2

TrademarkBots®
TrademarkBots.com, Inc.
5100 Tamiami Trail North, Suite 105
Naples, Florida 34103
t-1-239-434-3850 – f-239-642-9115

Delivered by Email

OCC
Attention: Docket No. 03-18
Public Information Room
Office of the Comptroller of the Currency
Fax: (202) 874-4448
e-mail: regs.comments@occ.treas.gov

FRB
Refer to: Docket No. OP-1155
Ms. Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
Fax: (202) 452-3819 or (202) 452-3102
e-mail: regs.comment@federalreserve.gov

FDIC
Robert E. Feldman, Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
Fax: (202) 898-3838
e-mail: comments@fdic.gov

OTS
Regulation Comments
Refer to: No. 03-35
Chief Counsel's Office
Office of Thrift Supervision
Fax: (202) 906-6518
e-mail: regs.comments@ots.treas.gov

Attn: OCC, FRB, FDIC, and OTS

August 22, 2003

Re: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice – dated August 12, 2003

We are submitting our research paper dated August 14, 2003[1] on a set of relevant risks from the content of the Internet that are identified by the DOJ's Public Advisory of May, 2003[2] that are not included within your release dated August 12, 2003[3]. These risks relate to the misuse of online corporate identities (brand/trademarks) within the content of the Internet to defraud online banking consumers through fake web sites, as one timely example. We recommend that these risks be considered and addressed for the benefit of the online banking consumers.

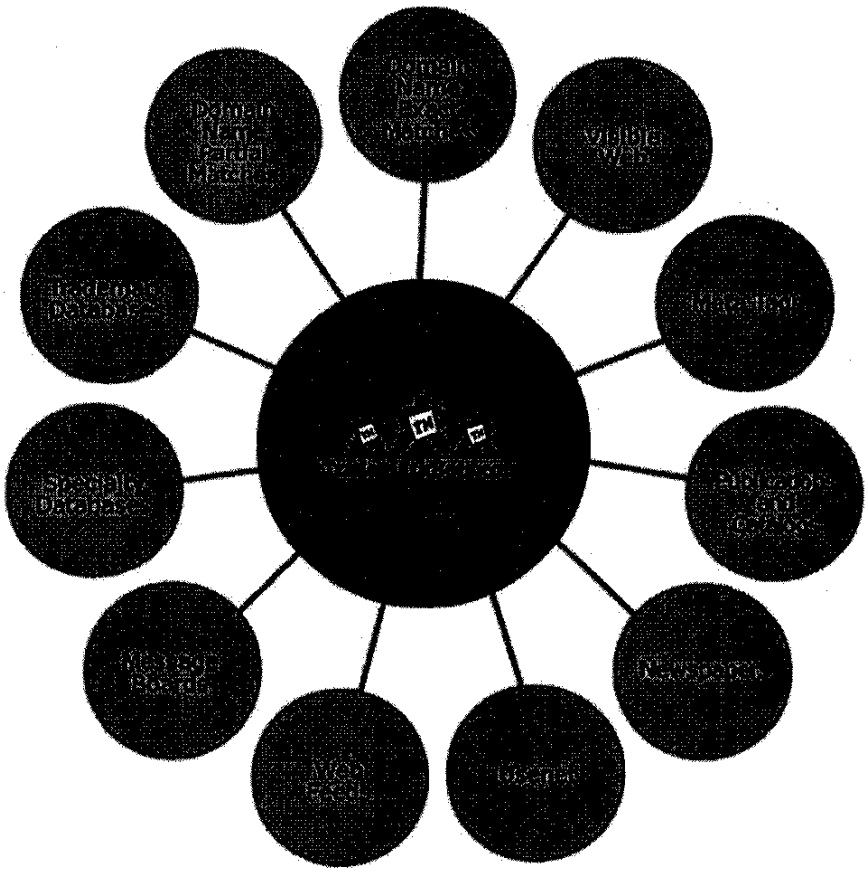
Respectfully submitted,

Beckwith B. Miller

Footnotes:
[1]tmb_580057.pdf: "Online Corporate Identity Risks: Banking & Finance: August 14, 2003"
[2]www.usdoj.gov/opa/pr/2003/May/publicadvisory1.pdf
[3]http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030812/attachment.pdf.

Enclosure:
tmb_580057.pdf: "Online Corporate Identity Risks: Banking & Finance: August 14, 2003"

Online Corporate Identity Risks
Banking and Finance
Central & South America – August 14, 2003
Internet Risks on Trademarks



 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

How well are banks protecting their Corporate Identity (brands & trademarks) and online clients from identity theft across **the content of the Internet?**

The leading banks in North America are not taking adequate measures to protect their corporate identities from misuse within the content of the internet. This, consequently, is contributing to confusion and potential personal identity losses for online clients.

Fraudulent web sites (FDIC, 9-15-2000), web site "spoofing" (DOJ and Canada's Solicitor General, 5-2003), external hacking with "look alike web sites (BITSinfo.org, 6-2003), and "phishing" (WSJ, 7-22-03) are all addressing the risk of corporate identities, defined as brands and/or trademarks, being used in a variety of techniques on the internet to mislead and steal the personal identity assets (social security numbers, credit card numbers, etc.) of unsuspecting consumers. Identity thefts will use exact matches and/or embedded matches of a corporate brand within emails, web sites, domain names, meta tags, trademarks and discussion groups to capture their prey.

Examples of active domain names and web sites owned by parties other than the rightful bank (3rd parties) that are confusingly similar to bank trademarks, as of August 12, 2003, include: bankonecreditcard.com, chasemanhattan.com, citicorps.com, lehmanbrothers.com, mellon.net, northerntrust.info, pncbanking.com, royalbankofcanada.com, suntrust-banks.com, thekeybank.com, retirementplanwellsfargo.com, and schwabmortgagecenter.com. (Source: Study #3 and ebusinesstrademarkreports.com.)

Factors that are contributing to this problem, per our Report, include:

- BITS, a technology consortium for the 100 largest US banks, is concentrating on identity theft arising from transaction systems but not from the content of the internet.
- Banks are not following the appropriate Regulatory guidelines for protecting and monitoring their corporate identities within the content of the Internet. (Addendum 1).
- Recent US legislation is focusing on identity theft risks arising from system failures.
- The August 12, 2003 "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" from the OCC, FRB, FDIC, and OTS (the Agencies) is also focusing, as it relates to the internet, on identity theft risks arising from network and/or customer information systems.
- An article published 6-03 by The American Bar Association addresses the risks for lawyers and their clients when lawyers do not use new technology, specifically the Internet, for client research.

The potential severity of this problem is presented within our Report:

- Globally, very few banks (139 banks from 30 countries) have proactively fought cybersquatters by using the global domain name arbitration system (UDRP). (Study #1)
- Within North America, an extraordinarily high percentage of bank trademarks are at risk for cybersquatting, e.g., 87% or 3,445 of the 3,964 live, unique trademarks, owned

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

by the banks and brokerage firms with the 50 largest trademark portfolios in the US, are at risk for cybersquatting and misuse within the content of the Internet. A timeline analysis shows this risk is rapidly growing during 2002 and the 1st Q of 2003. (Study #2)

- Deeper searching of individual bank trademarks, using our technology, is yielding the foregoing examples of domain names owned by 3rd parties. (Study #3)

Our separate study, on the state level, for the 200 largest banks in Florida shows a similar trend whereby the banks are not taking adequate measures to protect their brands from online theft and misuse. 89% of the official Florida bank names are at risk for online identity theft as of August 14, 2003. This study will be extended to other major states.

Recommendations for building safe eBusiness Brands™: In order to create a safer online environment and to prevent personal identity theft from the misuse of brands within the content of the internet, each business, including the 9,000 US banks and the 4,000 banks in the TheBanker.com's database, should be proactive and:

1. Register each primary brand as a trademark in every country of operation in order to fight the misuse of brands within those countries and within the content of the internet.
2. Register matching domain names for trademarks in order to prevent cybersquatting and subsequent personal identity theft and UDRP filings ($1,150 per domain name).
3. Monitor the content of the Internet to identify and stop the fraudulent use of corporate identities with today's technology. (Our search technology is widely available for the public through www.Hoovers.com on each Company Capsule Page and through www.eBusinessTrademarkReports.com. Search fees begin @$20.)
4. Fight trademark infringements and, when needed, use UDRP filings.
5. Disclose, for online consumers, the potential risks of corporate identity theft and endorse a common standard for safe brand management on the Internet.

In effect, each business needs do their part to protect their brands and online consumers.

