UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 10 | Issue 1 Article 15

2006

Small Businesses and Identity Theft: Reallocating the Risk of Loss

Penelope N. Lazarou

Small Businesses and Identity Theft: Reallocating the Risk of Loss

I. INTRODUCTION

"He devised and repeatedly perpetrated a sophisticated scheme for securing personal identification information from unwitting strangers and then stealing from banks." [1] This portion of the "Statement of Facts" from *United States v. Morehouse*, an identity theft case, reads more like a mystery novel than a district court opinion. But, perhaps this is fitting given the nature of identity theft. Labeled "one of the fastest growing crimes in the world,"[2] many people are unaware of the damage identity theft can cause or how it even occurs.[3]

Identity theft can take a variety of forms;[4] but, regardless of the form, identity theft is often difficult to detect and extremely challenging to correct once it has occurred.[5] The question every victim must ask is: who is responsible for the damages?[6] Should an identity theft victim turn to the police, the financial institution that issued the credit or debit card, the business where the purchases were made, an insurance agency, or all of the above?[7]

While a victim may be tempted to explore all of these options, there are some solutions that are far more effective and beneficial than others, such as punishing the perpetrator or collecting from an insurance agency.[8] Small businesses typically do not have the financial resources to cover the costs associated with identity theft, yet they are sometimes

---

1. United States v. Morehouse, 345 F.Supp.2d 3, 4 (D. Me. 2004).

2. Chris E. McGoey, *Identity Theft Facts: Fastest Growing Crime Worldwide*, CRIME DOCTOR, http://www.crimedoctor.com/identity.htm (last visited Jan. 23, 2006).

3. *Id.*

4. *Id.* Identification such as social security numbers and dates of birth can be used by illegal immigrants to obtain jobs, individuals who charge purchases or establish utility services, or criminals with outstanding warrants. *Id.*

5. *See* U.S. Postal Inspection Service, *Identity Theft: Stealing Your Name* and *Your Money*, http://www.usps.com/postalinspectors/IDtheft2.htm (last visited Jan. 23, 2006).

6. *See Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, FED. TRADE COMM'N. (June 2004), http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf ("What steps should you take and whom should you contact if personal information is compromised?").

7. *See infra* Part IV.

8. *See infra* Parts IV.A, IV.D.

forced to spend a significant amount of time and money as a result.[9] The costs could stem from purchases made by an identity thief from the small business, efforts to assist officials in locating the perpetrator, providing identity theft victims with information, decreases in performance of affected employees, security measures, and more.[10] Small businesses suffer heavier losses than other unwitting participants in the identity theft crime.[11] The costs to a small business for prevention and compensation compared to other participants that are in a much better financial position to bear the loss are significant.[12]

This Note is concerned with the losses borne by small businesses when an identity theft victim's credit or debit card[13] is used for an unauthorized purchase of goods or services from the small business. Part II of this Note defines small businesses and explains their role in the process of identity theft and the ways in which they are implicated.[14] Part III addresses the impacts of identity theft on small businesses in terms of time, money, and other costs, focusing on online retail as an example.[15] Finally, Part IV explores alternative methods for apportioning the costs of identity theft.[16]

II. THE ROLE OF SMALL BUSINESSES IN IDENTITY THEFT

A. Definition of Small Business

"The law defines a small business concern as 'one that is independently owned and operated and which is not dominant in its field of operation.'"[17] In addition to the above requirement, a small business is subject to size standards determined by the Small Business

9. *SBA Sponsors Identity Theft Seminars for Small Businesses Throughout Massachusetts in April, May & June*, IT'S YOUR BUS. (U.S. Small Bus. Admin., Boston, M.A.) (Apr. 2005), at 2, *available at* http://www.sba.gov/ma/april2005_newsletter.pdf.

10. *See infra* Part III.A.

11. *See infra* notes 91-102 and accompanying text.

12. *SBA Sponsors Identity Theft Seminars for Small Businesses Throughout Massachusetts in April, May & June*, *supra* note 9.

13. This Note only considers liability for situations where the same rules apply for both credit and debit cards.

14. *See infra* notes 17-53 and accompanying text.

15. *See infra* notes 54-132 and accompanying text.

16. *See infra* notes 133-193 and accompanying text.

17. *What is Small Business*, U.S. SMALL BUS. ADMIN., http://www.sba.gov/businessop/standards/smallbus.html (last visited Jan. 23, 2006).

Administration (SBA).[18] The standards may be based on "number of employees, dollar volume of business, net worth, net income, a combination thereof, or other appropriate factors."[19]

The SBA establishes the size standards for small businesses, and also serves to "aid, counsel, assist and protect, insofar as possible, the interests of small business concerns."[20] This is no small task given that there were approximately 22.9 million small businesses in the United States in 2002.[21] Small businesses provide about 75% of the net new jobs added to the economy and represent 99.7% of all employers.[22] Furthermore, small businesses employ 50.1% of the private work force.[23] These staggering statistics may lead some to believe "small" business is somewhat of a misnomer.[24] It may be true that collectively small businesses are a force to be reckoned with, but individually, losses from identity theft are felt far more greatly by small businesses than by large businesses.[25]

B. The Role of Small Businesses in the Process of Identity Theft

"These days, it is almost impossible to be in business and not collect or hold personally identifying information—names and addresses, Social Security numbers, credit card numbers, or other account numbers—about your customers, employees, business partners, students, or patients."[26] Thus, by merely maintaining these records, especially in an electronic format, the small business puts itself and its customers at risk.[27] Identity thieves are well aware of the treasure trove

18. Small Business Act of 1953, Pub. L. No. 85-536, 72 Stat. 384 (1958).

19. *Id.*

20. *History of Small Business in the United* States, SMALL BUS. NOTES, http://www.smallbusinessnotes.com/history/ushistory.html (last visited Jan. 23, 2006).

