UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
CENTER FOR CLINICAL EDUCATION

CLINICAL PROFESSOR AND DIRECTOR
Deirdre Mulligan
(510) 642-0499
dmulligan@law.berkeley.edu

SCHOOL OF LAW (BOALT HALL)
BERKELEY, CALIFORNIA 94720-7200
TELEPHONE (510) 643-4800
FAX (510) 643-4625
http://www.law.berkeley.edu/academics/samuelson/

[SUBMITTED ELECTRONICALLY VIA https://secure.commentworks.com/ftc-SSNPrivateSector/]

Federal Trade Commission/Office of the Secretary
Room H-135 (Annex K)
600 Pennsylvania Avenue, NW
Washington, DC 20580.

Comments of the Samuelson Law, Technology & Public Policy Clinic to the Federal Trade Commission on SSNs In The Private Sector - Comment, Project No. P075414

September 5, 2007

Introduction

Thank you for soliciting comments on the collection and use of the Social Security number (SSN) in the private sector.

The Commission's guidance to consumers on avoiding identity theft includes this advice:

> *Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.*[1]

Mounting evidence suggests that some credit grantors engage in the practice warned against in the Commission's identity theft materials, albeit with the full SSN: they use the SSN as a password in verifying an individual's identity.

This practice is irresponsible and makes identity theft a simple crime to commit. The SSN is already used as a record locator by credit grantors and consumer reporting agencies. And therefore, businesses engaging in this practice are not only using the same

[1] FEDERAL TRADE COMMISSION, FACTS FOR CONSUMERS, May 2006, available at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.shtm

identifier for both identification and authentication, they are using an obvious one to do so.

Additionally, other data provided on credit applications, such as name and address, are being ignored by some grantors, making identity theft trivially simple to commit. As more fully explained below, the development of "synthetic identity theft" documents these troubling identification/authentication schemes, and suggests that simple changes in authentication practices could reduce incidence of identity theft. That is, rather than adopting expensive and more invasive authentication mechanisms to prevent identity theft, the Commission should first explore the efficacy of simple steps, such as matching the SSN to basic identifiers, including the name, address, and other data currently present on credit headers.

Comments

Our comments below on lax authentication practices and synthetic identity theft focus on the following topics specified by the Commission:

2. The Role of the SSN as an Authenticator

- *The use of the SSN as an authenticator – as proof that consumers are who they say they are – is widely viewed as exacerbating the risk of identity theft. What are the circumstances in which the SSN is used as an authenticator?*
- *Are SSNs so widely available that they should never be used as an authenticator?*

4. The Role of the SSN in Fraud Prevention

- *Many segments of the private sector use the SSN for fraud prevention, or, in other words, to prevent identity theft. How is the SSN used in fraud prevention?*

5. The Role of the SSN in Identity Theft

- *Which private sector uses of the SSN do thieves exploit to obtain SSNs, i.e, SSN as identifier or SSN as an authenticator? Which of those uses are most vulnerable to identity thieves?*
- *Once thieves obtain SSNs, how do they use them to commit identity theft? What types of identity theft are thieves able to commit with the SSN? Do thieves need other information in conjunction with the SSN to commit identity theft? If so, what other kinds of information must they have?*
- *Where alternatives to the SSN are available, what kind of identity theft risks do they present, if any?*

Many companies use the SSN both to identify an individual when an account is established, and later as an authenticator or password to access the same account. Wireless phone companies, for instance, commonly used this scheme to secure customer records. The practice made pretexting for phone records trivially easy, as private

investigators have access to databases of SSNs that could be used to satisfy the carriers' authentication systems.

In our comment, we focus on a different, but similar practice: one where credit grantors use the SSN both to identify an applicant and to authenticate the applicant, sometimes in combination with the date of birth.[2] This practice makes identity theft trivially easy. All a thief needs to do is make an application with a SSN of another and a date of birth that is consistent with the SSN's issuance.[3]

A series of lawsuits against credit issuers for negligence in opening new accounts to impostors shows a pattern of such authentication practices. These practices result in approved applications where there is a SSN match, even where other information on the application is obviously wrong. This reliance on the SSN as identifier and authenticator allows even unsophisticated individuals who have little personal information of another person to obtain credit accounts. For instance, in *Wolfe v. MBNA America Bank*, the plaintiff alleged that MBNA issued a credit card to an impostor without verifying any of the application information:

> *...Limited discovery has shown that an MBNA-hired "telemarketer" supplied MBNA an "application" in Plaintiff's name, replete with critical false, missing, and incomplete information (wrong address, wrong phone number, "nearest relative" who was not near or a relative, and a host of blank lines on its forms). MBNA had no signature and turned a blind eye to red flags: a 21 year-old college kid supposedly earned $55,000 annually, but no employer's name was listed. Before suit was filed, MBNA's [sic] internally documented the reality: "Nothing was verified."*[4]

In that case, MBNA America Bank argued that the law imposed no duty to verify the identities of customers or non-customers.[5] This raises an obvious question: if the issuer believes it has no duty to verify applicants, but nevertheless does so using widely-

---

[2] It is possible that other information from credit applications, such as name and address, are used in the authentication process, but they are weighted in such a way that errors still result in new accounts being issued to impostors.

[3] Free, publicly-available databases explain the relationship between SSNs and their issuance dates. See, e.g. COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, STRUCTURE OF SOCIAL SECURITY NUMBERS, May 15, 2001, available at http://www.cpsr.org/prevsite/cpsr/privacy/ssn/ssn.structure.html; SOCIAL SECURITY ADMINISTRATION, HIGH GROUP LIST AND OTHER WAYS TO DETERMINE IF AN SSN IS VALID, Aug. 16, 2007, available at http://www.socialsecurity.gov/employer/ssnvhighgroup.htm.

[4] 485 F. Supp. 2d 874 (WD. Tenn. 2007)(quoting Plaintiff's Response in Opposition to Defendant MBNA's Motion to Dismiss Fourth Amendment Complaint)(attached).

[5] Defendant MBNA America Bank's Memorandum of Law in Support of its Motion to Dismiss Plaintiff's Third Amended Complaint for Failure to State a Claim for Which Relief May Be Granted at 7-8.

available personal information, how can one insulate oneself from identity theft, short of obtaining a credit freeze? The court acknowledged that credit issuers, "have become the first, and often last, line of defense in preventing the devastating damage that identity theft inflicts. Because the injury resulting from the negligent issuance of a credit card is foreseeable and preventable…under Tennessee negligence law, Defendant has a duty to verify the authenticity and accuracy of a credit account application."[6] Thus, the court allowed a negligence claim to proceed against MBNA for exposing the Plaintiff to identity theft through lax authentication practices.

