PROTECTING CUSTOMERS' PRIVATE DATA FROM MISAPPROPRIATION BY INSTITUTIONAL IDENTITY THIEVES

ROBERT A. BOURQUE
BLAKE A. BELL*
SIMPSON THACHER & BARTLETT LLP

SEPTEMBER 15, 2000

I. INTRODUCTION

On December 2, 1999, Reuters reported that a division of the Office of the New Jersey Attorney General had filed a lawsuit in New Jersey state court "against three men for allegedly duping on-line investors of $750,000 through an Internet stocktrading Web site they pretended belonged to MLC Ltd., a well-known Australian financial services company." According to Reuters, the eight-count complaint charged the men with using the Web site and printed brochures to dupe investors into sending $750,000 to them.[1]

The Reuters report served as a wakeup call to financial institutions throughout the country. Many realized, for the first time, that online institutional identity theft can place the personal data and financial assets of their customers and prospective customers at grave risk.

Institutional identity theft gained renewed attention recently when the Office of the Comptroller of the Currency issued an alert entitled Protecting Internet Addresses of National Banks in which it revealed that "[r]ecently, 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 transmitting confidential information to these other similar Web sites".[2]

While most financial institutions have devoted substantial time, attention and resources to protecting the privacy of their customers' personal data by safeguarding their computer systems against hacking by outsiders, not all have taken appropriate steps to reduce the risk of online institutional identity theft. Yet, such identity theft can present just as grave a risk to the privacy of customers' personal data. This article will summarize some of the techniques used by identity thieves as well as mechanisms that institutions may consider deploying to reduce the risk of institutional identity theft and further protect their customers from inadvertently disclosing private data to identity thieves.

---

* **Robert A. Bourque** *is a partner and* **Blake A. Bell** *is senior knowledge management counsel with Simpson Thacher & Bartlett in New York.*

II. MEANS OF INSTITUTIONAL IDENTITY THEFT

There are vastly different ways for unscrupulous operators to engage in online institutional identity theft. Most instances involve some form of manipulation of the domain name system that governs the Internet.

Institutions establish Internet addresses through registration of a domain name such as www.company.com with a domain name "registrar." Examples of domain name registrars include Network Solutions, Inc. and Register.com. When registering a domain name, an institution typically must provide the domain name registrar with the unique domain name that it wants to register (which no one else may have), the name of the registrant, contact information including a valid e-mail address and technical data about the computer server to which the domain name will "point".

There are several ways to manipulate the domain name process to facilitate institutional identity theft. Each will be discussed in turn in this article. They include typo-pirating, pagejacking, cybersquatting, domain name hijacking, online message board imposters, and domain name server intrusions.

A. Typo Pirating

So-called "typo pirates" rely on the natural tendency of Web surfers to mistype a well-established Web address. Perhaps the most famous such instance involving a financial institution used the domain "wwwpainewebber.com" – with no "dot" between the "www" and "painewebber.com." As is the case in so many such instances, the typo pirate pointed the domain to an adult-oriented Web site to the embarrassment of PaineWebber, which sued for trademark infringement and dilution. United States District Court Judge Claude M. Hilton of the Eastern District of Virginia granted PaineWebber injunctive relief against use of the domain.[3]

Other financial institutions found themselves the target of the same typo pirate. Citicorp and Morgan Stanley Dean Witter & Co. reportedly filed lawsuits against the same individual, alleging that he had registered more than fifty such typo-based domain names. Additionally, lawyers for Geico Insurance recently discovered that Geigo.com, as well as 50 other typo-based domains, transported Web surfers to sites maintained by Progressive Insurance, a Geico competitor. Progressive reportedly stated that it was not aware of the use of the "typo tactic."[4] The risk involving typo pirates is that they will craft a Web site that looks like the institution's. When challenged typists stumble across the site, they are solicited with what appear to be official requests to provide personal data including account passwords and the like.

B. Pagejacking

Another institutional identity theft technique involves so-called "pagejackers." In such instances, someone copies an institution's Web pages, changes them slightly to suit his or her

illicit purposes, posts those pages on the Web and registers the new pages with numerous search engines using keywords that suggest the pages are affiliated with the institution. When customers use those search engines looking for the institution's Web site, they inadvertently stumble across the fake site instead where, once again, they can be solicited to reveal private financial and personal data.

Pagejacking, like typo pirating, was pioneered by adult Web site operators. The tactic has become such a widespread problem in that arena that late last year the U.S. Federal Trade Commission brought a high-visibility enforcement action against alleged pagejackers. According to the FTC, the targets of its action copied and misused as many as 25 ***million*** Web pages including pages from sites such as the Harvard Law Review and the Japanese Friendship Garden in order to misdirect traffic to adult-oriented Web sites.[5]

C. Cybersquatting

One of the most common categories of domain name disputes also lends itself to identity theft. Typically, cybersquatting involves registering a domain name that is confusingly similar to an institution's name and then attempting to sell the name back to the institution. Occasionally, however, cybersquatted domains are used to attract people who inadvertently type the cybersquatted domain name rather than the actual domain name of the Web site they intend to visit. Perhaps the best known example of such a circumstance involves www.whitehouse.com -- an adult Web site that preys on many otherwise innocent people who are actually trying to visit www.whitehouse.gov.