Our Report studied the following banks and brokerage firms with the 50 largest USPTO trademark portfolios: AG Edwards, AmSouth Bancorp, Bank of America, Bank of Hawaii, Bank of Montreal, Bank of New York, Bank One, BB&T, Bear Stearns, Canadian Imperial, Charles Schwab, Citicorp, Comerica, Commerce Bancorp, Compass, e*Trade, Fifth Third, First Merit, First Tennessee, FleetBoston, F.N.B. Corporation, Franklin Resources, Goldman Sachs, Huntington Bancshares, JP Morgan Chase, Key Corp, Legg Mason, Lehman Brothers, M&T Bank, Marshall & Isley, MBNA, Mellon Financial, Merrill Lynch, Morgan Stanley, National City, Northern Trust, PNC Financial, Providian, Raymond James, Regions Financial, Royal Bank of Canada, SouthTrust Corp, State Street Corp, SunTrust, Synovous, Union Planters, US Bancorp, Wachovia, Wells Fargo, and Zions.

Visit www.OnlineCorporateIdentityRisks.com to order these Reports as of 8-14-03:

Online Corporate Identity Risks: Banking & Finance Report: Global & North America
Fee: $1,000. 39 pages per Table of Contents on page 4. Format: PDF

Detailed Trademark Portfolio Analysis: Each of the Top 50 North American Banks
Fee: $1,250. 29 pages per each bank report. Format: PDF

Online Corporate Identity Risks By Bank By State: Volume 1. No. 1: Florida
Fee: $750. 12 pages covering 200 of the Largest Banks in Florida. Format: PDF

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Online Corporate Identity Risks: Banking & Financial Services
Global & North American
Table of Contents

Page	Topic
5	Introduction & Executive Summary: Online Corporate Identity Theft
6	The Big Picture: Metrics and Initiatives to Fight Online Identity Theft o Network Identity Theft vs. Online Corporate Identity Theft
7-11	Timeline Analysis of Key Events In Fight Against Online Identity Theft
11-15	Network Identity Theft vs. Online Corporate Identity Theft o Bank Regulations addressing Online Corporate Identity Theft Key Initiatives for Network Identity Theft Issues: o Gramm-Leach-Bliley Act o Notice of Security Breach - Civil Code Sections 1798.29 and 1798.82 (Ca) o Senate Bill (S.1350), "Notification of Risk to Personal Data Act" o US Banking Industry Initiative led by BITS (Bitsinfo.org) o Interagency Guidance: FDIC, FRB, OCC, OTC: August 12, 2003
16	American Bar Association's 6-03 Article: "Not Using New Technology"
17	Summary: Factors Contributing to Online Corporate Identity Theft
17	Scope and Focus of the Study: 3 Levels of Risk Analysis: o Global UDRP (Uniform Domain Name Dispute Resolution Policy) Trends (Study 1) o North American Review (Study 2) o A Deeper Content Analysis (Study 3)
18-20	Global UDRP Case Studies: Online Corporate Identity Theft: Global Banks
21	Study #1: Global UDRP Analysis
22-24	Study #2: North American Review of the 50 Largest Banks and Brokerage Firms
25	Study #3: A Deeper Content Analysis using TrademarkBots® Search Technology: www.eBusinessTrademarkReports.com
26	Final Observations and Recommended eBusiness Brand™ Strategy
27	Reports Available for Purchase: o Detailed Trademark Portfolio Analysis: 50 North American Banks
28-31	Table 1: Online Corporate Identity Risks: Global & North American Banks
32-39	Addendum 1: Bank Regulations

References:

[1]BITS: (www.bitsinfo.org)

June, 2003	[2]Financial Identity Theft: Prevention and Consumer Assistance http://www.bitsinfo.org/bitsidtheftwhitepaper.pdf
April, 2003	[3]Fraud Prevention Strategies for Internet Banking http://www.bitsinfo.org/mointernetwp.pdf

American Bar Association:

June, 2003	[4]"Not Using New Technology: Ethical and Liability Risks. Face Up or Face Peril" http://www.abanet.org/genpractice/magazine/june2003/keepup.html

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

[illegible]

How well are banks protecting their Corporate Identity (brands & trademarks) and online clients from identity theft across **the content of the Internet**?

[illegible]

Banks are primarily focusing on identity theft issues arising from the systems and not the content of the internet. By adopting a more balanced, proactive approach, banks can create a safer online environment using today's technology for the benefit of all stakeholders.

[illegible]

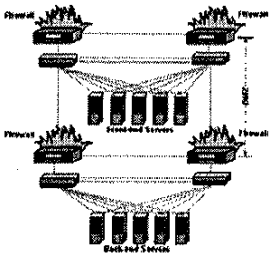
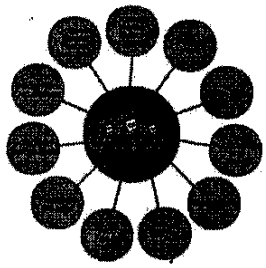
Corporate Identity theft on the Internet is defined, for this study, to include fraudulent use by third parties of trademarked corporate brands within the content of the Internet that mislead online consumers into releasing their personal identity assets, i.e., social security numbers, credit card numbers and/or drivers license. Identity theft and fraud occurs within the content of the Internet when unauthorized third parties acquire and/or market domain names and key words within the visible web, newspapers, publications, usenet, message boards, and meta tags that are either an exact or partial match to a firm's brands and/or trademarks. Such theft contributes to consumer confusion and trademark dilution, which in turn, generates direct economic losses for (1) the bank through lost sales, weakened intellectual property rights and litigation and (2) for consumers who are deceived and surrender cash, credit card numbers and/or their social security number.

[illegible]

This paper focuses on the global trends by the banking industry to fight corporate identity theft and misuse within the content of the Internet. It includes 2 core studies:

- Study #1: Our analysis of UDRP claims finds there are only 139 banks globally from 30 countries that have submitted UDRP claims from late 1999 with the beginning of the UDRP process through the end of our research or 3-31-03.
- Study #2: By analyzing the 50 largest USPTO (United States & Patent Trademark Office) trademark portfolios owned by banks and brokerage firms in North America, as of March 31, 2003, one finds that at least 87% of the 3,964 trademarks belonging to these 50 North American Banks are at risk for cybersquatting or corporate identity theft on the Internet. (This research has been double-checked as of July 31, 2003 and 87% are still at risk.) A timeline analysis shows this risk trend has been constant since the 1980's and is now rapidly growing in size as 48% or 1,922 of the 3,964 trademarks in this study have been submitted in the 4 quarters of 2002 and the 1st quarter of 2003. If this trend continues for the remainder of 2003 and into 2004 and the banks continue with their historical brand protection strategies, then the banks and their online clients will be subject to even greater online identity theft.

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Consumers on The Internet	Internet Network **Systems**	Internet **Content**
		
Growth Trends for: o Online Consumers o Banks o Domain Disputes	o Gramm-Leach-Bliley o Ca. Civil Code 1798.29 o Senate Bill 1350 o BITS (Bitsinfo.org) o Banking Regulators (8-12-03)	o Secret Service o Department of Justice o Trademark Law o Banking Regulations: (Addendum 1)

This matrix outlines many of the interrelated initiatives in the battle against identity theft for individuals and corporate identities (brands and trademarks) on the Internet. The initiatives and resources dedicated to improving the Internet Network Systems have successfully addressed many issues in the battle against online identity theft. We address a number of these initiatives in order to demonstrate insufficient attention and resources have been allocated to protecting corporate brands within the content of the Internet. This has given rise to significant risk exposures for the brands of the banking industry within the content of the Internet along with matching warnings from the FDIC, DOJ and WSJ. We disclaim any errors or omissions in our historical review of the network issues but stand firm by our analysis of the unmitigated risks of the online corporate identities of the global and major North American banks.

- There are 100,000,000 households worldwide using online banking with 28,000,000 of these users in the USA as of December, 2002. (OnlineBankingReport.com)
- There are 9,314 deposit-taking institutions in the USA as of March, 2003 and 4,000 banks in the FT's global banking database (TheBanker.com).
- The UDRP (Uniform Domain Name Dispute Resolution Policy) was created in late 1999 as a global arbitration forum to reclaim "cybersquatted" domain names. Only 139 banks from 30 countries have filed UDRP claims from late 1999 through Q1 2003 per our Study 1.

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

A review of key initiatives shows an increasing awareness and concern in 2003 about the risks posed by Online Corporate Identity Risks (OCIR) in its many forms, i.e., cybersquatting, fraudulent web sites, web site "spoofing", external hacking with "look alike web sites, and "phishing". If any of these terms or risks are mentioned in the following initiatives, then "OCIR" will be placed in the "Focus" column. Initiatives addressing Network Identity Risks (NIR) will also be identified in the Focus column. Broad-based initiatives will not be given any special designation.

The names and related abbreviations of organizations listed below are as follows:

- BITS, is a nonprofit industry consortium of the 100 largest financial institutions in the United States.
- DOJ: The US Department of Justice.
- FDIC: Federal Deposit Insurance Corporation's mission is to maintain the stability of and public confidence in the nation's financial system.
- FRB: Federal Reserve Board
- FTC: Federal Trade Commission.
- OCC: The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises national banks to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.
- OTC: Office of Thrift Supervision
- Secret Service, a part of the US Department of Homeland Security.
- WIPO: World Intellectual Property Organization.
- WSJ: Wall Street Journal.