In other cases, a similar set of facts are alleged pointing to lax identity verification practices. For instance, in *Vazquez-Garcia v. Trans Union De P.R., Inc*., an impostor successfully obtained credit with a SSN that matched the victim's but an incorrect date of birth and an address thousands of miles away from the victim.[7] In *United States v. Peyton*, impostors obtained six American Express cards using the correct name and SSN of victims but directed all six to be sent to the impostors' home.[8] In *Aylward v. Fleet Bank*, a bank issued two credit cards based on matching name and SSN but incorrect address.[9] Finally, in *Dimezza v. First USA Bank*, Inc., an impostor obtained credit with a matching SSN but incorrect address.[10]

Credit granting practices that rely excessively upon the SSN have given rise to the problem of "synthetic identity theft," a form of new account fraud where the impostor creates a new identity. The new identity is comprised of some information from a real person, which the thief enhances with fabricated personal information.[11] For example, the impostor may use a real SSN, but a falsified name and address. A synthetic identity based on some real information, and sometimes supplemented with artfully created credit histories, can then be used to apply for new credit accounts.

The synthetic identity theft problem is not well elucidated, and is only discussed in detail in a handful of newspaper articles and industry white papers.[12] For instance, the Salt Lake Tribune outlined the problem in June 2004:

---

[6] 485 F. Supp 2d at 882.
[7] 222 F. Supp. 2d 150 (D.P.R. 2002).
[8] 353 F.3d 1080 (9th Cir. 2003).
[9] 122 F.3d 616 (8th Cir. 1997).
[10] 103 F. Supp. 2d 1296 (D.N.M. 2000).
[11] FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (Dec. 14, 2004), available at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html; FRED H. CATE, INFORMATION SECURITY BREACHES AND THE THREAT TO CONSUMERS (2005), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf.
[12] *See e.g.* IDANALYTICS, NATIONAL FRAUD RING ANALYSIS, UNDERSTANDING BEHAVIORAL PATTERNS, Feb. 2005.

> *Making purchases on credit using your own name and someone else's Social Security number may sound difficult -- even impossible -- given the level of sophistication of the nation's financial services industry…But investigators say it is happening with alarming frequency because businesses granting credit do little to ensure names and Social Security numbers match and credit bureaus allow perpetrators to establish credit files using other people's Social Security numbers."*[13]

The same article reports that Ron Ingleby, resident agent in charge of Utah, Montana and Wyoming for the Social Security Administration's Office of Inspector General, as stating that SSN-only fraud makes up the majority of cases of identity theft.[14] Other initial indications suggest that it is a growing problem. According to Mike Cook of ID Analytics, a company that specializes in the reduction of fraud risk, synthetic identity fraud "is a larger problem than [standard new account] identity theft and is growing at a faster rate."[15]

A sophisticated example of the crime is illustrated by a case brought by the U.S. Attorney for the District of Arizona in August 2006.[16] The indictment charges two men with a variety of federal crimes for allegedly using real SSNs from credit reports and fabricated names to apply for credit cards.[17] One of the defendants owned a small consumer reporting agency, and apparently has a high level of sophistication in credit practices.[18] The pair established credit histories for synthetic identities by reporting favorable payment information to consumer reporting agencies. These reports made the synthetic identities appear to be real people with a record of paying bills. The defendants then allegedly obtained 250 credit cards from fifteen banks, and charged $760,000 to these synthetic identities.[19]

These cases suggest that simple changes in authentication practices could reduce incidence of identity theft. That is, rather than adopting expensive and more invasive authentication mechanisms, the Commission should explore simple steps, such as

---

[13] Lesley Mitchell, *New wrinkle in ID theft; Thieves pair your SS number with their name, buy with credit, never get caught; Social Security numbers a new tool for thieves*, The Salt Lake Tribune, June 6, 2004, at E1

[14] *Id*.

[15] Mike Cook, *The Lowdown on Fraud Rings*, 10 COLLECTIONS & CREDIT RISK 6 (2005), *available at* http://www.idanalytics.com/pdf/CCRAugust05MikeCook.pdf.

[16] William Carlile, *Two Indicted in Credit-Card Scheme That Used SSNs From Credit Reports*, 5 PRIVACY & SECURITY L.REP. 1257 (2006); Donald G. Aplin, Privacy, *Security Protection Will Remain Key Part of FTC's Agenda, Majoras Says*, 5 PRIVACY & SECURITY L. REP. 1552 (2006).

[17] United States v. Rose, CR06-0787PHK-JAT (VAM) (D. Az. 2006), *indictment filed* Aug. 22, 2006 (attached).

[18] *Rose*, Indictment at 2.

[19] *Rose*, Indictment at 3-4.

matching the SSN to basic identifiers, including the name, address, and other data currently present on credit headers.

California has attempted to address identity theft by requiring certain credit grantors to comply with basic, but heightened authentication procedures. California Civil Code § 1785.14 requires credit grantors to actually match identifying information on the credit application to the header held at the consumer reporting agency. Credit cannot be granted unless three identifiers from the application match those on file at the credit bureau. The categories to be matched include "first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number." These procedures are only required in situations where an individual applies for credit at a retailer.

While much of the information qualifying for matching purposes under the California law can be obtained through publicly-available sources, the ease with which impostors can obtain credit even with fabricated data suggests that a simple requirement to actually check applications could reduce the incidence of identity theft. This simple approach could be tested empirically without risk to consumers or the economy: the Commission could acquire a representative sample of successful fraudulent credit applications and analyze them for the presence of incorrect identifying information. Based on relative rates of error, the Commission could determine the minimum number of identifiers or combinations of identifiers that should match on an application before credit is granted.

Respectfully submitted,

/s

Chris Jay Hoofnagle
Senior Staff Attorney
Samuelson Law, Technology & Public Policy Clinic

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION AT MEMPHIS

MARK L. WOLFE,	)	
Plaintiff,	)	
	)	
v.	)	**No. 2:05-cv-02972-BBD-dkv**
	)	
MBNA AMERICAN BANK and	)	
NCO FINACIAL SYSTEMS, INC.,	)	
Defendants.	)	

PLAINTIFF MARK WOLFE'S RESPONSE IN OPPOSITION TO DEFENDANT MBNA'S MOTION TO DISMISS FOURTH AMENDED COMPLAINT

I. Introduction

This Court should deny Defendant MBNA's Motion to Dismiss Plaintiff's Fourth Amended Complaint. Plaintiff has previously responded to the arguments in Defendant's initial Motion to Dismiss and will endeavor not unduly to repeat them here.

II. Facts

Facts count.