21. *Small Business Statistics*, U.S. SMALL BUS. ADMIN., http://www.sba.gov/aboutsba/sbastats.html (last visited Jan. 23, 2006).

22. *Id.*

23. *Id.*

24. *See supra* notes 21-23 and accompanying text.

25. *SBA Sponsors Identity Theft Seminars for Small Businesses Throughout Massachusetts in April, May & June*, *supra* note 9.

26. *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, *supra* note 6.

27. *Id.*

of information businesses have access to and use a variety of methods to attempt to obtain it.[28]

For the less computer savvy thief, there are physical ways of obtaining personal information.[29] For example, credit cards can be stolen through "robberies, burglaries, [and] postal theft."[30] Criminals can listen in on public telephone conversations when a person provides businesses with a credit card number over the phone.[31] Another method is "dumpster diving," which entails combing through people's trash for old receipts, paycheck stubs, and bank statements, which all contain vital information.[32] "Crooks sometimes seek jobs that will give them access to financial information, or they may bribe employees in such positions to supply them with the data they want."[33] Additionally, "20% of identity theft is committed by the betrayal of personal friends, relatives, employees, and others who are close to you."[34]

In fact, the methods described above are used more frequently to steal identities than technological ones.[35] One survey found that "only 11 percent of known identity cases occurred online, with low-tech dumpster diving and phone fraud accounting for far more thefts than the Internet."[36] One analyst suggests that although the Internet is responsible for a share of identity theft, it might also "help consumers remain vigilant against theft because they can monitor their accounts multiple times over the month."[37] Given that "70% of all identity theft starts with the theft of personal records from the workplace,"[38] consumers should be more wary of the ways in which they store and discard physical information.

---

28. *See infra* notes 29-44 and accompanying text.

29. McGoey, *supra* note 2.

30. 81 AM. JUR. POF 3D § 113 (2005).

31. *Identity Theft and Fraud*, U.S. DEP'T. OF JUSTICE, http://www.usdoj.gov/criminal/fraud/idtheft.html (last visited Jan. 23, 2006).

32. McGoey, *supra* note 2.

33. U.S. Postal Inspection Service, *supra* note 5.

34. *Facts and Figures*, KNIGHTSBRIDGE CASTLE INC., http://www.knightsbridgecastle.com/facts-and-figures.html (last visited Jan. 23, 2006).

35. *See supra* notes 29-34 and accompanying text.

36. *ID Theft: The Real Risk*, CNN MONEY, Mar. 22, 2005, http://money.cnn.com/2005/03/22/technology/personaltech/id_theft/index.htm.

37. *Id.*

38. *Facts and Figures*, *supra* note 34.

Despite these statistics, the use of computers appears to be growing.[39] Via the Internet, thieves could gain access to information provided by individuals for online banking and shopping if there is a security breach.[40] Computer hackers can make their way into the files of a consumer's personal computer or that of the small business with whom the consumer transacts to retrieve valuable information.[41] Furthermore, since the Internet is not regulated, it is an invaluable resource for thieves.[42] While many people are aware of the dangers of providing personal information on the Internet, they continue to do so perhaps because of the speed and ease of Internet transactions.[43] Moreover, many merchants and institutions advertise the security of their transactions.[44]

Despite the precautions many small business owners take, small businesses are especially vulnerable to security breaches.[45] "Awareness and preparation are the biggest differences between a large enterprise and a small business."[46] Identity theft is an issue that is rarely contemplated by small business owners.[47] Perhaps owners are unaware of the problem or maybe they just think they are immune because of their size or do not think they can afford to fix the problem.[48] In fact, the director of a small business development center said "the issue of data security has never come up during his meetings with small business owners."[49]

---

39. McGoey, *supra* note 2.

40. *Identity Theft and Spam Will Deter Online Shopping This Holiday Season*, FORRELEASE.COM, Dec. 1, 2003, http://www.forrelease.com/D20031201/sfm068.P2.12012003105147.20809.html.

41. *Identity Theft and Fraud*, *supra* note 31.

42. 81 AM. JUR. POF 3D § 113 (2005).

43. *Identity Theft and Spam Will Deter Online Shopping This Holiday Season*, *supra* note 40.

44. *See, e.g.*, MASTERCARD INT'L INC., ELECTRONIC COMMERCE SECURITY ARCHITECTURE BEST PRACTICES 1-1 (2003), *available at* http://www.mastercardmerchant.com/docs/best_practices.pdf.

45. *Identity Theft and Spam Will Deter Online Shopping This Holiday Season*, *supra* note 40.

46. Tracy Kershaw-Staley, *Identity Theft Can Be Costly to Small Business*, DAYTON BUS. J., Apr. 22, 2005, http://dayton.bizjournals.com/dayton/stories/2005/04/25/story6.html.

47. *Id.*

48. *Id.*

49. *Id.*

While their skepticism is understandable, small business owners should be very concerned about the crime that is affecting owners and customers alike.[50] With enough identifying information, "a criminal can take over [an] individual's identity to conduct a wide range of crimes: for example . . . obtaining other goods or privileges which the criminal might be denied if he were to use his real name."[51] Moreover, if the criminal ensures that the bills for the purchased items are sent to another address, he can escape detection that much longer.[52] Thus, an identity thief could make countless purchases at the expense of the victim and the small business owner.[53]

III. THE IMPACT OF IDENTITY THEFT ON SMALL BUSINESSES

A. The Impact of Identity Theft on Small Businesses in General

"Identity theft can take months and sometimes even years to detect and can take about the same time to correct the damage."[54] According to one research group,[55] victims of identity theft spend an average of 175 hours and $808 in costs, not including attorney fees, to fix the problem.[56] The problem is magnified when business losses are added to individual ones. In 2003, nearly ten million Americans had their identities stolen by criminals who robbed both the individuals and businesses of nearly fifty billion dollars.[57]

Identity theft could create losses for the small business in several ways.[58] First, if the financial institution refuses to cover the losses, for example, because of a consumer's delay in reporting unauthorized transactions, the small business may not get paid at all.[59]

---

50. Yan Ross, *Identity Theft Can Devastate YOUR Business*, ALL LAW (2004), http://www.alllaw.com/articles/business_and_corporate/article 27.asp.

