: to augment physical branches (click-and-mortar banks) or in place of physical branches (Internet-only banks). Whereas the strategic core of the click-and-mortar banking model is to route standardized, low-value-added transactions (e.g., bill payment, balance inquiries, account transfers, credit card lending) through the inexpensive Internet channel, the logic of the Internet-only banking model is straightforward: a bank eliminates its costly branch overhead, uses the savings to subsidize its prices (paying higher deposit rates or charging lower fees and lower loan rates), and as a result, it can grow faster than its rivals without sacrificing profitability. However, DeYoung (2005) analyzing the performance of a dozen Internet-only banks in the US between 1997 and 2001, found that these banks were, on average, less profitable than their branch banking counterparts, but also have access to deeper scale economies, suggesting that they are possibly becoming more financially competitive over time as they grow larger.