Without Plaintiff's knowledge, MBNA recklessly, negligently or wrongfully issued a credit card in his name. Limited discovery has shown that an MBNA-hired "telemarketer" supplied MBNA an "application" in Plaintiff's name, replete with critical false, missing, and incomplete information (wrong address, wrong phone number, "nearest relative" who was not near or a relative, and a host of blank lines on its forms). MBNA had no signature and turned a blind eye to red flags: a 21year-old college kid supposedly earned $55,000 annually, but no employer's name was listed. Before suit was filed, MBNA's internally documented the reality: "**Nothing was verified.**"

MBNA allowed a third party to run up charges on the credit card, added late charges and "over-limit fees" totaling about $870, and sent correspondence to the phony address. Its own agents learned the phone number listed on the telemarketer's application was phony and knew there was no signature card or picture id. Yet, MBNA persisted in trying to collect the debt, but not from Plaintiff, tagged Plaintiff a deadbeat, sent the false information to a debt collector and credit reporting agencies,[1] knowing that others would rely upon it, and disadvantaged him in getting a job opportunity. Upon contacting MBNA to clear his name, MBNA could not be troubled.

Plaintiff's Fourth Amended Complaint declares that MBNA initiated acts that sullied his good name, and to this day, it still refuses to admit that it issued a card to the wrong individual or the foreseeable consequences of its own actions.[2] Defendant MBNA's reckless, negligent, and wrongful acts forced Plaintiff Mark Wolfe to traverse the netherworld of identity theft, and he still is trying to clear his name. Though Defendant MBNA has significantly resisted discovery or turning over many requested documents, it has admitted some facts or handed over some documents.

First, Defendant MBNA hired a telemarketer[3] of its own choosing [that it has yet to identify] presumably to obtain credit card applications from prospective customers, and in April 2000, received an application card in Plaintiff's name.[4] Neither MBNA nor

---

[1] The Fourth Amended Complaint alleges that Defendant knew that third parties would rely upon and see the false and erroneous credit information. It makes the incredulous claim in discovery that it has no knowledge about how credit reporting agencies use the information. *See* Fourth Amended Comp. ¶ 66; Exh. 8, MBNA's Response to Interrogatory No. 4.

[2] *See* Exh. 8, Defendant MBNA's Response to Interrogatory No. 1: "MBNA contends that Mark Wolfe … submitted a telemarketing application"; Defendant MBNA's Response to Interrogatory No. 9: "… it was a telemarketing account which, to MBNA's knowledge, was opened by Mark Wolfe."

[3] *See* Exh. 8, Defendant MBNA's Response to Interrogatory No. 5: "At this time, MBNA contends that Mark Wolfe was the applicant, based upon the **telemarketing application received by MBNA**" (emphasis added).

[4] *See* Fourth Amended Complaint, ¶ 5.

its telemarketer ever conversed, communicated, or dealt with Plaintiff Mark Wolfe. By definition, a "telemarketer" works by telephone.

Second, Defendant MBNA has no signature[5] from the Plaintiff or even anyone purporting to be him. It has no signature card – period.

Third, MBNA's internal document virtually admits that it relied upon dubious information and did not verify materially false, incomplete, and inaccurate facts in its "telemarketing application." MBNA's words were plain: "**Nothing** was **verified**."[6] The information contained within the "Customer Information System" confirms it. MBNA's notes entered April 10, 2000 include: The address verified since "4/2000, not verified"; and "phone number not verified, unpublished."[7] Tellingly, on April 12, 2000, MBNA's employees dialed the incorrect phone number listed on its telemarketer's application[8] as the Plaintiff; however, MBNA learned it was not Plaintiff's number and did not leave a message: the recording on the answering machine responded with a different name.[9]

Fourth, other critical information on its telemarketer's "application" – upon which it issued a credit card in Mr. Wolfe's name, is often just flat-out wrong, missing or incomplete, dubious, or on its face raises questions about its veracity and accuracy. MBNA ignored these red flags. Mr. Wolfe's address, phone number and date of birth are all listed incorrectly and wrongly; he never lived at the particular address or had that phone number. The application purports then to list the income of the "21" year old Mr. Wolfe, a college student, at $"55,000" per year, but no employer is listed and the "work"

---

[5] *See* Exh. 8, Defendant MBNA's Response to Interrogatory No. 9: "This was **not a signed application**; it was a **telemarketing account** … (emphasis supplied)." On the basis of that unsigned telemarketing application, Defendant MBNA incredibly continues to wrongly assert its untenable position: the account "… to MBNA's knowledge … was opened by Mark Wolfe."

[6] *See* Exh. 1, p. 2.

[7] *Id.* at p 1.

[8] *See* Exh. 2.

[9] *See* Exh. 1, p. 1.

phone and erroneous "home" phone numbers are identical, which phone numbers MBNA could not verify and should have known or knew were wrong[10] and never sent an invoice or any other information to Plaintiff at his real address.[11]

In addition, another notation directs that all activity on the account should be verified, but the notation stated that MBNA lacked a picture "id," which MBNA should have secured, but never did. Other material information is blank. The MBNA-produced form lists the item, "maiden name." Mr. Wolfe is a male. In context, the term is non-sensical; however, his Mother's maiden name differs from the one listed on the application. One MBNA report lists "nearest relative" and names a "Louis Johnson." Plaintiff has no relative named "Louis Johnson." *See* Exh. 4, Aff. Mark Wolfe.

Fifth, while it claims to have information from credit reporting agencies, the reports are thin and contain little information. For instance, an Experian report stated that Mr. Wolfe's "ISAAC score …[is] not available due to lack of credit history." It did however list Plaintiff's correct address, 532 W. Riveredge Drive, Cordova, TN 38018,[12] not the bogus address supplied by its telemarketer. Thus, MBNA actually had a document in its files listing Mr. Wolfe's correct address, but persisted in sending billings and correspondence to the wrong address and wrong person.

Sixth, Defendant MBNA expressly authorized charges, fees and expenses to be invoiced and added to this credit card account. After unauthorized charges piled up and totaled about $457.52 (to Phillips, Stride Rite, and Dillards about March, 2000), in succeeding months it then added "over credit line fees" and "late charge(s)." Altogether,

---

[10] *See* Exh. Ex. 1, a responsive document, which states that on April 10, 2000, "Phn … Tried the phn# ch actvd account from cld nt vrfy … cm up unpblshd."
[11] *See* Exh. 3.
[12] *See* Exh. 4.

it claimed that Mr. Wolfe owed it $864.88, which he did not and does not owe. Defendant MBNA willfully reported this false, derogatory information to various credit reporting agencies and NCO, a debt collector, knowing that it would subsequently and frequently be given to other firms and individuals, just as a potential employer did before denying Plaintiff a job.[13]

Seventh, in spite of its own documented concerns and knowledge, Defendant MBNA sent the account to NCO for collection.[14] Its notes reflect serious problems with the veracity or accuracy of the information in its possession and with good reason: it relied upon a telemarketer and its bogus, incomplete, or wrong information.