Date	Focus	Source and Initiative
Nov. ,1990		Secret Service: On November 5, 1990, the Congress enacted legislation that gave the Secret Service concurrent jurisdiction with the Department of Justice to investigate fraud, both civil and criminally against any federally insured financial institution or the Resolution Trust Corporation. http://www.treas.gov/usss/financial_crimes.shtml
1998		BITS' Website Recommendations: "Given the importance of the privacy issue, BITS and The Financial Services Roundtable (FSR) have issued alerts, white papers, and updates to CEOs of financial institutions with frequency. At the Roundtable's 1998 Fall Conference, the Boards of both BITS and FSR unanimously endorsed the following recommendations related to banks' Internet Web sites. These recommendations have been communicated to all FSR members…" The url below, as of 8-10-03, lists recommendations for posting privacy statements and educating consumers. http://www.bitsinfo.org/websiterec.html

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

1998		DOJ: The 1998 federal law, Identity Theft and Assumption Deterrence Act, which prohibits knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. http://www.usdoj.gov/criminal/fraud/idtheft.html
Oct., 1999	OCIR	October, 1999, OCC: "The Internet Handbook defines 14 Internet Risks, i.e., Credit Risk, Interest Rate Risk, Liquidity Risk, Price Risk, Foreign Exchange Risk, Transaction Risk, Compliance Risk, Strategic Risk, and Reputation Risk. A bank's reputation can be damaged by Internet banking services that are poorly executed...It should be clear to the customer when they have left the bank's Web site so that there is no confusion about the provider of the specific products and services offered or the security and privacy standards that apply." (Addendum 1)
1999		Gramm-Leach-Bliley Act of 1999 outlaws "pretexting". Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you.
Sept., 2000	OCIR	The FDIC's web site on Safe Internet Banking, last updated 9-15-00 as of 8-10-03, warns "Protect yourself from fraudulent Web sites": "For example, watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as, that of a real financial institution. The intent is to lure you into clicking onto their Web site and giving your personal information, such as your account number and password. Always check to see that you have typed the correct Web site address for your bank before conducting a transaction." http://www.fdic.gov/bank/individual/online/safe.html
Nov., 2000	OCIR	FDIC: "Protecting Internet Domain Names". "Risk Management Techniques to prevent customer confusion, reputational harm, fraud and legal disputes, bank management can employ a number of practices and techniques... Timely registration and renewal of a bank's domain name(s) are important to assure that the bank acquires and retains ownership of the Internet addresses that it desires.... Institutions may benefit from conducting periodic Internet searches to determine whether there are names being used that are similar to their domain name, legal name or other trade/product names." (Addendum 1)
April, 2001	NIR	The Board of Governors of the Federal Reserve System issued a letter (SR 01-11 (SUP)) dated April 26, 2001 on the subject of Identity Theft and Pretext Calling. The "SR letter addresses how state member banks

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

		and other banking organizations supervised by the Federal Reserve that provide products or services to the public or that maintain customer account information should protect customer information against identity theft." http://www.federalreserve.gov//boarddocs/SRLetters/2001/sr0111.htm
Nov., 2001		Florida Bankers Association's issued a press release alerting the general banking public to online identity theft on 11-21-01. http://www.banksprotectprivacy.com/news.htm
Sept., 2002		The FTC publication, "ID Theft: When Bad Things Happen To Your Good Name" is often cited as a definitive resource on the factors contributing to online Identity Theft. http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm
Dec., 2002	OCIR	WIPO's 2002 Survey states: "Trademark owners also face new challenges with respect to use of their marks in the digital environment. In the current marketplace, it is estimated that a typical large business owns between 200 and 500 corporate, product and service identities, that need to be registered, maintained and defended.196 A corporate presence on the Internet requires trademark owners to defend their rights against new forms of trademark abuse and across millions of discrete sites, in multiple languages and domains. For example, trademarks and logos may be used in a site or domain name in connection with pornographic or other objectionable sites, or by trade competitors to divert search engine traffic, or dilute or tarnish a brand." (Addendum 1)
Jan., 2003		The Federal Reserve Board announced a new booklet designed to help consumers protect themselves against identity theft. It was developed by the Federal Reserve Bank of Boston and is available online: http://www.bos.frb.org/consumer/identity/idtheft.htm
April, 2003	NIR	BITS: "Fraud Prevention Strategies for Internet Banking". On page 5, the report defines the scope of its research paper with this quote: "In discussing Internet threats, it is important to differentiate between two major threat types: (1) Application Threats, in which the person committing the fraud appears to be a legitimate user of the online banking application, but is instead conducting illegal activities. (Firewalls, proxy servers, network filters and similar products will not protect an institution from application-based threats.) (2) Network-based threats, such as hacks, site-defacement attacks, denial of service attacks, and viruses and worms, which attack the core network and infrastructure but don't directly try to carry out transactions and are not application-specific. (Established tools, such as firewalls, can be used to counter such attacks.) This paper addresses application threats only; it does not address network issues. (p.5) This paper, a product of the efforts of the BITS Internet Fraud Working Group, reviews the processes financial

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

		institutions use when enrolling a customer in online banking and opening an account online. It also outlines successful strategies institutions employ to address Internet fraud, including identity theft, and minimize risk in servicing customers via the Internet. The paper covers the processes involved in enrolling customers in online banking, opening a deposit account, and using bill pay services, as well as key points of employee and customer communication that can help prevent Internet fraud." (p.6) http://www.bitsinfo.org/mointernetwp.pdf
May, 2003	OCIR	The joint Special Report by The United States Department of Justice and the Department of the Solicitor General of Canada was issued in May, 2003 to advise the public on current trends and developments in Identity Theft. It warns that "many criminals who want to obtain personal data from people online use a technique known as "spoofing": the creation of e-mails and websites that appear to belong to legitimate businesses, such as financial institutions or online auction sites." http://www.usdoj.gov/opa/pr/2003/May/publicadvisory1.pdf
June, 2003	OCIR	BITS: "External Hackers". "Hackers establish look-alike web sites that entice unsuspecting consumers to post sensitive information."[2] http://www.bitsinfo.org/bitsidtheftwhitepaper.pdf (P. 16)
June, 2003	NIR	BITS: "Financial Identity Theft: Prevention and Consumer Assistance".[2] This report was described in a July 15, 2003 article in the Wall Street Journal, "Finance and Tech Groups To Combat Identity Theft". The WSJ reported that two of the major recommendations are that banks (1) set up a single point of contact within each company for reporting identity theft and (2) "share on an ongoing basis successful fraud prevention strategies in areas that include: Account opening and online transactions, Monitoring Controls, Loss tracking and reporting, Personnel training to detect suspicious activity". http://www.bitsinfo.org/bitsidtheftwhitepaper.pdf
June 26, 2003	NIR	Senator Feinstein introduced Senate Bill 1350, Notification of Risk to Personal Data Act, to set a national standard for notification of consumers when a database breach occurs. This is modeled after the new California law.
June 30, 2003	NIR	BITs "Fraud Reduction Guidelines, Strategies For Identity Theft Prevention and Victim Assistance". "Mission - Members of The Financial Services Roundtable and BITS are committed to creating and implementing a set of efficient, effective and consistent procedures to restore a victim's financial identity and to prevent ongoing incidences of identity theft. To that end we, the participating financial institutions, agree to share and implement the following successful strategies." "Prevention and Victims Assistance." http://www.bitsinfo.org/bitsfraudguidelinesJULY03.pdf

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

July 1, 2003	NIR	California's "Notice of Security Breach - Civil Code Sections 1798.29 and 1798.82 (Calif.)" mandates, as of 7-1-03, public disclosure of computer security breaches in which confidential information of any California resident may have been vulnerable.
July 22, 2003	OCIR	WSJ: "Identity-Theft Scam Rises on Web". "Federal officials warned consumers about an increasingly common Internet scam ("phishing") in which identity thieves use e-mails to lure consumers to bogus Web sites where they are tricked into revealing credit-card numbers and other personal information."
Aug. 12, 2003	NIR	The August 12, 2003 "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" from the OCC, FRB, FDIC, and OTS (the Agencies) is also focusing on identity theft risks arising from system failures or internal security breaches. www.federalreserve.gov/boarddocs/press/bcreg/2003/20030812/attachment.pdf

[illegible]

Further information on the most relevant and recent initiatives is presented below. The Network Identity Theft initiatives are the dominant themes within the:

- recent legislation in California and the US Senate,
- recent publications issued by BITS, the banking industry's eCommerce consortium,
- August 12, 2003 Interagency Guidance from the US banking regulators.