Domain name disputes involving cybersquatters are legion. Indeed, the problem grew to such alarming proportions that late last year Congress passed, and President Clinton signed into law, the Anticybersquatting Consumer Protection Act.[6] That statute essentially makes it unlawful to register a domain name based on an organization's or an individual's name for the sole purpose of trying to obtain money in exchange for giving up the name.

D. Domain Name Hijacking

Domain name hijackings occur in a variety of different ways, but each seems to revolve around the issuance of a forged request to the domain name registrar seeking changes to the administrative contact, technical contact and computer server information that the true owner of the domain name provided to the registrar at the time the domain name was registered. For example, one technique involves the creation of a forged e-mail "header" made to look like the e-mail comes from the true owner of the domain name. The forged e-mail is sent to the registrar and typically requests that the registrar insert the identity thief (or the thief's alias) as the administrative and technical contacts and change the technical Domain Name System pointers so that Web surfers who type the domain name will now go to the thief's Web site rather than the Web site of the actual owner of the domain.

One recent and widely-publicized domain name hijacking involved shoe manufacturer Nike, Inc. In that instance, protesters successfully hijacked the Nike.com domain name and repointed it to an anti-Nike Web site operated by a social activist group.[7]

E. Imposters Posing as Company Officials

Another means of online identity theft that is emerging on the Web involves an imposter who poses as an official of the institution and makes postings to online message boards that would seem to have the imprimatur of the institution. Recently, for example, the New York Stock Exchange filed a lawsuit in the United States District Court for the Southern District of New York against unknown John Doe defendants who posed as Exchange Chairman Richard A. Grasso using aliases such as "richardgrasso" and "RichAGrasso" and posted messages about various companies on message boards maintained by Raging Bull, a financial message board host.[8]

Similarly, California securities regulators recently prosecuted and settled a lawsuit brought against a man who allegedly posed as Frank G. Mancuso, former Chairman and Chief Executive Officer of Metro-Goldwyn-Mayer, and posted messages on a message board devoted to the company. The negative messages, according to the regulators were part of an alleged scheme to manipulate the company's stock.[9]

F. Domain Name Server Intrusions

Another risk of loss of institutional identity online involves unauthorized intrusions into an institution's so-called domain name server, a computer that essentially routes online visitors to the correct computer containing the institution's Web site, among other things. In such instances, hackers infiltrate a poorly-secured domain name server and instruct the computer to reroute such visitors to a different location – one that might be designed to look like the institution's but may be used to capture customers' private data by asking them, for example, to confirm account information including passwords. This issue gained attention recently when the Office of the Comptroller of the Currency warned national banks that an "intrusion into a domain name server can result in a bank losing its online identity, even if a bank carefully selects and protects its domain names."[10]

III. PREVENTING INSTITUTIONAL IDENTITY THEFT

Vigilance and preparation are the watchwords for preventing online institutional identity theft. What follows are descriptions of some of the most common steps that a company may consider taking to reduce the risk of online identity theft.

Register Similar Domain Names. Although it may be neither possible nor economically rational for an institution to try to register every conceivable iteration of domain names that might be similar to the institution's name, it is good practice to register at least those names that are most intuitively similar to the institution's name. Additionally, institutions

should consider working with their senior officials to ensure that their individual names are registered as domain names.

Monitor the Internet. With some surveys now suggesting that the "Web" consists of billions of Web pages, monitoring the Internet, which includes the Web, for misuses of the names of the institution and its senior officials is easier said than done. Yet, there are basic precautions that may be taken. At the high end of the spectrum, there are a host of pay services that use sophisticated technologies that automatically monitor the Web for institutional customers. Such services include Cyveillance (www.cyveillance.com), Intelliseek (www.intelliseek.com), and eWatch (www.eWatch.com). An institution can hire these services to monitor the Internet and to generate extensive, information-rich reports about use and misuse of the institution's identity on the Internet. At the other end of the spectrum, in-house information technology specialists can be instructed to monitor pertinent message boards, domain name registrations, search engines and the like for misuses of the company's and senior officials' identities. Much of this monitoring can be automated using free services already available on the Web.[11]

Deal Promptly With Suspect Circumstances. Institutions should watch for confusingly similar domains and deal promptly with situations when they arise. One way to automate the process is to use any of a number of free domain-monitoring services such as the free name monitoring service known as NameGuard offered by NameProtect.com. Such services provide free alerts when domain names similar to the one you wish to protect are registered.

When a confusingly-similar domain name is identified, a company may wish to consider the following.