III. Plaintiff's Fourth Amended Complaint States a Claim for Relief, Confirmed by Facts Learned to Date

The Fourth Amended Complaint claims that MBNA's acts and practices constituted unfair or deceptive acts or practices in violation of the Tennessee Consumer Protection Act, T.C.A. § 47-18-101 *et seq.*, in particular 47-18-104 (Count 2, ¶¶ 37-45), Negligence (Count 2, ¶¶ 46-51B), Gross negligence or reckless conduct (Count 3, ¶¶ 46-53B), Libel (Count 4, ¶¶ 54-63A), damages, injuries, and losses (Count 5, ¶¶ 54-63A)4-67A), injunctive relief (Count 6, ¶¶ 68-69). The Complaint specifically pleads malice and reckless disregard, ¶ 36A and by relief seeks monetary damages, treble or special damages, attorney's fees, and injunctive relief requiring MBNA to clear Plaintiff's name.

Plaintiff has plainly pleaded allegations for each count:

First, Defendant MBNA's business in part is issuing credit cards, a business that it has voluntarily entered.

---

[13] Defendant has not admitted this fact, but it is alleged in the Fourth Amended Complaint.
[14] *See* Exh. 8, Response to Interrogatory No. 2 "… MBNA states that it sold this past due account to NCO Financial."

Second, Defendant chose to use a telemarketer – apparently without apology – to obtain credit card applications via telephone, an application that stated a 21 year old college kid incorrectly earned $55,000 per year, but failed to list any past or current employer.

Third, Defendant knew or learned that the phone numbers it had on file were wrong. At the time it issued the credit card, Defendant had in its files – obtained for the purpose of considering issuing a credit card, Plaintiff's correct address.

Fourth, the telemarketer's application was incomplete and had numerous blanks, contained material false information, and lacked a signature or a picture of the third party. MBNA knew that the phone number was wrong, admitting "Nothing was verified."

Fifth, MBNA issued a credit card, allowed charges and late fees to be rung up, knew or learned the information on the application was unreliable and raised questions about its veracity and accuracy, reported the bogus information about Plaintiff to credit reporting agencies realizing others would make use of it, and sent it to NCO, a debt collector. As a result, Plaintiff's name and reputation have been dragged through the mud.

Thus, Plaintiff has pleaded negligence, gross negligence, and/or recklessness **separately** or **together** –

(1) By relying upon a telemarketer and a telemarketer's application, by not having a signature or picture id, by knowing or it should have known that it had incomplete and false information, by having Plaintiff's correct address and not using it, Defendant MBNA issued a card that Plaintiff never authorized or knew about.

(2) By allowing charges, late fees, and other expenses to be piled on without Plaintiff's knowledge or consent and though it knew about the problems and issues with its own files regarding this account, Defendant acted irresponsibly and illegally to Mr. Wolfe's detriment.

(3) Even though Defendant MBNA specifically learned the truth or facts were learned and red flags raised that would lead a reasonable person to know of its horrible error and effects on Plaintiff Mark Wolfe, Defendant MBNA still referred the account to a debt collector, a third party.

(4) Defendant MBNA refused to correct the problem it alone created when Plaintiff learned about it or converse or deal with Plaintiff.

(5) Defendant MBNA refused to correct the false and disparaging information about Mr. Wolfe to all third parties who saw or received it, even though MBNA's own records reflected, "Nothing was verified."

Under Tennessee law, spreading falsehoods and lies about Mr. Wolfe to third parties, including NCO, constitutes libel. As to libel involving credit reporting firms, Plaintiff has alleged malice or reckless disregard.

Finally, these acts and practices affected trade or commerce in Tennessee, where Plaintiff lives. Third parties in Tennessee saw the false reports MBNA issued or caused to be issued, purchases were made on the card in Tennessee, and Plaintiff's reputation suffered mightily where he lives, namely in Tennessee.

IV. Legal Authorities and Argument

A. Federal Law Does Not Preempt Plaintiff's Claims

As it must, Defendant grudgingly seems to admit that Tennessee law governs. It spent the bulk of its argument arguing against application of settled principles of Tennessee law. The reason is clear: the federal law it relies upon does not touch upon a telemarketer or telemarketer's application for or the issuing a credit card, period. Moreover, the same federal law does not regulate either (i) authorizing charges or piling on late fees when a defendant bank knows or should know that it has wrongly permitted them, (ii) a Defendant bank's referring the account to a debt collector when it knew or should have known it fingered the wrong party, (iii) Defendant's refusing to correct its horrible errors when brought to its attention, or (iv) not correcting unambiguously the false information that it sent out about Plaintiff. The federal law covers certain disclosures to credit reporting firms, but does not preempt the field in its entirety or come close to doing so; however, some cases distinguishes between a firm that is a mere furnisher of information supplied by a third person and the actual creditor whose practices actually injured a citizen,[15] as MBNA did here to Mark Wolfe.

B. Tennessee Law Gives Plaintiff Powerful Remedies against MBNA

Plaintiff did nothing, nothing at all. Unbeknownst to him, Defendant MBNA issued a credit card based upon its own telemarketer's application, which was filled with incomplete, wrong, and false information, without getting any signature or picture id, let charges pile up, smeared his name, sent the matter to a debt collector, and buried its head in the sand when Plaintiff asked for its assistance to clear his name. This Fortune 500

[15] *See* Plaintiff's Response to Defendant's Initial Motion to Dismiss at 15-19; see generally *King v. Asset Acceptance, LLC,* 2006 WL 2714734 (N.D. Ga. Sept. 19, 2006) (attached as Exh. 6).

Defendant directly victimized Mark Wolfe. Though it produced meager records and answered relatively little by discovery, the facts unearthed to-date are astounding.

In their memoranda, Defendant has disregarded inconvenient Tennessee legal principles. It essentially asks this Court to divine and fashion a rule of civil immunity for banks, let them commit negligence, gross negligence, reckless behavior, libel, and other torts and violate consumer protection laws, and leave their victims high and dry. Neither the Tennessee Supreme Court nor the Tennessee legislature has created such an exemption, and this Court should deny Defendant's MBNA's invitation. To the contrary, the Tennessee Supreme Court and Tennessee intermediate appellate courts have decided cases involving banks for claims in negligence, tort and other causes of actions dating to the 19th Century. *See, e.g.*, *Union Bank v. Hicks*, 1843 WL 1865 (Tenn. 1843) (defaulted negligence claim against bank upheld) (attached as Exh. 6).

In addition, there are hundreds of reported cases in Tennessee naming or involving banks as parties in tort, negligence, gross negligence, and other causes of actions. Though they may involve a bank-to-customer relationship, under Tennessee law, banks may also be negligent to other persons. Contrary to Defendant's contention, there is no principle in reported Tennessee decisions that a bank cannot be negligent to non-customers. For example, a bank has faced or lost negligence or tort claims for failing to respond to a garnishment. *See, e.g.*, *NCNB Nat. Bank of North Carolina v. Thrailkill*, 856 S.W.2d 150 (Tenn. Ct. App. 1993). The question is not whether the person who obtained a garnishment against the bank is its customer, but whether the bank was negligent or failed to honor it. Similarly, banks have faced or been held liable for premises liability or slip and fall cases. *See, e.g.*, *Sawyer v. First Tennessee Bank*, 1998 WL 199645 (Tenn.