Interestingly, on the other side, the Banking Regulators have issued a series of guidelines addressing the issue of Online Corporate Identity Theft per our Addendum 1 but, based on our research, these guidelines have been largely overlooked or ignored.

[illegible]

Banking Regulators that include the FDIC, OCC and BIS have issued a series of alerts and guidelines from October 1999 through March 17, 2003 for banks to protect their corporate identities on the Internet by registering matching domain names and monitoring for illegal uses of their corporate brands. Based on our research in Study #2 and Study #3, the majority of the banks in our study are not following the recommended guidelines of registering matching domain names and monitoring and stopping potentially confusing web sites. (Reference Addendum 1).

Recent initiatives for the Network Identity Theft issues include:

[illegible]

Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. Pretexting is against the law. Under a new federal

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

law - the Gramm-Leach-Bliley Act - it's illegal for anyone to:

- use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost, or stolen documents.

Pretexting can lead to "identity theft." Identity theft occurs when someone hijacks your personal identifying information to open new charge accounts, order merchandise, or borrow money. Consumers targeted by identity thieves usually don't know they've been victimized until the hijackers fail to pay the bills or repay the loans, and collection agencies begin dunning the consumers for payment of accounts they didn't even know they had.

This law, operative July 1, 2003, requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The law requires an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified.

On June 26, 2003, Senator Feinstein introduced Senate Bill 1350, "The Notification of Risk to Personal Data Act". "This would set a much needed national standard for notification of consumers when a database breach occurs. The legislation would:

- require a business or government entity to notify an individual when there is a reasonable basis to conclude that a hacker or other criminal has obtained unencrypted personal data maintained by the entity;
- define as personal data an individual's Social Security number, driver's license number, state identification number, bank account number, or credit card number;
- subject entities that fail to comply with fines by the Federal Trade Commission of $5,000 per violation or up to $25,000 per day while the violation persists.
- and allow California's new law to remain in effect, but preempt conflicting state laws, so as not to put companies in a situation that forces them to comply with database notification laws of 50 different states."

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

BITS is a nonprofit industry consortium of the largest 100 financial institutions in the United States. Serving as the strategic "brain trust" for the industry, BITS focuses on issues related to e-commerce, payments and emerging technologies. (Source: www.bitsinfo.org).

The strategic focus of this organization is essentially on 2 of the 3 components of the Internet, i.e., promoting and developing safe and secure transaction systems within the Internet for the benefit of online consumers. Specifically, "BITS' mandate is to:

- Facilitate the growth of electronic banking and financial services
- Facilitate development of superior, market-driven technologies
- Maintain the industry's role at the heart of the payments system as e-commerce evolves
- Sustain consumer confidence and trust by ensuring the safety, soundness, privacy, and security of financial transactions
- Leverage resources and infrastructure across the industry."

We agree with BITS' broad definition of Identity Theft on page 9 of its June, 2003 White Paper, i.e., "Identity theft is the unlawful capture and use of another's personal identifying information (name, address, date of birth, Social Security number, account information, mother's maiden name or other family identifiers)."[2]

From a macro point of view, we believe it is important to have a common understanding that Identity Theft on the Internet is a complex issue due to the complexity of the Internet and a comprehensive solution for addressing this issue needs to attack and address each of the major sources of this problem within the Internet, i.e. the systems, content and perpetrators of these actions. Based on this perspective, we believe our recommendations and research compliment the research activities of BITS as we are focused on content risks and BITS is focused primarily on system risks. Combining our recommendations with those of BITS will lead, we believe, to a more complete strategy for addressing Identity Theft risks on the Internet for consumers.

In its June, 2003 White Paper on the issue of identity theft, "Financial Identity Theft: Prevention and Consumer Assistance[2], BITS' begins to address, on page 16, certain content risks as well as system risks as it lists the most common methods of online and offline Identity Theft. For the online Identity Theft it references these sources of:

- **System Risk, i.e.,**
  - **External Hacking** where "Hackers can penetrate company networks and internal systems, such as a Web site, and walk away with a large listing of customer names and account information."

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

- "**Intercepting sensitive information** – Hackers can access clear text (unencrypted) information from Internet transactions."
- **Content Risk. i.e.,**
  - "**Use of personal Web sites** – Personal Web sites can provide a host of information about an individual from which identity thieves can draw."
  - "**External hacking** –In some instances the hackers establish look-alike Web sites that entice unsuspecting customers to post sensitive information."

It then outlines a new voluntary set of guidelines for addressing system risks and consumer issues arising from identity theft. A July 15, 2003 article in the Wall Street Journal, "Finance and Tech Groups To Combat Identity Theft", describes this initiative as follows:

"Groups representing the nation's largest financial institutions and technology strategists plan to announce Tuesday a nationwide program to put the brakes on identity theft and help consumers and businesses that fall victim to it.
The Financial Services Roundtable, which is a group of the 100 top financial institutions, and BITS, which is a technology and business-strategy group, have agreed on a number of relatively simple steps that the two organizations say could go a long way toward stopping identity theft .
Topping the list are setting up a single point of contact within each company for reporting identity theft and using a uniform affidavit to report the crime to law-enforcement authorities. Customers of institutions that participate in the program won't have to fill out multiple forms with their banks, credit-card companies and others. Instead, a consumer who has been a victim of identity theft will have to fill out only one form, which will be sent to each company."

It also recommends a set of voluntary "Fraud Reduction Guidelines" that focus on system and transaction risks. It recommends that banks "share on an ongoing basis successful fraud prevention strategies in areas that include: Account opening and online transactions, Monitoring Controls, Loss tracking and reporting, Personnel training to detect suspicious activity".

There are, however, no specific recommendations within these two White Papers for addressing the risks of identity theft from the **content** of the Internet. Based on our research, banks should immediately adopt a proactive, common strategy for building safe eBusiness Brands™ that will:

- prevent as well as identify, attack and correct the fraudulent use of their brands within the content of the Internet.
- educate online consumers about the risks of corporate identity theft and fake web sites.

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

The August 12, 2003 "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" from the OCC, Federal Reserve Board, FDIC, and OTS (the Agencies) is also focusing on identity theft risks arising from system failures or internal security breaches as it relates to the Internet.

The 25 page document defines clear, broad objectives on page 4 for its Security Guidelines (see below) but then on pages 20 and 21 narrowly defines, to the exclusion of Online Corporate Identity Risks, 5 examples of identity theft that require notice to be given to the customer. In our opinion, Online Corporate Identity Theft, as defined by the Department of Justice and the FDIC, should be included in the risk group requiring notice to be given to the customer.

Security Guidelines (Page 4):
The Security Guidelines direct financial institutions to: (1) identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3) assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

"Examples of When Notice Should be Given" (Pages 20-21):
An institution should notify affected customers when it is aware of the following incidents unless the institution, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers.

- An employee of the institution has obtained unauthorized access to *sensitive customer information* maintained in either paper or electronic form;
- A cyber intruder has broken into an institution's unencrypted database that contains *sensitive customer information*;
- Computer equipment such as a laptop computer, floppy disk, CD-ROM, or other electronic media containing *sensitive customer information* has been lost or stolen;
- An institution has not properly disposed of customer records containing *sensitive customer information*; or
- The institution's third party service provider has experienced any of the incidents described above, in connection with the institution's *sensitive customer information*.

In our opinion, based on our 3 Studies in this report, "Examples of when Notice Should be Given", needs to include a reference to Online Corporate Identity Risks that cover fake, fraudulent web sites, domain names and other uses of bank brands by third parties for defrauding unsuspecting online consumers of their sensitive customer information.

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

We are mentioning this article within this report for the simple purpose of including another perspective on the importance of understanding and addressing the Internet and in using new technology to address the issue of online corporate identity theft within the content of the Internet.

This article[3] was written by: "Diane Karpman, a California ethics expert. [sic] She represents attorneys before the California State Bar, handles risk management for firms, and is frequently retained as an expert witness in legal malpractice, conflicts of interest, and related matters."

"We lawyers are on a precipice. The standard of care imposing liability on lawyers for legal malpractice is changing owing to the increasing use of computers. Internet accessibility is about to profoundly change our research obligations, since vast amounts of information are readily available to everyone, including courts and clients."

We encourage readers interested in this article to read the full report online[3].

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

[illegible]
Our research shows there are significant unmitigated risks for the banks and their online clients as it relates to the fraudulent use of bank brands within the content of the Internet. The lack of attention to this issue by the banks and possibly by the legal community is facilitating a rapid and unchecked growth of risks as shown by our research in Study #2 and Study #3. Our research is presented below.