51. *Identity Theft and Fraud*, *supra* note 31.

52. *Id.*

53. Press Release, Better Bus. Bureau, BBB Targets Identity Theft Campaign to Businesses (Oct. 23, 2003), *available at* http://www.bbb.org/alerts/article.asp?ID=447.

54. McGoey, *supra* note 2.

55. *Id.* The California Public Interest Research Group and the Privacy Rights Clearing House. *Id.*

56. *Id.*

57. Remarks on Signing the Identity Theft Penalty Enhancement Act, 29 WEEKLY COMP. PRES. DOC. 1305 (July 19, 2004).

58. *See infra* notes 59-61 and accompanying text.

59. *See* Visa USA, *Visa Security Program: Zero Liability*, http://usa.visa.com/personal

In addition to the costs of merchandise that may be lost, it requires significant amounts of time and money to prevent identity theft and then investigate thefts on behalf of customers or the business if they do occur.[60] Lastly, there may be costs associated with the small business if its employees become victims of identity theft.[61]

The charge card agreement between a merchant and a bank may provide that "in the event of a dispute between the merchant and a customer who paid by credit card, the bank could debit the merchant's account for the amount involved."[62] Many merchant agreements use virtually the same language regarding liability for these disputes: "Merchant agrees that it is fully liable to Bank and VCS [Verus Card Services] for all Chargebacks, and that Bank and VCS are authorized to offset from incoming transactions and to debit via ACH [Automated Clearing House] the Account . . . in the amount of any Chargeback."[63] Agreements such as this one specify that the merchant's liability can exist as a result of several situations, one of which is: "The Cardholder alleges that he or she did not participate in the sale [or] authorize the use of the Card."[64]

The justification for this policy is that the merchant profits from increased sales due to his acceptance of credit in addition to cash.[65] Therefore, "the risk that a credit card customer may dispute the transaction and refuse to pay is borne by the party who actually accepted payment by credit card."[66] The risk is not unlike that taken by a business that accepts a check which is later dishonored.[67] Although merchants and banks are free to negotiate such arrangements, many

/security/visa_security_program/zero_liability.html (last visited Jan. 23, 2006).

60. *See infra* notes 62-88 and accompanying text.

61. *See infra* notes 89-90 and accompanying text.

62. Schorr v. Bank of N.Y., 91 A.D.2d 125, 128 (N.Y. App. Div. 1983).

63. VERUS CARD SERVICES INC., MERCHANT CREDIT CARD PROCESSING AGREEMENT, Oct. 25, 2004, http://www.busams.com/guide/Harris.pdf; *see also* WESTAMERICA BANK, MERCHANT AGREEMENT, Dec. 4, 2003, http://www.busams.com/guide /westamerica.htm; ADVANTAGE, MERCHANT AGREEMENT, Feb. 14, 2003, http://www.advantagemerchant.com /termsconditions.pdf.

64. VERUS CARD SERVICES INC., MERCHANT CREDIT CARD PROCESSING AGREEMENT, Oct. 25, 2004, http://www.busams.com/guide/Harris.pdf (last visited Jan. 23, 2006).

65. *Schorr*, 91 A.D.2d at 129.

66. *Id.*

67. *Id.*

financial institutions are now promoting agreements with less liability for businesses.[68]

"While the effect on individuals who employ one or more people could be bad enough, the real impact is more likely to be on small to midsize businesses."[69] This is true not only when a loss in goods or payment occurs, but also because regulations impose the same penalties regardless of size.[70] Under the Fair and Accurate Credit Transactions Act (FACTA),[71] an employer could face civil liability, federal fines up to $2,500 for each violation,[72] and/or state fines up to $1,000 for each violation,[73] for failing to comply with the safety requirements imposed to protect consumer information.[74] A couple of thousand dollars may not be a great deal of money to a large business, but to a small business owner, it could be a significant part of profits.[75]

The effects of identity theft are also felt in non-monetary ways. "The crime of identity theft undermines the basic trust on which our economy depends . . . . Identity theft harms not only its direct victims but also many businesses and customers whose confidence is shaken."[76] It is hard for anyone who has suffered at the hands of an identity thief to feel safe enough to engage in similar transactions again.[77] Consumers become more wary and small business, especially online retailers, may be forced to close their businesses if the losses to identity theft become too great.[78] Moreover, identity theft can damage the reputations of consumers and merchants, which may take months or years to repair.[79]

---

68. Visa USA, *supra* note 59.

69. Mindy Fetterman, *Identity Theft, New Law About to Send Shredding on a Tear*, USA TODAY, Jan. 14, 2005, at 1A, *available at* http://www.usatoday.com/money/perfi/general/2005-01-14-shredder-cover_x.htm (requiring businesses to properly dispose of the personal information of its customers).

70. *Id.*

71. 15 U.S.C. § 1681 et. seq. (2005).

72. 15 U.S.C. § 1681s(a).

73. 15 U.S.C. § 1681s(c).