Ct. App. 1998) (attached as Exh. 6). The question in bank slip and fall cases does not fix upon whether the injured victim was a bank customer, but ordinary rules of negligence apply, and a non-customer has a cause of action against a bank. The rules governing torts and consumer protection laws apply to businesses, both banks and other firms.

Further, under Tennessee law, when two innocents are victimized by a third party, the loss falls upon the one whose act or omission occasioned it, a long standing principle repeated by Tennessee courts. *See* Plaintiff's Response to Defendant's Initial Motion to Dismiss at 6. This principle applies to banks. In *Commercial Bank & Trust Co. v. Southern Indus. Banking Corp.*, 66 S.W.2d 209 (Tenn. Ct. App. 1932), the Court unequivocally applied this maxim to a bank. There, an impostor defrauded the maker of a note, and the maker placed in the impostor's hands a negotiable instrument. The bank cashed the negotiable instrument. The Court cited the legal maxim: "When one of two persons must suffer loss by the act or fraud of a third party, he who enables that third party to occasion the loss or to permit the fraud ought to be the sufferer." There, the maker bore the loss because it gave the check to the impostor, and its actions caused the loss. This maxim applied to a bank. Assuming *arguendo* that MBNA were innocent,[16] it must bear the loss here. It occasioned the loss, not Plaintiff Mark Wolfe.

Though MBNA has the gall to try to don the robes of victim and compare itself to the 21 year old Mark Wolfe, its claims are wrong, wrong-headed, and illogical. Defendant makes the incredulous contention that Tennessee and federal law protects it, not Plaintiff. It asks this Court to let it freely injure Mr. Wolfe's good name and walk

[16] Plaintiff does not concede that MBNA was an "innocent victim." Its internal documents acknowledge admit, "Nothing was verified," and it chose a telemarketer.

away scot-free. Its hollow pleas are reminiscent of the infamous quote by a 19th Century robber baron: "The public be damned."[17] That sentiment is not the law.

C. Tennessee Does Not Exempt a Bank from Its Tort, Negligence, Libel or Consumer Protection Laws.

Under Tennessee and federal law, no one is above the law. Tort, negligence, gross negligence, recklessness, libel and consumer protection laws apply across the board. Neither federal nor state law recognizes an exemption for MBNA. Neither federal nor state law has carved out an exception based upon commercial convenience, the fact that the perpetrator is a bank or that a defendant is a Fortune 500 company. The information in Defendant's files put it on notice that it had the wrong person at the wrong address at the wrong phone number, and it ignored a host of red flags. Yet, MBNA issued the card and authorized and piled on charges. In spite of this knowledge, it referred the account to a debt collector and refused to even talk to the plaintiff or his father to straighten out the mess it caused.

V. Conclusion

This Court should deny Defendant MBNA's Motion to Dismiss and let a Memphis jury hear and decide this case.

Respectfully submitted,

/s/ Perry A. Craft
Perry A. Craft, (BPR # 6056)
Tim W. Smith, (BPR # 12803)
CRAFT & SHEPPARD, P.L.C.
Shiloh Bldg, 214 Centerview Dr., Ste 233
Brentwood, TN 37027
Phone: (615) 309-1707; fax: (615) 309-1717

[17] Hirsh, THE NEW DICTIONARY OF CULTURAL LITERACY (3rd edition, Houghton Mifflin: 2002).

Certificate of Service

I hereby certify that a true and exact copy of the foregoing document has been filed electronically with the Western District of Tennessee or sent by United States mail, postage prepaid, on this 30th day of October, 2006, to

Leslie Curry-Johnson
R. Dale Bay
Lewis, King, Krieg & Waldrop, P.C.
201 Fourth Avenue South, Ste. 1500
P.O. Box 198615
Nashville, Tennessee 37219

Chad Graddy
Leo Bearman, Jr., Esq.
Baker, Donelson, Bearman, Caldwell & Berkowitz
First Tennessee Bank Bldg, 20th Floor
Memphis, Tennessee 38103

David Israel
Bryan Shartle
Sessions, Fishman & Nathan, LLP
114 Northpart Blvd. Suite 10
Covington, Louisiana 70433

/s/ Perry A. Craft
Perry A. Craft

SEALED

REDACTED FOR PUBLIC DISCLOSURE

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

United States of America,

Plaintiff,

v.

James J. Rose,
(Counts 1-60)

Malcolm D. Newton,
(Counts 40-57)

Defendants.

NO. CR06-0787PHX -JAT (VAM)

INDICTMENT

VIO: 18 U.S.C. §1028(a)(7)
(Fraudulent Use of Identification Documents)
Counts 1-12

18 U.S.C §1029(a)(1)
(Use of Counterfeit Access Devices)
Counts 13-24

18 U.S.C. §1341
(Mail Fraud)
Counts 25-34

18 U.S.C §1343
(Wire Fraud)
Counts 35-39

18 U.S.C. §1956(h)
(Conspiracy to Commit Money Laundering)
Count 40

18 U.S.C. §1956(a)(1)(A)(i) and (ii)
(Promotional Money Laundering)
Counts 41-51

18 U.S.C. §1956(a)(1)(B)(i) and (ii)
(Concealment and Disguise of Source of Funds)
Counts 52-57

18 U.S.C. §1957(a)
(Monetary Transactions in Excess of $10,000)
Counts 58-60

18 U.S.C. §2
(Aid and Abet)

INTRODUCTORY ALLEGATIONS:

At all times relevant to this Indictment:

1. JAMES J. ROSE was the leader and organizer of the scheme to defraud.

2. JAMES J. ROSE was a resident of Phoenix, Arizona and during the early 1990's owned a credit reporting company in California called American Mortgage Services, Inc. ("AMS"). Mortgage brokers used the services of AMS to obtain credit reports for their customers. JAMES J. ROSE retained credit reports, or copies of credit reports over the years. JAMES J. ROSE subsequently used social security numbers contained in these credit reports to establish fictitious identities.

3. MALCOLM D. NEWTON assisted JAMES J. ROSE in executing the scheme to defraud.

4. MALCOLM D. NEWTON first met JAMES J. ROSE in the 1980's.

5. MALCOLM D. NEWTON moved to Arizona in 2001 to work with JAMES J. ROSE.

7. JAMES J. ROSE, with the help of others known and unknown to the Grand Jury created the fictitious businesses Pacific Western Servicing, Pac West Services Corporation, Glen Rock Development, Jadeco Financial Services, North County Services Company, California Western Services, Integrated Electronic & Computer Company, Logical Systems Company, Phoenix Reports Credit, Jotbot, Inc., Equity Funding Corporation, National Software Services, Inc., Industrial Design Center, Inc., Metavue, LTD, Property Appraisals Unlimited, Software Tech, Data Processors, and RSI International, for the purpose of establishing credit histories for fictitious persons by (1) providing false employment histories for the fictitious persons and (2) establishing credit accounts for the fictitious persons.