[illegible]	
This study was prepared with 3 levels of Risk Analysis:	
Study 1:	This is a Global Review by Country of the 139 Banks that have submitted UDRP claims from late 1999 through 1st Q 2003. Banks in North America are listed by name in Table 1.
[illegible]	This is a study to determine how well 50 leading banks in North America have protected their live, unique, text-based trademarks through UDRP claims and a matching .com domain name. The 50 banks in this study own the 50 largest USPTO (United States & Patent Trademark Office) trademark portfolios amongst North American Banks and Brokerage firms as of March 31, 2003. There are a total of 3,964 live, unique text-based trademarks in this study as of March 31, 2003.
Study 3:	This is a deeper analysis of the content of the internet using the TrademarkBots® Internet Search Technology to discover additional trademark infringements for selected priority brands of the 50 banks. Examples of priority brands that are protected by live, federal USPTO trademarks but are owned as a domain name and marketed on the content of the Internet by third parties include: bankonecreditcard.com, chasemanhattan.com, citicorps.com, lehmanbrothers.com, mellon.net, northerntrust.info, pncbanking.com, royalbankofcanada.com, retirementplanwellsfargo.com, schwabmortgagecenter.com, suntrust-banks.com, and thekeybank.com. Each domain name could be used in fraudulent email campaigns and/or redesigned to steal personal identity assets. Resource: www.eBusinessTrademarkReports.com.

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Case #	Complainant	Domain Name	Complaint/Risks
D2003-0103	NASDAQ	Nasdaq.com	Complainant claims that the domain name <nasdasq.com> has been, or is being, used by Respondent in bad faith, particularly by directing visitors to a website at least in potential competition with Complainant's business.
133632	MBNA	MBNAaccess.net	Respondent uses the infringing <mbnaaccess.net> domain name to misdirect Internet users to its own website. Complainant asserts without contest that this redirection is motived by profit, either from commissions for pop-up advertising or referral fees for websites that the disputed domain name links to. The Panel agrees. This diversion of Internet consumers, done for commerical gain, qualifies as bad faith use and registration of a domain name under Policy.
128653	Freddie Mae	FreddyMae.com	Respondent uses the domain name to divert Internet traffic to a website that offers mortgage-related services.
118174	Bank of America	BankofAmerica.com	Respondent is using the disputed domain name in order to divert Internet users to a website that advertises a credit card. It can be inferred that Respondent is receiving some type of commercial revenue for diverting Internet traffic to the <superinternetdeals.com/creditcards.html> website. The use of a domain name confusingly similar to Complainant's mark in order to divert Internet users to an unconnected advertising website is

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

			not considered to be in connection with a bona fide offering of goods or services pursuant to Policy ¶ 4(c)(i), or a legitimate noncommercial or fair use pursuant to Policy ¶ 4(c)(iii).
D2001-0626	Royal Bank of Scotland	RoyalBankofScotland Tenerife.com	The Complainants use their web site to advertise their banking and financial services, to provide online banking services, and information about the Complainants and their services. One potential use for any web site set up by the Respondent at the <royalbankofscotlandtenerife.com> address, would be to advertise or sell services, which compete with those, provided by the Complainants. Any such use would result in the Complainants losing business and could cause damage to the Complainants and their customers if the Respondent's services were shoddy.
D2002-0672	Royal Bank of Canada	RBCalliancebank.com	The Complainant says that on June 24, 2002, it received an email from a Mr. Hyatt, inquiring as to whether the Complainant was in any way affiliated with RBC Alliance Bank. A copy of this email was annexed to the Complaint. The email said that, while the operators of the [Respondent's] website claimed to be a foreign exchange brokerage based in Switzerland, an Internet check done by Mr. Hyatt showed the website as listed to an individual in New York. The email stated that Mr. Hyatt had sent them over $20,000 to trade foreign exchange, but that "now no-one answers the phone and I do not get a reply to my emails".

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

			The email went on to express Mr. Hyatt's view that, if the operators of the [Respondent's] website were not associated with the Complainant, they were defrauding the public with the Complainant's name. As the email put it: "making it seem like they are in an 'alliance' with RBC".
135012	Bank of America	BankofAmericacom.com	Respondent's <bankofamericacom.com> domain name hosts a website which features sexually oriented material. Respondent either gains direct commercial profit from this website, or earns referral fees from the owners of the content.
D2001-0637 and D2001-0639	Union Bank of Switzerland	UBS-privatebanking.com and MarcelOspel.com (CEO of UBS)	On these websites, it (Respondent) has published material making grave allegations against the Complainant, including money laundering and forgery. The Respondent acknowledges that the domain name <ubs-privatebanking.com> is confusingly similar to the Complainant's mark and that the domain name <marcelospel.com> is identical to the name of the President of the Complainant. The Respondent refers to a domain name <marcel-ospel> owned by a French registrant, where the relevant website contains material critical of the Complainant and/or Mr. Ospel.

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Study #1: Global UDRP Analysis

A Global Review by Country of the 139 Banks that have submitted UDRP claims. Banks in North America are listed by name in the fee-based Table.

Study # 1:	Analytical Function	Universe of Study	Summary Results
	UDRP:	4,000 Banks	139 Banks and Finance Firms from 30 Countries

Fact 1: There are **4,000 global banking institutions** in The Financial Times' online database. (http://www.thebanker.com/database_frameset.html)

Fact 2: The Uniform Domain Name Dispute Resolution Policy (UDRP) was adopted on August 26, 1999 by ICANN to help trademark owners protect their intellectual property rights and online businesses from unfair competition by third parties. (http://www.icann.org/udrp/udrp-policy-24oct99.htm)

Fact 3: The UDRP filing cost for 1 domain name with 1 panelist ranges from $1,150 (NAF) to $1,500 (WIPO).
($1,150: 1 domain, 1 panelist) http://www.arb-forum.com/domains/UDRP/fees.asp
($1,500: 1 domain, 1 panelist) http://arbiter.wipo.int/domains/fees/index.html

Conclusions:

- Global UDRP activity has produced 5,032 cases (1999 to May, 2003).
- Only 6% or 278 of the 5,032 cases are from banking and finance companies. 100% of the 278 cases, in turn, have been submitted by:
  - 139 banks and finance companies located in 30 countries around the world covering 467 domain names. Further study shows only:
    - 43 or 31% of the 139 banks are from North America as shown in Table 1. A further review shows that only:
      - 17 of the 43 banks from above are also in [redacted] of the 50 largest trademark banking portfolios. Table 1 lists these 17 banks as well as the remaining 33 banks from [redacted] that have not yet submitted a UDRP case.
- UDRP activity from North American banks should be growing significantly, considering that:
  - there are 9,314 deposit-taking institutions in the US and
  - third parties, and not the banks, own 34% or 1,352 of the matching .com domain names for 1,352 of the 3,964 live, unique trademarks within [redacted]. Each case is contributing, at least, to brand confusion for online consumers. Furthermore, a timeline analysis presented in [redacted] shows this is a rapidly growing problem as 45% of these cases occurred in the 5 most recent quarters ending 3-31-03.

 © 2003 All Rights Reserved

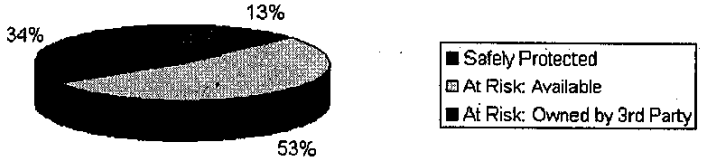
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

This is a study of the 50 largest USPTO (United States & Patent Trademark Office) trademark portfolios owned by North American Banks and Brokerage firms, as of March 31, 2003, to determine how well each of the 50 banks have protected their live, unique, text-based trademarks through UDRP claims and a matching .com domain name. There are 3,964 live, unique text-based trademarks in this study as of 3-31-03.

Based on this study, we discovered that:

- only 17 or 34% of the 50 largest banks in North America have used the UDRP process per Study #1 and [redacted] This also means that the majority or 66% of the 50 banks or 33 banks have not yet used the UDRP process to protect their brands.

- 87% of the 3,964 live, unique text-based trademarks are at risk for cybersquatting on the internet as the matching .com domain names are either Owned by a Third Party [redacted] or were Available [redacted] for registration as a matching .com domain as of April 31, 2003. Only 13% or 519 of the trademarks were Safely Protected [redacted] by a matching .com domain by the rightful bank.



  - **13% or 519** of the trademarks were Safely Protected [redacted] by a matching .com domain owned by the rightful bank.
  - **53% or 2,093** of the trademarks were Available [redacted] due to inaction by the 50 banks, for Registration by any party.
  - **34% or 1,352** matching .com domain names were Owned by a Third Party [redacted]. (Study #1: 33 of the 50 banks have not yet filed UDRPs.)

- A Timeline Analysis of the foregoing risks on the 3,964 trademarks from the 1980's, 1990's and each of the years of 2000, 2001, 2002 and 2003 (thru March, 31, 2003) shows, in the following chart, a

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

consistent risk pattern in each of the 3 risk categories in each year through the end of our study as of 3-31-03.