74. Fetterman, *supra* note 69.

75. *Number of Businesses by Annual Revenue*, BIZSTATS.COM, http://www.bizstats.com/bizsizes98.htm (last visited Jan. 23, 2006). While 69.9% of all corporations report annual receipts of over $50,000, only 20.2% of sole proprietorships have annual receipts of over $50,000. In fact, 67.6% of sole proprietorships report annual revenue of less than $25,000 compared to only 24.1% of corporations. *Id.*

76. Remarks on Signing the Identity Theft Penalty Enhancement Act, *supra* note 57.

77. *Id.*

78. Mitchell Pacelle, *At Online Stores, Sniffing Out Crooks Is a Matter of Survival*, WALL ST. J., Aug. 4, 2005, at 1, *available at* http://online.wsj.com/article_print/0,,SB112311

For these reasons, and others, the Federal Trade Commission (FTC) takes measures to mitigate the damages.[80] The FTC requires businesses to notify law enforcement officials if they feel that the security guarding their customer's information has been breached.[81] The FTC also requires businesses to alert the individuals whose information has been compromised and other affected businesses, such as banks or credit issuers, "to allow them to take steps to mitigate the misuse of their information."[82]

Once it is established that identity theft has occurred, small businesses cannot just sit back and let law enforcement handle the matter; they are required to assist significantly in the apprehension of the perpetrator.[83] The FACTA requires "a business from which an identity thief obtained credit, products, or services to provide the victim with copies of an application, if reasonably available, and business transaction records within its control."[84]

Naturally, retrieving and providing copies of this information is time-consuming and costly.[85] The employer may have to reassign an employee or several employees to deal with the effects of identity theft.[86] Small business owner, Neil Kugelman, had to "reassign a staffer to work exclusively on detecting credit-card fraud."[87] Given the few employees and resources small businesses often have, this reassignment can be a major cost.[88] An additional cost is the effect on the

---

786883304593,00.html.

79. Remarks on Signing the Identity Theft Penalty Enhancement Act, *supra* note 57.

80. *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, *supra* note 6.

81. *Id.* ("If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service.").

82. *Id.*

83. Gail Hillebrand, *After the FACTA: State Power to Prevent Identity Theft*, 17 LOY. CONSUMER L. REV. 53, 61-62 (2004).

84. *Id.*

85. *SBA Sponsors Identity Theft Seminars for Small Businesses Throughout Massachusetts in April, May & June*, *supra* note 9.

86. Pacelle, *supra* note 78.

87. *Id.*

88. Jennifer Robison, *Whither the Workers? Small Businesses Lose Employees to Bigger Companies*, LAS VEGAS REV. J., May 4, 2005, http://www.reviewjournal.com/lvrj_home/2005/May-04-Wed-2005/business/1383731.html ("Nationally, SurePayroll said the average number of employees per small business rose 0.2 percent, from 5.86 to 5.87, while the average paycheck dropped 1.8 percent, from $29,261 to $28,737.").

performance of an employee of a small business who has been a victim of identity theft.[89] "Victims on average spent up to 600 hours trying to resolve identity crime, which can impact on their productivity and morale at the workplace."[90]

A small business owner's lack of resources is underscored when compared to the resources available to financial institutions and private corporations. "Banks are including in the monthly statements they send customers pamphlets explaining . . . ways consumers can avoid identity theft and what they can do if they are victims."[91] Providing similar pamphlets to its customers is likely an added expense that small businesses simply may not be able to afford.[92] One bank uses "a confidential trash vendor that provides special bins for documents that contain customer information"[93] as a way of disposing its sensitive documents. For a small business to do its own destruction of such documents, it can cost "about $15 to $250 for a personal shredder to nearly $2,000 for one for an office."[94]

Financial institutions have another resource. "Due in large part to the rash of identity-theft cases involving financial powerhouses such as Bank of America, Ameritrade and ChoicePoint, the financial industry has banded together to provide shared data on all cases of identity theft to the Federal Trade Commission."[95] Now, not only do individual institutions have the time and money to combat identity theft, they also have access to additional information to make security easier and more effective.[96] Unfortunately, the same cannot be said for small businesses that must fend for themselves.[97]

Financial institutions are not the only entities with extra resources. Corporations and larger businesses also are in a better

89. Press Release, Better Bus. Bureau, *supra* note 53.

90. *Id.*

91. Leslie Zganjar, *Banks Are Trying to Help Rub Out Identity Theft*, BIRMINGHAM BUS. J., Nov. 16, 2001, http://www.bizjournals.com/birmingham/stories/2001/11/19/story4.html.

92. *SBA Sponsors Identity Theft Seminars for Small Businesses Throughout Massachusetts in April, May & June*, *supra* note 9.

93. Zganjar, *supra* note 91.

94. Fetterman, *supra* note 69.

95. Karen D. Schwartz, *Financial Institutions to Share Identity-Theft Data*, EWEEK.COM, July 6, 2005, http://www.eweek.com/article2/0,1759,1834487,00.asp?kc=EWNKT0209KTX1K0100440.

96. *Id.*

97. *See id.*

position to combat identity theft than their smaller counterparts.[98] Many large businesses have privacy policies that contain almost the same words: "We have appropriate physical, electronic and procedural security safeguards to protect and secure the information we collect."[99] These promises involve costs in terms of time and money in creating the policies and implementing them.[100] In addition, many businesses employ costly methods to protect personal information, such as Target's "Secure Sockets Layering."[101] Few small businesses are able to afford the costs associated with these security measures or even have the knowledge of when and how to use them.[102]

B. *The Impact of Identity Theft on Electronic Commerce/Online Retailers*

"Electronic commerce is the business of buying and selling products, information, or services in an Internet based environment. Unlike traditional face-to-face transactions, e-commerce shoppers and merchants communicate through a public computer network."[103] Because online merchants conduct business mostly through the Internet, the databases they compile are extremely valuable to an identity thief and potentially easier to access than the information stored by a

98. Kershaw-Staley, *supra* note 46.

99. Target, Online Privacy Policy, http://target.com/target_group/legal/privacy-policy.jhtml?_request=10427722 (last visited Jan. 23, 2006); *see also* Nordstrom, Nordstrom Privacy, http://www.nordstrom.com (last visited Jan. 23, 2006) ("We maintain physical, electronic and procedural safeguards to protect the confidentiality and security of personally identifiable information transmitted to us using this website."); Food Lion, Privacy Statement, http://www.foodlion.com/PrivacyStatement.asp (last visited Jan. 23, 2006) ("Rest assured that we have put into place physical, electronic and managerial procedures to prevent unauthorized access, maintain data accuracy, ensure the correct use of information and safeguard and secure the information we collect about you.").