8. JAMES J. ROSE then reported the fictitious persons credit histories to credit reporting bureaus Experian,TransUnion, and Equifax.

9. JAMES J. ROSE and others known and unknown to the grand jury applied for and obtained credit cards in the names of these fictitious persons utilizing this fabricated credit history.

10. In all, JAMES J. ROSE used over 200 different apartments and business suites located in 14 states, including Arizona, to aid in establishing credit histories, applying for credit cards, receiving credit cards in the mail, establishing merchant accounts,[1] and bank accounts.

11. JAMES J. ROSE opened several merchant and business bank accounts in the names of the fictitious businesses and persons.

12. JAMES J. ROSE utilized these business accounts to pay the expenses of his operation, to conceal funds moving between accounts, and ultimately to obtain money for his own use.

13. By having a merchant bank account, JAMES J. ROSE was able to obtain a credit card machine, which he would then use to swipe fictitious individual's credit cards for fictitious purchases. The credit card issuer would then credit JAMES J. ROSE'S merchant account. Funds from the merchant accounts were transferred to other business bank accounts controlled by ROSE.

14. JAMES J. ROSE recruited other individuals to, among other things, pick up mail for him, cash checks, set up phone lines, rent apartments, file and mail documents, and apply for credit cards.

15. In all, JAMES J. ROSE possessed over 800 social security numbers and used over 250 credit cards from approximately 15 issuing banks.

---

[1] A merchant account is an account set up by a business at a bank in order to deposit income from the purchase of the business goods and services. If a customer purchases goods or services from the business with a credit card, the credit card company transfers the money to the merchant account.

16. In all, JAMES J. ROSE, by withdrawing money from the merchant and business bank accounts he established in the names of fictitious entities and persons, obtained over $760,000.00 through his credit card scheme.

COUNTS 1-12
(Fraudulent Use of Identification Documents)

17. The factual allegations in paragraphs 1-16 of the Indictment are incorporated herein by reference and re-alleged as though fully set forth herein.

18. Beginning on or about February of 2001 to on or about May of 2003, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud at least 15 financial institutions issuing credit cards and obtain money in excess of $760,000.00 by means of false and fraudulent pretenses and representations.

19. On or about the dates listed below in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, for the purpose of executing the aforesaid scheme and artifice to defraud, knowingly used, without lawful authority, a means of identification of another person, to wit, social security numbers obtained from credit reports acquired by ROSE from his credit reporting business, with the intent to commit unlawful activity that constitutes a violation of Federal law, to wit, use of counterfeit access devices in violation of Title 18 U.S.C. §1029 (a)(1), the said means of identification was transported in the mail in the course of such use, and by such conduct JAMES J. ROSE obtained the following items of value aggregating $1,000.00 or more during a one year period:

///

///

Count	Date (on or about)	False Name	Amount of money obtained from use	Credit card #
1	05/02/2002	Hanna Curin (SSN 7483 assigned to Haqqani Saifullah)	$3,481.00	Fleet #0519
2	05/02/2002	Danni Curin (SSN 1969 assigned to Polly Hatch	$4,981.00	HHB #5179
3	05/02/2002	Adam Gregory (Las Vegas) (SSN 9855 assigned to Mary Harry	$4,983.00	HHB #0141
4	05/24/2002	A.J. Rose (Seattle) (SSN 4487, assigned to Mehdi Sonboli)	$3,486.00	Fleet #3988
5	05/28/2002	Jamei Enrico (SSN 3707 assigned to Manuel Hernandez	$2,984.00	Nova #4595
6	05/29/2002	Scott Johnson (SSN 8342, assigned to Leslie Smith)	$3,485.00	Fleet #3980
7	06/04/2002	AJ Rose (Phoenix) (SSN 3725, assigned to Jaime Serrano)	$4,916.00	Nova #6759
8	06/04/2002	Keith P. Allen (SSN 1981, assigned to Oscar Solis	$4,895.00	Wells Fargo #1124
9	06/11/2002	Andrew Riddell (SSN 2666 assigned to Chong Edwards)	$4,908.00	Fleet #8419
10	06/30/2002	James T. Avon (SSN 7247 assigned to Travis Muller	$3,498.00	Fleet #4343
11	08/08/2002	Byron Jordan (North Hills, CA) (SSN 3193 assigned to Raymond Allen	$4,965.00	Fleet #8369
12	10/15/2002	Felice Kuda (Seattle) (SSN 2129 assigned to Joanne Solomon)	$4,314.00	Sears #0138

In violation of Title 18, United States Code, Section 1028 (a)(7).

COUNTS 13-24
(Use of Counterfeit Access Devices)

20. The factual allegations in paragraphs 1-16 of the Indictment are incorporated herein by reference and re-alleged as though fully set forth herein.

21. From on or about February of 2001 to on or about May of 2003, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud at least 15 financial institutions issuing credit cards and obtain funds in excess of $760,000.00 by false and fraudulent pretenses and representations.

22. On or about the dates listed below in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others know and unknown to the Grand Jury, did for the purpose of executing the aforesaid scheme and artifice to defraud, knowingly and with intent to defraud use one or more counterfeit access devices, to wit, credit card accounts obtained by the submission of fraudulent information, said use affecting interstate commerce, in that banking channels were used to facilitate the following credit card transactions:

Count	Date	Access Device	Amount of money obtained from use
13	05/02/2002	Fleet #0519 Hanna Curin	$3,481.00
14	05/02/2002	Household Bank Platinum #5179, Danni Curin	$4,981.00
15	05/15/2002	Capital One #4450 Scott Johnson	$199.00
16	05/23/2002	Amex #61005 Hanna Curin	$745.00
17	05/28/2002	Fleet E Titanium #3980, Scott Johnson	$199.00
18	05/31/2001	Capital One #8012 AJ Rose	$199.00
19	06/04/2002	Wells Fargo #6759 AJ Rose	$4,916.00
20	06/04/2002	Household Bank Platinum #6178, Andrew Riddel	$4,987.00
21	06/04/2002	Wells Fargo #1124, Keith Allen	$4,895.00
22	06/30/2002	Fleet Titanium #4343, James T. Avon	$3,498.00

Count	Date	Access Device	Amount of money obtained from use
23	09/11/2002	Fleet Platinum #8369, Byron Jordan	$500.00
24	09/05/2002	Fleet Platinum #8419, Andrew Riddell	$500.00

In violation of Title 18, United States Code, Section 1029 (a)(1).