Year(s)	Total TM's	Owned by a Third Party	Available	Safely Protected
1980's	43	23	14	6
1990's	1,015	393	540	82
2000	424	134	240	50
2001	560	183	294	83
2002	**1,264**	411	655	198
2003 (3/31/03)	**658**	203	355	100
Total	3,964	1,352	2093	519
%	100%	34%	53%	13%
1980's	100%	53%	33%	14%
1990's	100%	39%	53%	8%
2000	100%	32%	57%	12%
2001	100%	33%	53%	15%
2002	100%	33%	52%	16%
2003 (3/31/03)	100%	32%	53%	15%
Total	3,964	34%	53%	13%

This analysis:

- reinforces our conclusion that the majority of the Top 50 banks have not yet adopted a sensible policy for protecting either their corporate identities or their online clients from online corporate identity theft.
- shows **this problem is rapidly growing** as 48% or 1,922 of the 3,964 trademarks in this study have been recently submitted in 2002 and the 1st quarter of 2003. If this trend continues for the remainder of 2003 and into 2004 and the banks continue with their historical brand protection strategies, then the banks and their online clients will be subject to even greater online identity theft. **This is our real concern.**
- is based on the consolidated results of the 3,964 trademarks from each of the 50 banks and brokerage firms in this study. **Individual studies** for each of the 50 banks and brokerage firms may be purchased online: www.eBusinessTrademarkReports.com.

- Potential economic losses associated with the 1,352 matching .com domain names Owned by 3rd Parties for the Top 50 banks include:
  - UDRP fees of $1,554,800 or $1,150 for each of the 1,352 domain names.
  - Lost online sales on 34% of their brands/trademarks due to

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

[redacted]	customer confusion with matching third party www sites. o Privacy losses and related financial losses for consumers who are duped by third party www sites that match their bank's trademark. o Potential economic losses associated with the 2,093 matching .com domain names, that are Available [redacted] for registration, include: o Lost online sales on 53% of their brands/trademarks. o UDRP fees approaching $2,406,950 or $1,150 for each of the 2,093 matching .com domains, should they all be registered by 3rd parties and then, subsequently, all reclaimed by the banks.
[redacted]	To reverse these trends, banks need to create a safer online environment for their consumers and lower the risk and related expenses of online identity theft with a proactive, cost-effective strategy centered on our recommended eBusiness Brand™ strategy.

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Study #3: A Deeper Analysis using TrademarkBots® Internet Search Technology	
	For a deeper analysis of the content of the internet for trademark infringements on priority brands, we recommend using the TrademarkBots® Search Technology or a service with similar search and reporting capabilities. Our search technology is widely available for the public through www.Hoovers.com on each Company Capsule Page and through www.eBusinessTrademarkReports.com. Search fees begin @$20.

Enter your business name here [illegible]

Please check the reports you would like to receive and click the "Buy Now" button at the bottom of the page.

Trademark Intelligence				
ITR	International Trademarks	Sample	☐	$75
DNEMR	Domain Names - Exact Matches	Sample	☐	$65
DNPMR	Domain Names - Partial Matches	Sample	☐	$65
VWR	Visible Web	Sample	☐	$20
MR	Metatag	Sample	☐	$150
UDRPR	Uniform Domain Name Dispute Resolution Policy Cases	Sample	☐	$20
Brand Intelligence				
SDR	Specialty Databases (FDA)	Sample	☐	$35
NR	Newspapers	Sample	☐	$25
UR	Usenet	Sample	☐	$25
MBR	Message Boards	Sample	☐	$25
WFR	Webfeeds	Sample	☐	$25
PCR	Publication and Catalogs	Sample	☐	$28
CPR	Customized Portfolio Research	Sample	Contact TmBots	

Buy Now!

Examples: Domains owned by 3rd parties that are similar to bank TMs.	bankonecreditcard.com, chasemanhattan.com, citicorps.com, lehmanbrothers.com, mellon.net, northerntrust.info, pncbanking.com, royalbankofcanada.com, thekeybank.com, suntrust-banks.com, retirementplanwellsfargo.com, and schwabmortgagecenter.com. Each domain name is already active and could be used in fraudulent email campaigns and/or redesigned to steal personal identity assets. (These examples are as of July 27, 2003.)
Conclusion:	Unfair competitors are using bank trademarks in many content locations of the Internet to confuse bank customers and the banks have been slow to embrace the best business practices and technology to stop these risks.

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Final Observations:	
	Banks can create a safer online environment for their consumers and lower the risk and related expenses of online identity theft with a proactive, cost-effective strategy centered on our recommended eBusiness Brand™ strategy.
Disclaimer:	Our firm provides trademark monitoring services.

Recommended eBusiness Brand™ Strategy to Limit Online Corporate Identity Theft:

In order to create a safer online environment and to prevent personal identity theft from the misuse of brands within the content of the internet, each business, including the 9,000 US banks and the 4,000 banks in the TheBanker.com's database, should be proactive and:

1. Register each primary brand as a trademark in every country of operation in order to fight the misuse of brands within those countries and within the content of the internet.
2. Register matching domain names for trademarks in order to prevent cybersquatting and subsequent personal identity theft and UDRP filings ($1,150 per domain name).
3. Monitor the content of the Internet to identify and stop the fraudulent use of corporate identities with today's technology. (Our search technology is widely available for the public through www.Hoovers.com on each Company Capsule Page and through www.eBusinessTrademarkReports.com. Search fees begin @$20.)
4. Fight trademark infringements and, when needed, use UDRP filings.
5. Disclose, for online consumers, the potential risks of corporate identity theft and endorse a common standard for safe brand management on the Internet.

In effect, each business needs do their part to protect their brands and online consumers.

Best Business Practices:

1. Empower a brand champion for protecting your online corporate identity (and customers).
2. Generate an ROI of 115x's by investing the cost of 1 UDRP filing, i.e., $1,150, towards the registration of 115 matching domain names (at approximately $10 per year per domain name). This will boost sales and prevent 115 potential UDRP Cases with a total cost of $132,250 and potential privacy losses for the bank and its clients. (115x's = Cost savings of $132,250/Investment of $1150).
3. Create operational efficiencies by consolidating the online brand functions (trademark and domain name registration and brand monitoring) with a smaller team dedicated to the goal of building strong, online brands.

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Reports Available for Purchase include:	
$1,250 per each of the 50 Bank Reports.	50 Individual Bank Reports: Online Corporate Identity Risks: North America: March 31, 2003. Each Bank Report is approximately 27 pages. (Risks were rechecked as of July 31, 2003 and no significant changes were noted.) A sample Bank Report is available online with the Order Form. Reports may be purchased as of August 14, 2003 either at www.OnlineCorporateIdentityRisks.com or within www.Hoovers.com at these locations: o on each Bank Capsule Page o the Participating Vendor Page: www.hoovers.com/global/ecommerce/vendors/index.xhtml#TRADEMARKBOT

August 14, 2003
TrademarkBots.com, Inc.

 © 2003 All Rights Reserved
TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

Table 1
Online Corporate Identity Risks
Banking and Finance
Global & North America – May, 2003

Study 1: Global UDRP
UDRP Study: 139 Banks from 30 Countries

	Country	# of Banks	Market Share	UDRP Bank	[illegible]
1	Argentina	1	1%		
2	Australia	3	2%		
3	Belgium	2	2%		
4	Brazil	3	2%		
5	Canada	3	2%	Yes (1/43)	[illegible]
				Yes (2/43)	The Toronto-Dominion Bank
				Yes (3/43)	Westminster Savings Credit
6	Chile	2	2%		
7	China	2	2%		
8	Columbia	3	2%		
9	Denmark	1	1%		
10	France	4	3%		
11	Germany	5	4%		
12	Guatemala	1	1%		
13	Hong Kong	2	2%		
14	India	1	1%		
15	Italy	1	1%		
16	Japan	1	1%		
17	Lebanon	1	1%		
18	Luxembourg	1	1%		
19	Mexico	1	1%		
20	Netherlands	2	1%		
21	New Zealand	1	1%		
22	Saudia Arabia	1	1%		
23	Spain	23	17%		
24	Sweden	1	1%		
25	Switzerland	10	8%		
26	Taiwan	1	1%		

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

27	Turkey	2	2%		
28	UK	19	14%		
29	United Arab Emirates	1	1%		
30	USA	40	30%	(See Below)	[redacted]
30	-----Totals------	139	100%		[redacted]
	40 UDRP USA Banks:				These banks are in both studies.
	N.A.M. - UDRP Bank			Yes - 4/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 5/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 6/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 7/43	[redacted]
	Country	# of Banks	Market Share	UDRP Bank	[redacted]
	N.A.M. - UDRP Bank			Yes - 8/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 9/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 10/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 11/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 12/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 13/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 14/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 15/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 16/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 17/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 18/43	[redacted]
	N.A.M. - UDRP Bank			Yes - 19/43	[redacted]