100. *See* Kershaw-Staley, *supra* note 46 ("[C]onsumers have a right to be notified if their information is violated, regardless of the cost to the business.").

101. Target, *supra* note 99. Secure Sockets Layering (SSL) is "a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers." WEBOPEDIA: ONLINE COMPUTER DICTIONARY FOR COMPUTER AND INTERNET TERMS AND DEFINITIONS, http://webopedia.internet.com/TERM/S/SSL.html (last visited Jan. 23, 2006).

102. *See* Kershaw-Staley, *supra* note 46.

103. MASTERCARD INT'L INC., *supra* note 44 at 1-1.

conventional retailer.[104] Furthermore, "the absence of direct physical contact between transacting parties makes it easier to use stolen data to impersonate an individual."[105]

Financial institutions are also well-aware of the added risks online retailers face: one survey indicated that "fraud across participating merchants reached 1.7 percent of online sales in 2003, over 28 times higher than in the brick-and-mortar world." [106] Accordingly, the rules governing identity theft are sometimes different from those applying to other small business owners.[107]

> When a crook uses a stolen credit card in a traditional store, and the store follows proper procedures, the card-issuing bank usually swallows the loss. For online retailers, the tables are turned. Credit-card association rules dictate that merchants who accept charges from cyberspace, a riskier endeavor, must also shoulder the risk of fraud.[108]

The explanation for the difference in treatment between online business owners and traditional business owners accepting credit cards comes down to authentication.[109] Authentication, "a critical element in the credit card authorization process, implies that the merchant has obtained a piece of verifiable private information," which in face-to-face cases usually involves comparing the signature on the back of the card to the one on the receipt.[110]

Alternatively, authentication for transactions taking place over the Internet "is far more difficult," and therefore, "[u]nder bank card association rules, such transactions are placed in the 'unauthenticated' category."[111] Thus, the general rule, unless the parties have contracted

---

104. *Id.*

105. Julia S. Cheney, *Identity Theft: A Pernicious and Costly Fraud* 6 (Payment Cards Center of the Fed. Res. Bank of Philadelphia, Discussion Paper, Dec. 2003), *available at* http://www.phil.frb.org/pcc/papers/Identity_Theft.pdf.

106. *Id.* at 7.

107. *See eg.*, MASTERCARD INT'L INC., *supra* note 44, at 1-1.

108. Pacelle, *supra* note 78.

109. Cheney, *supra* note 105, at 8.

110. *Id.*

111. *Id.*

otherwise, is that "the issuer assumes the risk associated with authenticated transactions while the merchant assumes fraud risk associated with unauthenticated transactions."[112]

It would therefore appear that online retailers, as a subsection of small business owners, are in the worst position in regard to identity theft once it has occurred.[113] Arguably, the difference in treatment of e-commerce can also be an incentive to take greater preventative measures.[114] Of course, preventative measures themselves can be costly and not always effective.

For example, Neil Kugelman, an online retailer, took far more precautions than most and was still left with $8,432 in fraudulent charges.[115] Mr. Kugelman's attention was first drawn to a customer who placed two large orders for jewelry back-to-back.[116] He called the financial institution that had issued the card when he was suspicious of a strange order, but was assured that "the name, address, and phone number on the order matched the bank's own account information, except for one small detail about the address."[117] "Mr. Kugelman then called the customer, who explained the discrepancy to his satisfaction."[118] He then checked that the credit card limit had not been exceeded, and then filled the order.[119]

Despite Mr. Kugelman's efforts, the identity thief was able to deceive him.[120] The victim was unaware that someone had stolen her identity and so it was not until months later that Mr. Kugelman was informed that the orders were fraudulent.[121] By this time the perpetrator was probably gone without a trace, and so it fell to Mr. Kugelman or the

112. *Id.* at 9.

113. *See* Pacelle, *supra* note 78.

114. MASTERCARD INT'L INC., *supra* note 44 at 1-1 ("To encourage the adoption of security measures online, MasterCard has expanded the concept and developed the MasterCard Site Data Protection Program.").

115. Pacelle, *supra* note 78.

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

120. Pacelle, *supra* note 78.

121. *Id.*

financial institution to repair the damages.[122] At arbitration, it was determined that Mr. Kugelman "would have to eat the loss."[123]

Even though the victim of the identity theft was ultimately reimbursed by the online retailer, as a result of such incidents potential customers may be deterred from online shopping, especially because of possible security breaches.[124] According to Fran Maier, executive director of TRUSTe, "[t]he Internet was supposed to be the great equalizer - allowing small to compete with big. Yet this vision will never be realized as long as consumers are uncomfortable purchasing from e-tailers that don't put an emphasis on privacy."[125] E-commerce is quickly becoming a race to the top; retailers are faced with taking every available measure to satisfy consumers.[126] Accordingly, consumer purchases reflect this potential lack of security.[127] In fact, results of a survey relating to consumer privacy reveal that "forty-nine percent of survey respondents indicated that fears related to the misuse of personal information will limit their holiday online shopping to some extent."[128]

This may appear to be unfair to Mr. Kugelman, and other online small business owners like him, who tried to do everything he could to prevent such a disaster from occurring, but one might argue that this is the added cost of benefiting from an unregulated venue.[129] Regardless of any potential benefits, the costs may soon completely outweigh them: as Maier points out, "[t]he results of this survey reveal that privacy fears will be the Grinch that stole Christmas for many e-tailers."[130] Consumers' fears will mirror the growth of identity theft crimes.[131] Given that many online shoppers "were less willing to purchase items from a smaller online retailer than a large well-known brand," there

122. *See infra* notes 141-145 and accompanying text.