COUNTS 25-34
(Mail Fraud)

23. The factual allegations in paragraphs 1-16 of the Indictment are incorporated herein by reference and re-alleged as though fully set forth herein.

24. From on or about February of 2001 to May of 2003, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud at least 15 financial institutions issuing credit cards and obtain funds in excess of $760,000.00 by false and fraudulent pretenses and representations.

25. On or about the dates listed below, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, did for the purpose of executing the aforesaid scheme and artifice to defraud, knowingly deposit and caused to be deposited matters or things to be delivered by a commercial interstate delivery service and United States mail, according to the directions thereon, to or from various locations in Arizona as follows:

Count	Date (On or about)	From	To	Description of Mailing
25	05/11/2002	Capital One - Seattle, WA	Jamei Enrico Phoenix, AZ	Capital One Visa Gold statement card #2229
26	05/28/2002	Household Bank - Anaheim, CA	AJ Rose Chandler, AZ	Platinum Mastercard statement #6764

Count	Date (On or about)	From	To	Description of Mailing
27	05/28/2002	Fleet - Wilmington, DE	Scott Johnson Chandler, AZ	Fleet Titanium #3980
28	06/03/2002	American Express - Los Angeles, CA	Hanna Curin Phoenix, AZ	Mailing from American Express #61005
29	06/05/2002	Capital One - Seattle, WA	Scott Johnson Chandler, AZ	Capital One Gold Visa statement card #4450
30	06/20/2002	Household Bank - City of Industry, CA	Andrew B. Riddell Phoenix, AZ	Platinum Mastercard statement #6178
31	06/26/2002	Capital One - Seattle, WA	AJ Rose Chandler, AZ	Capital One card statement #8012
32	07/02/2002	Fleet - Wilmington, DE	Keith P. Allen Chandler, AZ	Fleet Platinum Card #8401
33	07/15/2002	Fleet - Wilmington - DE	James T. Avon Phoenix, AZ	Fleet Titanium statement #4343
34	08/07/2002	Fleet - Wilmington, DE	Andrew Riddell Chandler, AZ	Fleet statement card #8419

In violation of Title 18, United States Code, Section 1341.

COUNTS 35-39
(Wire Fraud)

26. The factual allegations in paragraphs 1-16 of the Indictment are incorporated herein by reference and re-alleged as though fully set forth herein.

27. From on or about February of 2001 to May of 2003, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud at least 15

financial institutions issuing credit cards and obtain funds in excess of $760,000.00 by false and fraudulent pretenses and representations.

28. On or about the dates listed below, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, for the purpose of executing the aforesaid scheme and artifice to defraud, did knowingly cause to be transmitted by wire in interstate commerce certain signs and signals, that is, wire transfers of proceeds of the scheme from a point of sale machine, located in Arizona and controlled by JAMES J. ROSE, for the purpose of swiping fictitious credit cards with the transactions being electronically transferred interstate to merchant account providers maintaining merchants accounts controlled by JAMES J. ROSE as follows:

Count	Date	Amount	False Name	Merchant Provider
35	04/26/2002	$4,854.85	Adam H. Gregory Household Bank #0141	Paymentech Dallas, Texas
36	05/03/2002	$3,481.60	Hanna S. Curin Fleet# 0519	Paymentech Dallas, Texas
37	06/05/2002	$4,987.18	Andrew B. Ridell Household Bank #6178	Paymentech Dallas, Texas
38	08/04/2002	$1,485.21	Randell Enrico Sears #6553	PNC Pittsburgh, PA
39	09/05/2002	$4,486.52	James T. Avon Fleet #4343	PNC Pittsburgh, PA

In violation of Title 18, United States Code, Section 1343.

COUNT 40
(Conspiracy to Commit Money Laundering)

29. The factual allegations in paragraphs 1-16 of the Indictment are incorporated herein by reference and re-alleged as though fully set forth herein.

30. From on or about February of 2001 to May of 2003, in the State and District of Arizona and elsewhere, defendants JAMES J. ROSE and MALCOLM D. NEWTON and others known and unknown to the Grand Jury, did knowingly and willfully conspire and agree with each other and with others known and unknown to the Grand Jury, to commit the following offenses against the United States:

Title 18, United States Code, Section 1956(a)(1)(A)(I) (Promotional Money Laundering).

Title 18, United States Code, Section 1956 (a)(1)(B)(I) (Concealment or Disguise of Proceeds)

METHOD AND MEANS

31. Defendants JAMES J. ROSE and MALCOLM D. NEWTON and others known and unknown to the Grand Jury, used the proceeds of access device fraud, fraudulent use of identification documents, and mail and wire fraud to promote the carrying on of these offenses all of which are specified unlawful activities.

32. Defendants JAMES J. ROSE and MALCOLM D. NEWTON knew the money and funds received from the use of the fraudulent credit cards represented proceeds of some form of unlawful activity.

33. After money and funds were obtained by processing fraudulent credit card transactions through merchant accounts located in Cheyenne, Wyoming and Memphis, Tennessee, controlled by ROSE, the proceeds were deposited into two Wells Fargo business bank accounts using the fictitious names Tockar Tobias and Vivian Turner. Checks were written against these accounts and used to pay the expenses of carrying on the fraudulent scheme, including; rent for apartments and business suites, payments to credit card companies, hotel rooms, and salaries. These payments for business expenses were made with the intent of further promoting the ongoing credit card scheme.

34. After money and funds were obtained by processing fraudulent credit card transactions, ROSE would obtain the proceeds by cashing checks from the accounts in

Arizona. Occasionally, defendant MALCOLM D. NEWTON was provided with proceeds of the scheme in one form and would convert the funds to another payment instrument or form, and then return some or all of the funds to JAMES J. ROSE in an effort to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the scheme.

35. JAMES J. ROSE transferred funds between two different financial institutions for the purpose of concealing or disguising the nature, location source, ownership, or control of the proceeds of the scheme.

OVERT ACTS

36. On or about the following dates, in the District of Arizona and elsewhere, in furtherance of the aforesaid conspiracy, and to effect the objects of the conspiracy, defendants JAMES J. ROSE and MALCOLM D. NEWTON and others known and unknown to the Grand Jury, committed and caused to be committed the following overt acts, which represent checks written on Glenrock Development Corp. bank accounts controlled by defendant JAMES J. ROSE, to Malcolm Newton:

Overt Act	Date	Check#	Amount	Payee	Memo
(a)	04/17/01	2041	$800.00	Malcolm Newton	Rents MO
(b)	04/19/01	2043	$1,587.00	Malcolm Newton	Commission #56874
(c)	06/04/01	1036	$4,826.00	Malcolm Newton	Cashier's check
(d)	07/18/01	1066	$2,958.00	Malcolm Newton	Payroll
(e)	07/18/01	1064	$2,985.36	Malcolm Newton	Payroll
(f)	08/07/01	15050	$9,467.32	Malcolm Newton	Equipment purchase
(g)	08/16/01	1080	$2,497.45	Malcolm Newton	Payroll

In violation of Title 18, United States Code, Section 1956(h).