	Country	# of Banks	Market Share	UDRP Bank	(These firms have submitted UDRPs but are not large enough to be in the Top 50 Study.)
	N.A.M. - UDRP Bank			Yes - 20/43	Ameritrade Holding
	N.A.M. - UDRP Bank			Yes - 21/43	Boardwalk Bank
	N.A.M. - UDRP Bank			Yes - 22/43	Chicago Mercantile Exchange
	N.A.M. - UDRP Bank			Yes - 23/43	Chittendon Corporation
	N.A.M. - UDRP Bank			Yes - 24/43	Christiana Bank and Trust
	N.A.M. - UDRP Bank			Yes - 25/43	DaimlerChrysler Corporation
	N.A.M. - UDRP Bank			Yes - 26/43	Direct Line Group LTD
	N.A.M. - UDRP Bank			Yes - 27/43	DLJ
	N.A.M. - UDRP Bank			Yes - 28/43	Dollar Financial Group
	N.A.M. - UDRP Bank			Yes - 29/43	Emoney
	N.A.M. - UDRP Bank			Yes - 30/43	Federal Home Loan
	N.A.M. - UDRP Bank			Yes - 31/43	Federal National Mortgage
	N.A.M. - UDRP Bank			Yes - 32/43	First American Funds
	N.A.M. - UDRP Bank			Yes - 33/43	HEMAR Insurance Corporation
	N.A.M. - UDRP Bank			Yes - 34/43	IndyMac, Inc.
	N.A.M. - UDRP Bank			Yes - 35/43	LTD Commodities

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

	N.A.M. - UDRP Bank			Yes - 36/43	MasterCard International
	N.A.M. - UDRP Bank			Yes - 37/43	NASDAQ
	N.A.M. - UDRP Bank			Yes - 38/43	Plymouth Savings Bank
	N.A.M. - UDRP Bank			Yes - 39/43	Regions Financial
	N.A.M. - UDRP Bank			Yes - 40/43	Southern Bank
	N.A.M. - UDRP Bank			Yes - 41/43	T. Rowe Price Associates
	N.A.M. - UDRP Bank			Yes - 42/43	The Vanguard Group
	N.A.M. - UDRP Bank			Yes - 43/43	Transamerica Corporation

	Country	# of Banks	Market Share	UDRP Bank	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]
				No UDRPs	[redacted]

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

				No UDRPs	[redacted]
				No UDRPs	
				No UDRPs	
				No UDRPs	
				No UDRPs	
				No UDRPs	
				No UDRPs	

 © 2003 All Rights Reserved

TrademarkBots.com, Inc.
5100 Tamiami Trail North – Suite 105, Naples, Florida 34103
t-239-434-3850 – f-239-642-9115
www.TrademarkBots.com

TrademarkBots®

eBusiness Brands™ and eBusiness Trademarks™

A Current Risk Assessment

March 18, 2003

Reputation Risks and related Legal Risks on the Internet: Banking Industry

Addendum 1

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

TrademarkBots®

eBusiness Brands™ and eBusiness Trademarks™

A Current Risk Assessment
March 18, 2003
Reputation Risks and related Legal Risks on the Internet: Banking Industry

Introduction:

The following quotes from the OCC (dated 3-17-03) and Bank For International Settlements (dated May, 2001) set the stage for our presentation on pages 3-8. These principles, in our opinion, accurately define the macro-economic risks presented by the Internet but they do not fully reflect the convergence of Reputation and Legal Risks on the Internet nor the current technology or Best Business Practices to address these risks in a cost-effective and timely manner. This Current Risk Assessment will address these issues and provide related recommendations.

The OCC, the National Bank Charter, & Current Issues Facing the National Banking System[1] (News Release 2003-21, March 17, 2003, www.occ.treas.gov)

"We, and the banking industry, are keeping a closer watch on how banks identify, assess and address activities or transactions that pose reputation risk to the Bank".

Risk Management Principles for Electronic Banking[2]
Basel Committee Publications No. 82, May 2001, Executive Summary

"Continuing technological innovation and competition among existing banking organizations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and wholesale customers through an electronic distribution channel collectively referred to as e-banking. However, the rapid development of e-banking capabilities carries risks as well as benefits.
The Basel Committee on Banking Supervision expects such risks to be recognized, addressed and managed by banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology. While not creating inherently new risks, the Committee noted that these characteristics increased and modified some of the traditional risks associated with banking activities, in particular strategic, operational, legal and reputational risks, thereby influencing the overall risk profile of banking.
Based on these conclusions, the Committee considers that while existing risk management principles remain applicable to e-banking activities, such principles must be tailored, adapted and, in some cases, expanded to address the specific risk management challenges created by the characteristics of e-banking activities. To this end, the Committee believes that it is incumbent upon the Boards of Directors and banks' senior management to take steps to ensure that their institutions have reviewed and modified

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

where necessary their existing risk management policies and processes to cover their current or planned e-banking activities. The Committee also believes that the integration of e-banking applications with legacy systems implies an integrated risk management approach for all banking activities of a banking institution.

To facilitate these developments, the Committee has identified fourteen *Risk Management Principles for Electronic Banking* to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities.

These *Risk Management Principles* are not put forth as absolute requirements or even "best practice." The Committee believes that setting detailed risk management requirements in the area of e-banking might be counter-productive, if only because these would be likely to become rapidly outdated because of the speed of change related to technological and customer service innovation. The Committee has therefore preferred to express supervisory expectations and guidance in the form of *Risk Management Principles* in order to promote safety and soundness for e-banking activities, while preserving the necessary flexibility in implementation that derives in part from the speed of change in this area. Further, the Committee recognizes that each bank's risk profile is different and requires a tailored risk mitigation approach appropriate for the scale of the e-banking operations, the materiality of the risks present, and the willingness and ability of the institution to manage these risks. This implies that a "one size fits all" approach to e-banking risk management issues may not be appropriate.

For a similar reason, the *Risk Management Principles* issued by the Committee do not attempt to set specific technical solutions or standards relating to e-banking. Technical solutions are to be addressed by institutions and standard setting bodies as technology evolves. However, this Report contains appendices that list some examples current and widespread risk mitigation practices in the e-banking area that are supportive of the *Risk Management Principles*.

Consequently, the *Risk Management Principles* and sound practices identified in this Report are expected to be used as tools by national supervisors and implemented with adaptations to reflect specific national requirements and individual risk profiles where necessary. In some areas, the Principles have been expressed by the Committee or by national supervisors in previous bank supervisory guidance. However, some issues, such as the management of outsourcing relationships, security controls and legal and reputational risk management, warrant more detailed principles than those expressed to date due to the unique characteristics and implications of the Internet distribution channel.

The *Risk Management Principles* fall into three broad, and often overlapping, categories of issues that are grouped to provide clarity: *Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management*."[2]

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

TrademarkBots®

eBusiness Brands™ and eBusiness Trademarks™

A Current Risk Assessment

March 18, 2003

Reputation Risks and related Legal Risks on the Internet: Banking Industry

Objective of the Current Risk Assessment	To provide: o an analysis, as of March 18, 2003, on the current state of Reputation Risks and related Legal Risks on the Internet for the Banking Industry. o a revised definition of Reputation Risks and related Legal Risks on the Internet. o a Best Business Practice Guide.
Executive Summary	o The growth of the Internet and new technology has spawned a combination of new communication and publication channels for the public, including unfair competitors, on the Internet, as well as, technology to automatically research and monitor for Reputation Risks and related Legal Risks on the Internet. o The current Alerts and Guidance documents from the BIS, Federal Reserve and the OCC should be updated to clearly define Reputation Risks and related Legal Risks on the Internet along with a Best Business Practice for addressing these risks.
New Definition of Reputation Risks and related Legal Risks on the Internet	Reputation Risks and related Legal Risks on the Internet should be analyzed from the perspective that well-known reputations are embodied in a brand and brands are best protected by trademark law and a policy for building brands on the Internet. Based on this, o Reputation Risks on the Internet include the use by external parties of your name or brand or branded products in negative ways on the Internet to attract your stakeholders to their www sites, through unfair advertising, thus causing confusion, lost sales, potential privacy risks and dilution to your brand, trademark, and business. o The related Legal Risks include a range of trademark law violations, i.e., unfair advertising, cybersquatting, and brand dilution, as well as, privacy risks for your customers who unwittingly trust and conduct business with these unfair competitors. o A policy for building brands on the Internet should state that each brand be protected by a trademark and matching domain names in each country of operation along with a system for automatically researching, monitoring and addressing potential trademark violations on the Internet. [3] o Today's leading technology for monitoring potential trademark violations is comprehensive in scope, browser-based and cost-effective, thus providing a positive ROI.