123. Pacelle, *supra* note 78.

124. *Identity Theft and Spam Will Deter Online Shopping This Holiday Season*, *supra* note 40.

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

129. *See* Pacelle, *supra* note 78.

130. *Identity Theft and Spam Will Deter Online Shopping This Holiday Season*, *supra* note 40.

131. *Id.* ("A survey conducted by market research firm NFO WorldGroup and sponsored by the nonprofit TRUSTe reveals that fears related to consumer privacy will have a significant negative impact on online shopping during the 2003 holiday season.").

may be a steady decline of online small businesses unless another option is elected for bearing the burden of identity theft.[132]

IV. ALTERNATIVE RISK OF LOSS ALLOCATIONS

A. Placing the Risk of Loss on the Perpetrator

The most satisfying option from the perspective of justice and fairness is to penalize the identity thief: "The bill I'm about to sign sends a clear message that a person who violates another's financial privacy will be punished."[133] President Bush spoke these words when he signed the Identity Theft Penalty Enhancement Act (the Enhancement Act) in 2004 and they indicate a sentiment, felt by many, that the law needs to take a harder line against identity thieves.[134] It was precisely this attitude that led to the creation of the Enhancement Act.[135] Prior to this Act, the Identity Theft and Assumption Deterrence Act[136] was the only law specifically addressing federal criminal punishment for identity theft. It made some strides, but "[p]rosecutors across the country report[ed] that sentences for these crimes [did] not reflect the damage done to the victim."[137]

With the Enhancement Act, the government hopes to send an even stronger message to criminals.[138] As the President said at the signing of the Enhancement Act,

> [t]oo often, those convicted have been sentenced too little or no time in prison. This changes today. This new law establishes in the Federal criminal court the offense of aggravated identity theft. And someone convicted of that crime can expect to go to jail for stealing a person's good name.[139]

---

132. *Id.*

133. Remarks on Signing the Identity Theft Penalty Enhancement Act, *supra* note 57.

134. *Id.*

135. 18 U.S.C. § 1028A (2005); *see* Remarks on Signing the Identity Theft Penalty Enhancement Act, *supra* note 57.

136. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998).

137. Remarks on Signing the Identity Theft Penalty Enhancement Act, *supra* note 57.

138. *Id.*

139. *Id.*

This highly optimistic stance may make some cardholders more comfortable, but only so long as capturing and prosecuting the identity thief is a realistic possibility.[140]

"The biggest problem is that law enforcement agencies lack the resources to investigate and prosecute identity thieves."[141] In fact, it is highly unlikely that an identity thief will be arrested.[142] If it is nearly impossible to catch an identity thief, the perpetrator will go unpunished, and someone else will be left to assume the loss.[143] Moreover, even if a thief is found, he may be judgment proof.[144] The Enhancement Act is silent as to restitution.[145] Presumably, the thief will need to be sued civilly for damages or one of the other players will assume the loss. This could include: the financial institution, the cardholder, the small business or an insurance company.

B. Placing the Risk of Loss on the Financial Institutions

If the identity theft has occurred because the thief was able to obtain personal information by breaching the security system of a financial institution, "[y]et another possible way for identity theft victims to seek relief for damages would be under the [Gramm Leach Bliley Act (GLBA)]."[146] The GLBA requires that financial institutions implement certain security measures, such as providing notice to customers before disclosing personal information, limitations on the sharing of account numbers, and limits on the reuse of information.[147] "[H]arm resulting from the violation of the [GLBA] could be seen as negligence per se."[148] The argument is that the financial institution, a storehouse of personal information, is in the best position to secure that

140. Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 MARQ. L. REV. 847, 866 (2005).

141. *Id.* at 857.

142. *Id.*

143. *Id.*

144. *Id.* ("Even if the identity thief is arrested, restitution is not always possible or required.").

145. 18 U.S.C. § 1028A (2005).

146. White, *supra* note 140, at 865.

147. 15 U.S.C. §§ 6801-6802 (2005).

148. White, *supra* note 150, at 865.

information.[149] Fear of such suits would theoretically provide an incentive for "financial institutions to either comply with the [GLBA] or to face potential liability if an actual security breach occurs."[150]

This alternative is problematic for several reasons. First, it may be difficult to prove that the financial institution indeed did not take the proper precautions.[151] Given the stakes that they face, it is likely that powerful institutions have spent at least a portion of their resources in protecting themselves and their customers.[152] It simply would be devastating to institutions who took unnecessary risks with their customers' information.[153] In fact, even with standard measures, "banks lost at least $1 billion to identity thieves last year," who took out home loans and credit cards in another's name.[154] As the director of government relations for the Alabama Bankers Association, put it, "It's in everyone's best interest to cut this crime out."[155]

Another reason for not burdening financial institutions is that they "pass their losses from identity theft onto consumers through higher interest rates and annual fees."[156] Many customers, especially those that have never felt the effects of identity theft, are not willing to pay the financial institution for added precautions.[157] If this is the case, financial institutions may lose a competitive edge by charging higher fees for more security.[158]

If, on the other hand, the theft did not take place because of a breach in the financial institution's security, but through some other

149. *See id.* at 859 ("This remedy is based on the premise that financial institutions are required to keep customer information confidential, unless authorization to disclose is given by the customer.").

150. *Id.* at 865.

151. *See infra* notes 152-155 and accompanying text.

152. *See* Zganjar, *supra* note 91 ("Banks are including in the monthly statements they send customers pamphlets explaining how the new law works, ways consumers can avoid identity theft and what they can do if they are victims.").

153. *See id.*

154. Bob Sullivan, *ID Theft Costs Banks $1 Billion a Year: Report: There's No Way to Positively Identify New Customers*, March 26, 2003, http://msnbc.msn.com/id/3078480.