///

COUNTS 41-51
(Promotional Money Laundering)

37. The factual allegations of paragraphs 1-16, and 31-36 of the Indictment are incorporated by reference and re-alleged as though fully set forth herein.

38. Beginning on or about February of 2001 to on or about May of 2003, in the State and District of Arizona and elsewhere, defendants JAMES J. ROSE, MALCOLM D. NEWTON and others known and unknown to the Grand Jury, knowing that the property involved in financial transactions represented the proceeds of some form of unlawful activity, knowingly and willfully conducted and attempted to conduct financial transactions, as set forth below, which in fact involved the proceeds of specified unlawful activity, to wit, mail fraud in violation of 18 U.S.C. §1341, wire fraud in violation of 18 U.S.C §1343, access device fraud in violation of 18 U.S.C. §1029(a)(1), and use of fraudulent identification documents in violation of 18 U.S.C. §1028 (a)(7), with the intent to promote the carrying on of the specified unlawful activities.

Count	Date	Amount	Payee (Promotional Purpose)	Payor
41	05/27/02	$1,082.00	Ritz Carlton Hotel Phoenix, Arizona (Employee expense)	American Express Card in name of Adam Gregory
42	06/04/02	$134.41	HQ Global Workplaces 2390 E Camelback Dallas, Texas 75284 (Office Suite)	RSI Research & Development Corporation
43	06/04/02	$219.92	HQ Global Workplaces 3800 Century Park East 5th Floor Los Angeles, California 90067 (Office Suite)	RSI Research & Development Corporation
44	06/04/02	$936.56	The Preserve 13820 S 44th Street #1230 Phoenix, Arizona (Apartment)	RSI Research & Development Corporation.

Count	Date	Amount	Payee (Promotional Purpose)	Payor
45	06/04/02	$975.00	RE/SYS Real Estate 2432 Silver Shadow Drive, Nevada (Office Suite)	RSI Research & Development Corporation.
46	06/04/02	$689.47	Mountain Canyon Apartments 3236 East Chandler Boulevard Phoenix, Arizona 85048 (Apartment)	RSI Research & Development Corporation
47	06/04/02	$425.00	Investment Realty/Grande Development 2611 East Oak Grove Drive Sandy, Utah 84792 (Office Suite)	RSI Research & Development Corporation
48	06/04/02	$1,101.90	Millennium Commercial Real Estate 3909 South Maryland Parkway #311 Las Vegas, Nevada 89119 (Office Suite)	RSI Research & Development Corporation
49	04/22/02	$379.09	One Castle Hill 1100 NW Loop 410, Ste. 215 San Antonio, Texas 78213	RSI Research & Development Corporation
50	06/06/02	$172.70	Executive Suite Services 9040 Executive Park Drive #200 Knoxville, Tennessee 37923 (Office Suite)	RSI Research & Development Corporation
51	06/06/02	$195.79	Clark Tower Executive Suites 5100 Poplar Avenue 27th Floor Memphis, Tennessee 38137 (Office Suite)	RSI Research & Development Corporation

In violation of Title 18, United States Code, Section 1956(a)(1)(A)(i) and (ii) and 2.

COUNTS 52-57
(Concealment and Disguise)

39. The factual allegations of paragraphs 1-16, and 31-36 of the Indictment are incorporated by reference and re-alleged as though fully set forth herein.

40. Beginning on or about February of 2001 to on or about May of 2003, in the State and District of Arizona and elsewhere, defendants JAMES J. ROSE and MALCOLM D. NEWTON and others known and unknown to the Grand Jury, knowing that the property involved in financial transactions represented the proceeds of some form of unlawful activity, knowingly conducted and attempted to conduct financial transactions, as set forth below, which in fact involved the proceeds of specified unlawful activity, to wit, mail fraud in violation of 18 U.S.C. §1341, wire fraud in violation of 18 U.S.C §1343, access device fraud in violation of 18 U.S.C. §1029 (a)(1), and use of fraudulent identification documents in violation of 18 U.S.C. §1028(a)(7), knowing the transactions were designed in whole or in part to conceal or disguise the ownership or the control of the proceeds of specified unlawful activity.

Count	Date	Amount	Payee	Payor
52	10/04/02	$9,440.76	Glenn Rock Development Corp.	RSI Research and Development
53	11/28/01	$8,905.00	Glenn Rock Development Corp. (Wells Fargo Bank)	Glenn Rock Development Corp. (Bank of America)
54	11/19/01	$3,963.18	Glenn Rock Development Corp. (Wells Fargo Bank)	Glenn Rock Development Corp. (Bank of America)
55	11/20/01	$1,989.00	Kathryn Roa	Glenn Rock Development Corporation
56	6/14/02	$4,750.00	Malcolm Newman	RSI Research and Development
57	8/23/01	$2,548.23	Malcolm Newman	Glenn Rock Development

In violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) and (ii) and 2.

COUNTS 58-60
(Monetary Transactions)

41. The factual allegations of paragraphs 1-16 of the Indictment are incorporated by reference and re-alleged as though fully set forth herein.

42. Beginning on or about February of 2001 to on or about May of 2003, in the State and District of Arizona and elsewhere, defendants JAMES J. ROSE and others known and unknown to the Grand Jury, knowing that the property involved in financial transactions represented the proceeds of some form of unlawful activity, knowingly conducted and attempted to conduct financial transactions, through a financial institution, affecting interstate commerce (in criminally derived property of a value greater than $10,000.00), as set forth below, which in fact involved the proceeds of specified unlawful activity, to wit, mail fraud in violation of 18 U.S.C. §1341, wire fraud in violation of 18 U.S.C §1343, access device fraud in violation of 18 U.S.C. §1029(a)(1), and use of fraudulent identification documents in violation of 18 U.S.C. §1028 (a)(7).

Count	Date	Transferor	Transferee	Amount
58	10/04/2002	RSI	Wells Fargo Bank Card Account 1124 Keith P. Allen (Oscar Solis)	$12,801.00
59	10/04/2002	RSI	Wells Fargo Bank Account 6759 AJ Rose (Jaime Serrano)	$10,697.00
60	10/04/2002	RSI	Wells Fargo Bank Account 9201 Carmen Valdez (Richard Soutsos)	$10,626.00

In violation of Title 18, United States Codes, Sections 1957(a).

///

///

A TRUE BILL

_____/s/_____
FOREPERSON OF THE GRAND JURY
Date: August 22, 2006

PAUL K. CHARLTON
United States Attorney
District of Arizona

/s/

_____
Michelle Hamilton-Burns
Assistant U.S. Attorney

/s/

Julie Halferty
Special Assistant U.S. Attorney