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

A Current Risk Assessment
March 18, 2003
Reputation Risks and related Legal Risks on the Internet: Banking Industry

An Emerging Online Definition of Reputation Risk

- October, 1999, OCC: The Internet Handbook defines 14 Internet Risks, i.e., Credit Risk, Interest Rate Risk, Liquidity Risk, Price Risk, Foreign Exchange Risk, Transaction Risk, Compliance Risk, Strategic Risk, and **Reputation Risk.**[3] "**Reputation Risk** is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customers and the community. A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries, or violations of customer privacy expectations. **A bank's reputation can be damaged by Internet banking services that are poorly executed** or otherwise alienate customers and the public. Well-designed marketing, including disclosures, is one way to educate potential customers and help limit reputation risk. Customers must understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using the system. As such, marketing concepts need to be coordinated closely with adequate disclosure statements. A national bank should not market the bank's Internet banking system based on features or attributes the system does not have. The marketing program must present the product fairly and accurately. National banks should carefully consider how connections to third parties are presented on their Web sites. Hypertext links are often used to enable a customer to link to a third party. Such links may reflect an endorsement of the third party's products or services in the eyes of the customer. It should be clear to the customer when they have left the bank's Web site so that **there is no confusion about the provider of the specific products and services offered** or the security and privacy standards that apply…."[4]
- July 19, 2000, OCC: "This alert highlights **the need for banks to carefully select and protect their Internet addresses.**

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

Recently, several banks discovered Internet Web sites with Internet addresses similar to the addresses of their national bank Web sites. **This confusing situation resulted in some bank customers mistakenly transmitting confidential information to these other similar Web sites.**"[5]

- November, 2000, FDIC: "Protecting Internet Domain Names". **Risk Management Techniques** to prevent customer confusion, reputational harm, fraud and legal disputes, bank management can employ a number of practices and techniques. Timely registration and renewal of a bank's domain name(s) are important to assure that the bank acquires and retains ownership of the Internet addresses that it desires. Any lapses in registration could result in the loss of a domain name to another party. Bank management may choose to consider acquiring more than one domain name to retain control over the use of all similar names. However, this strategy may entail financial and administrative costs. Either way, institutions may benefit from conducting periodic Internet searches to determine whether there are names being used that are similar to their domain name, legal name or other trade/product names. In addition to similar domain names that have different suffixes (e.g., *bankname.com and bankname.net*), management also may want to look for variations in spelling and punctuation (e.g., *bankname.com and bank-name.com*).[6]
- May, 2001, BIS: "**Reputational Risk**: is one of three broad, and often overlapping, categories of issues. The other two are Board and Management Oversight and Security Controls. Source: "Risk Management Principles for Electronic Banking".[7]
- May, 2001, BIS: "Banks should also develop appropriate incident response plans, including communication strategies, that ensure business continuity, **control reputation risk** and limit liability associated with disruptions in their e-banking services".[8]
- May, 2001, OCC (NR 2001- 42): "Our goal is to alert financial institutions and their supervisors to the nature of risks in electronic banking. We expect bankers will put these principles to use as they develop their own customized approaches to risk mitigation. Of primary importance is the principle on effective management oversight of electronic banking activities. After all is said and done, management recognition of the risks inherent

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

in e-banking and the need for an integrated risk management system are fundamental if the specific risks…are to be properly controlled," said Comptroller Hawke.[9]

- July 31, 2002: "Restoring Trust" By Kenneth Thompson, CEO, Wachovia: "All of us are facing the challenge of a large and non-traditional risk. I am referring to **reputational risk.** I doubt the traditional job description for a risk manager makes that person responsible for managing reputational risk. But in my view that is the largest risk on our plates today. If you are managing any company, if you are an auditor, or a regulator-all of those have had their reputations damaged by scandals and misdeeds in corporate America. Every one of these situations must be investigated thoroughly and aggressively. Having fled the markets, investors will only return when they see wrongdoers paying serious consequences. That's what it will take to restore their trust."[10]
- 3rd Q, 2002, Federal Reserve, Philadelphia: "As defined in the Commercial Bank Examination Manual, for a financial institution, **reputation risk** is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.[11]
- The December, 2002 Information Security Risk by the FFEIC (Federal Financial Institutions Examination Council) refers to Reputation Risk associated with network security issues but not in relation to Corporate Identity Issues.[12]
- The March 17, 2003 OCC Paper titled "The OCC, the National Bank Charter, & Current Issues Facing the National Banking System" states: "we, and the banking industry, are keeping a closer watch on how banks identify, assess and address activities or transactions that pose reputation risk to the bank.[13]
- Note: "Reputation Risk" is not mentioned in the following:
  - 1999, Uniform Rating System for Information Technology - March 31, 1999.[14]
  - February 29, 2000, Information Technology Examination Frequency SR 00-3 (SUP).[15]

Some of Reputation Risk and related Internet Risks on

Reputation Risks and related Legal Risks on the Internet is a large and growing issue per:

- the World Intellectual Property Organization and their December, 2002 survey. "The World Intellectual Property

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

Organization (WIPO) has surveyed the far-reaching impact that digital technologies - the Internet in particular - have had on intellectual property (IP) and the international IP system. The study, entitled "Intellectual Property on the Internet: A Survey of Issues," (available at: http://ecommerce.wipo.int/survey/) is designed as an overview for all those interested in gaining a perspective on how intellectual property has been affected by digital technologies, and the pivotal role played by the IP system itself in supporting and promoting e-commerce globally." [16]
Key relevant quotes include: "(ii) DEVELOPMENTS IN USE OF TRADEMARKS ONLINE 124. Trademark owners also face new challenges with respect to use of their marks in the digital environment. In the current marketplace, it is estimated that a typical large business owns between 200 and 500 corporate, product and service identities, that need to be registered, maintained and defended.196 A corporate presence on the Internet requires trademark owners to defend their rights against new forms of trademark abuse and across millions of discrete sites, in multiple languages and domains. For example, trademarks and logos may be used in a site or domain name in connection with pornographic or other objectionable sites, or by trade competitors to divert search engine traffic, or dilute or tarnish a brand. 125. One provider of digital brand management services, VeriSign, estimates that 70% of domain names associated with top brands are not registered by the true brand owner, prompting rightsholders to defensively register their marks as domain names, and take action to protect their mark through domain name dispute resolution procedures, as described in Chapter III(c). In addition to cybersquatting, trademark owners are facing new types of infringement, including user-traffic diversion through keywords and meta tags, or unauthorized linking and framing, as described below. Added to this, the Internet has vastly increased consumer choice by making available a global spread of online enterprises which, together with a new diversity of media channels and increased consumer control, has contributed to an erosion of brand loyalty.197 In this environment, trademark owners may employ services

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.

	of online brand management and 'cybersurveillance' companies, that assist in the protection and enforcement of their trademark rights in a digital environment.[17] o research conducted by TrademarkBots.com showing that approximately 80% of the live, unique trademarks on file with the USPTO from high-economic values brands, studied by TrademarkBots.com, are at risk since the trademark owner does not own the matching .com domain name for a given trademark.[3] The magnitude of this risk is even greater as firms are also failing to register other matching Top Level and Country Level Domain names for each brand and matching trademark.
BEST Business Practice Guide	To address Reputation Risks and related Legal Risks on the Internet outlined herein and in the enclosed Corporate Identity Risks[18], we recommend banks and their clients adopt the 8 steps outlined in the guide to Building eBusiness Brands™ and eBusiness Trademarks™ (enclosed) [19] as a new standard of excellence or Best Business Practice Guide and to review this periodically as part of the Audit Committee function.

[1] www.occ.treas.gov/ftp/release/2003-21a.pdf (Page 15 of 15)
[2] www.bis.org/publ/bcbs82.htm#pgtop
[3] www.InternetBrandPolicy.com by TrademarkBots.com, Inc.
[4] www.occ.treas.gov/handbook/intbank.pdf
[5] www.occ.treas.gov/ftp/alert/2000-9.txt
[6] http://www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-77-2000-tech_bull_protect_internet_domain_name.pdf (P. 3 of 3)
[7] www.bis.org/publ/bcbs82.pdf. (Page 6 of 36)
[8] www.bis.org/publ/bcbs82.pdf. (Page 7 of 36)
[9] www.occ.treas.gov/ftp/release/2001%2D42.txt
[10] www.banktech.com/story/coverStory/BNK20021004S00151
[11] www.phil.frb.org/src/srcinsights/srcinsights/q3si1.html
[12] http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/information_security_low_res.pdf
[13] www.occ.treas.gov/ftp/release/2003-21a.pdf (Page 15 of 15)
[14] www.federalreserve.gov/boarddocs/SRLETTERS/1999/SR9908.HTM
[15] www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0003.HTM
[16] www.wipo.int/pressroom/en/releases/2002/p334.htm
[17] http://ecommerce.wipo.int/survey/pdf/survey.pdf (Page 65 of 202)
[18] "Corporate Identity Risks" by TrademarkBots.com.
[19] "Building eBusiness Brands™ and eBusiness Trademarks™" by TrademarkBots.com.

Copyright 2003. All rights reserved. TrademarkBots.com, Inc.