155. Zganjar, *supra* note 91.

156. Maria Ramirez-Palafox, *Review of Selected 1997 California Legislation: Identity Theft on the Rise: Will the Real John Doe Please Step Forward?*, 29 MCGEORGE L. REV. 483, 488 (1998).

157. *See* Sullivan, *supra* note 154 ("Almost no one thinks the consumer is willing to give up much of anything to prevent ID theft.").

158. *See id.* ("And there are not a lot of easy ways to tighten up controls without putting yourself at a competitive disadvantage.").

means, such as "dumpster diving," the financial institution may still cover the losses.[159] Many institutions promote programs like Visa's "Zero Liability," whose policy "virtually eliminates consumer liability in cases of card fraud for all Visa card transactions processed through the Visa network."[160] Providing customers with added safety translates to increased profits for Visa.[161]

Thus, it would seem fair that the entity which stands to gain the most also bears the greatest burden. However, the concept of burdening the financial institution that did not commit the fraud, rather than the perpetrator, is troubling.[162] Additionally, a cardholder may not always be certain that the financial institution will cover the losses.[163] "Financial institutions may impose greater liability on the cardholder if the financial institution reasonably determines that the unauthorized transaction was caused by the gross negligence or fraudulent action of the cardholder," which can include something as simple as delays in reporting unauthorized transactions.[164]

C. *Placing the Risk of Loss on the Cardholder*

"Historically banks, like other credit card issuers, have attempted to allocate such fraud losses by contractual provisions in the

159. *See* Visa USA, *supra* note 59 ("Visa's Zero Liability policy means 100 percent protections for you. Visa's enhanced policy guarantees maximum protections against fraud. You now have complete liability protection for all of your card transactions that take place on the Visa system. Should someone steal your card number while you're shopping, online or off, you pay nothing for their fraudulent activity.").

160. Visa USA, *Operation & Risk Management: Zero Liability*, http://usa.visa.com /business/accepting_visa/ops_risk_management/zero_liability.html (last visited Jan. 23, 2006).

161. *See id.* ("By making customers feel more secure, Zero Liability helps increase card transactions, driving sales for participating merchants.").

162. *But see* Remarks on Signing the Identity Theft Penalty Enhancement Act, *supra* note 57 ("This law [Enhancement Act] also raises the standard of conduct for people who have access to personal records through their work at banks, government agencies, insurance companies, and other storehouses of financial data. The law directs the United States Sentencing Commission to make sure those convicted of abusing and stealing from their customers serve a sentence equal to their crimes.").

163. *See* Visa USA, *supra* note 59 ("Visa's Zero Liability policy took effect April 4, 2000, and is a great improvement on the previous policy. The former policy required that you report fraudulent activity within two business days of discovery. After this two-day period, you could be held responsible for up to $50 of the unauthorized charges.").

164. *Id.*

issuer-cardholder agreement."[165] Whether courts will always accept the contractual provisions is another matter.[166] There does appear to be a distinction between negligent and non-negligent cardholders for the purposes of liability.[167] For example, "a credit cardholder who permits use of the card by another for a specific purpose is liable for other uses not specifically authorized."[168] On the other hand, courts have been far more likely to find in favor of the consumer when there has been no negligence on his part, as in most cases of identity theft.[169] In *Rayor v. Affiliated Credit Bureau, Inc.*, an early case concerning identity theft, the Colorado Supreme Court exonerated the cardholders from liability for fraudulent purchases made by an unidentified thief.[170] Unfortunately, even with this distinction, holdings have been hard to predict.[171]

Consumers now rely more on statutes than case law.[172] One of the most important laws for consumers is the federal Consumer Credit Protection Act,[173] which "was amended to handle, in a comprehensive way, the problem of lost or stolen credit cards."[174] The Act makes a

---

165. BARKLEY CLARK & BARBARA CLARK, THE LAW OF BANK DEPOSITS, COLLECTIONS AND CREDIT CARDS ¶ 15.03 (A.S. Pratt & Sons 1970) (Vol. 2 2005).

166. *Id.*

167. *Id.*

168. Stieger v. Chevy Chase Sav. Bank, 666 A.2d 479, 481 (D.C. 1995) (holding that cardholder should bear financial responsibility for unauthorized charges made by his employee who had been given the card for a limited purpose); *see also* Walker Bank & Trust Co. v. Jones, 672 P.2d 73 (Utah 1983) (refusing to limit the liability of a cardholder for her estranged husband's charges because he had "apparent authority" to continue the use of the card "because he had previously been issued a card and his name had appeared on it.").

169. *See* CLARK & CLARK, *supra* note 165, at ¶ 15.03.

170. Rayor v. Affiliated Credit Bureau, Inc., 455 P.2d 859, 860 (Colo. 1969) ("We simply hold that the court erred in ruling that, under the facts and in the absence of any contractual obligation, the defendants were liable for unauthorized purchases made prior to the time they gave notification that the card was lost or stolen. In the absence of other factors (such as negligence, bad faith or estoppel) which are not involved here, such a liability must be predicated upon a contractual obligation.").

171. CLARK & CLARK, *supra* note 165, at ¶ 15.03 [1] ("One New York court went so far as to hold a notice clause incapable of shifting the fraud loss to a cardholder who did not know that her card had been stolen. On the other hand, some courts enforced the notice clauses without reservation."); *see* Allied Stores v. Funderburke, 52 Misc. 2d 872 (Civ. Ct. 1967). *But see* Uni-Serv Corp. v. Vitiello, 53 Misc. 2d 396 (Civ. Ct. 1967) (enforcing notice clauses without reservation).

172. *See id.* at ¶ 15.03.

173. 15 U.S.C. § 1643 (2005).

174. CLARK & CLARK, *supra* note 165, at ¶ 15.03 [2][a].

cardholder liable for unauthorized use of his card only if:

> (A) the card is an accepted card; (B) the liability is not in excess of $50; (C) the card issuer gives adequate notice to the cardholder of the potential liability; (D) the card issuer has provided the cardholder with a description of a means by which the card issuer may be notified of loss or theft of the card...; (E) the unauthorized use occurs before the card issuer has been notified that an unauthorized use of the credit card has occurred or may occur as the result of loss, theft, or otherwise; and (F) the card issuer has provided a method whereby the user of such card can be identified as the person authorized to use it.[175]

Moreover, the subsequent case law has indicated that despite the intended limit of $50 per card, "the federal statute may have generally eliminated cardholder liability for unauthorized use." [176] After examining this statute, and other pro-consumer laws, it appears that the government is not likely to place the loss from identity theft on an innocent and unaware victim.[177]

D. *Insuring Against the Risk of Loss*

Some insurance companies, such as Allstate, provide insurance to consumers to cover the costs associated with identity theft including attorney fees, lost wages, loan reapplication fees, and other expenses.[178] The Allstate product is called "identity restoration coverage."[179]

---

175. 15 U.S.C. § 1643 (2005).

176. CLARK & CLARK, *supra* note 165, at ¶ 15.03 [2][a].

177. *Federal & State Laws*, FED. TRADE COMM'N, http://www.consumer.gov/idtheft/law_laws.htm (last visited Jan. 23, 2006). Pro-consumer statutes include the Fair Credit Reporting Act, establishing procedures for correcting credit card records, the Fair Credit Billing Act, limiting consumer's liability, the Fair Debt Collection Practices Act, preventing debt collectors from using unfair or deceptive practices, and the Gramm-Leach-Bliley Act, ensuring that "financial institutions protect the privacy of consumers' personal financial information." *Id.*

178. Allstate, *Introducing Allstate's New Identity Restoration Coverage,* http://www.allstate.com/landingpages/home/idtheft.aspx (last visited Jan. 23, 2006).

179. *Id.*

Allstate promises to provide customers with "a dedicated team to handle the complicated, time-consuming and tedious work" needed to restore one's financial reputation.[180] Customers "may also be reimbursed up to $25,000 per premium period."[181]

Allstate charges "about $40 a year" for identity restoration coverage; this amount appears to be relatively modest given what is at stake and what stands to be saved.[182] Employers may wish to consider providing and paying for this coverage for their employees; this would save even larger costs from the lost productivity from identity theft victims spending many hours to clear their names.[183]

Identity theft insurance is the best method for allocating the risk of loss from identity theft in the likely event that the perpetrator cannot be found or successfully prosecuted.[184] Those willing to take the risk of having a credit card can protect themselves, rather than burdening an innocent participant in the economic process.[185] If consumers remain uninsured, it may be in the small business's best interest to purchase insurance.[186] It would then be easier to justify forcing the small business to bear the loss if it did not purchase insurance.[187] Especially for online retailers, the incentive would be strong.[188] Then when an identity thief strikes, the insurance agency will be there to pick up the pieces.[189]

Nevertheless, there are those who are a little cynical when it comes to the insurer's role.[190] Some fear that "insurers are capitalizing more on fear than facts."[191] Furthermore, when identity theft does

180. *Id.* Allstate offers to "make the phone calls, handle the paperwork and deal with the credit bureaus." *Id.*

181. *Id.*

182. *Id.*

183. Stephanie Armour, *Some Employers Offer ID Theft Coverage*, USA TODAY, Sept. 11, 2005, at 1B, *available at* http://www.usatoday.com/money/workplace/2005-09-11-id-theft-benefit_x.htm.

184. *See infra* notes 185-189 and accompanying text.

185. Bruce Mohl, *Providers Push Insurance Covering Theft of Identity*, THE BOSTON GLOBE, Feb. 6, 2005, http://www.boston.com/business/articles/2005/02/06/providerspush_insurance_covering_theft_of_identity/.

186. *Id.*

187. *Id.*

188. *See* Pacelle, *supra* note 78.

189. *See, eg.*, Allstate, *supra* note 178.

190. *See* Mohl, *supra* note 185.

191. *Id.*

occur, the types of expenses covered, such as loan reapplication fees, notary, phone, and mailing costs, "rarely add up to much."[192] Despite having its critics, many say this product has universal appeal and that this is exactly "the sort of problem insurance is meant to cover."[193]

V. CONCLUSION

While the cardholder and financial institution are not favorable candidates for bearing the burden of identity theft, the small business for the reasons discussed in Part IV, is the least viable option.[194] The lack of time, money, employees, and other resources put small businesses in the worst position to combat this devious crime.[195] Small businesses should not be excused from doing their fair share to combat identity theft, but when the damage has been done, efforts should be made to explore other options before burdening a small business that will truly suffer as a result.[196]

The most promising of these other options is currently identity theft insurance.[197] While it is questionable whether a particular policy would cover all of the losses incurred, the cost is minimal and the peace of mind may be well worth it.[198] If nothing else, insurance is a resource for knowing how to begin recovering financially after identity theft has occurred. As a spokesman for Identity Theft 911, counseling services, said, "If you're not experienced in this area, it can be a vast time sink. You're constantly wondering what else I need to do."[199] Thus, while "buyer beware" still rings true, identity theft insurance is a far fairer

192. *Id.* ("To recover the actual dollars stolen from a savings account or avoiding paying bills or credit card charges rung up by a thief, consumers are mostly on their own.").

193. *Id.*

194. *See supra* Part IV.A-C.

195. *See supra* notes 69-102 and accompanying text.

196. *See supra* Part IV.

197. *See supra* Part IV.D.

198. *See supra* notes 190-193 and accompanying text.

199. Mohl, *supra* note 185.

alternative than many others, especially as compared to burdening small businesses who do not agree to the risk as willingly as insurers who are at least receiving premium payments in return.[200]

PENELOPE N. LAZAROU

200. *See supra* notes 184-189 and accompanying text.