- Assess the motives and legitimacy of the site involved, to the extent possible.
- Assess the risk of confusion to people trying to access your own Web site(s).
- If the confusingly-similar name is determined to be legitimate and not an apparent attempt to sidetrack visitors away from your Web site, consider either increasing educational efforts with your customers to ensure they know your Web site address or, in appropriate circumstances, approach the owner of the confusingly-similar name about purchasing the domain.
- If the confusingly-similar name involves cybersquatting or an apparent instance of identity theft, consider disputing the use of the name either through a lawsuit filed under the Anticybersquatting Consumer Protection Act or through arbitration procedures set forth in the Uniform Domain Name Dispute Resolution Policy adopted by The Internet Corporation for Assigned Names and Numbers on August 26, 1999.[12]

Increase Security Level With Your Domain Registrar. Domain name registrars like Network Solutions, Inc. (www.nsi.com) typically will amend registration information when requested by the registrant. To reduce the risk of an unauthorized change to such registration information, institutions should communicate with their registrars and ensure that the levels of security and authentication required for such communications provide an adequate degree of protection. Many services provide for multiple levels of secure communications and authentication. Institutions should give thought to selecting the levels that best suit their needs and best protect their domains.

Protect Against Domain Name Server Intrusions. Although virtually all financial institutions have grown sufficiently sensitive to the risk of intrusion to their computer systems by outsiders, care should still be taken to ensure that the institution's domain name server computer is adequately protected against hackers. Indeed, the issue is of such importance that last May the Office of the Comptroller of the Currency provided guidance to national banks regarding how to deal with intrusion risks.[13]

Consider Reporting Obligations. If institutional identity theft occurs, consider your reporting obligations to appropriate regulatory and law enforcement officials. For example, banks that become aware of instances of identity theft typically are expected to file a so-called "Suspicious Activity Report" as provided under 12 C.F.R. § 21.11 and the instructions contained on the report.

IV. CONCLUSION

Unscrupulous operators, taking their lead from adult Web site operators, are growing ever more sophisticated in the techniques they use to steal private customer data. Institutions, consequently, must give special attention to safeguarding against online identity theft not only to protect themselves, but also to protect the privacy of their ccustomers' data.

ENDNOTES

1. *See N.J. Suit Claims Three Pretended To Be Australian Firm,* Reuters special to MercuryCenter.com (Dec. 2, 1999) (originally available at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/068307.htm,copy on file with the authors). *See also State News – Antifraud: Men, Firms Sued Over Fake Web Site; Investors Allegedly Bilked of $750,000,* 31(47) Sec. Reg. & Law Rep. (BNA) 1630 (Dec. 13, 1999); New Jersey Department of Law and Public Safety Division of Consumer Affairs, *State Files Suit Against Unregistered Englewood Broker-Dealer That Allegedly Diverted $750,000,* News Release (Dec. 2, 1999) <http://www.state.nj.us/lps/ca/press/engle.htm>; Australian Securities & Exchange Commission, *U.S. Authorities Act Against False MLC,* Media Release (Dec. 6, 1999) <http://www.asic.gov.au/pdf/99-451.pdf>.

2. Office of the Comptroller of the Currency, *Protecting Internet Addresses of National Banks,* Alert 2000-9 (Jul. 19, 2000) <http://www.occ.treas.gov/ftp/alert/2000-9.txt>.

3. *See PaineWebber Inc. v. wwwpainewebber.com and Rafael Fortuny,* No. 99-0456-A (E.D. Va., preliminary injunction issued Apr. 9, 1999). *See also* Chris Sherman, *The Identity Hijackers,* About.com (visited Aug. 7, 2000) <_____>.

4. *See* Carl S. Kaplan, *Cyberlaw Journal: 'Typo Pirates' Run Into Trouble With Corporations and Courts,* N.Y. Times on the Web (Apr. 23, 1999); Michael Pastore, *Rumblings – The Typo Pirates Strike Again,* InternetNews (Jul. 27, 1999).

5. *See* U.S. Federal Trade Commission, *FTC Halts Internet Highjacking Scam – Millions of Legitimate Web Pages Cloned by Highjackers; Innocent Surfers Barraged With Smut,* News Release (Sept. 22, 1999) <http://www.ftc.gov/opa/1999/9909/atariz.htm>; U.S. Federal Trade Commission, *Statement of Jodie Bernstein – Internet Pagejacking Press Conference,* FTC.gov (Sept. 22, 1999) <http://www.ftc.gov/opa/1999/9909/atarizjodie.htm>. *See also* John Snell, *'Pagejackers' Take Internet Surfers on a Wild Ride,* OregonLive (Oct. 18, 1999) <http://oregonlive.advance.net/technw/99/10/tn101803.html>; Chris Sherman, *FTC Halts Web Pagejackers,* About.com (Oct. 5, 1999) <http://websearch.about.com/internet/websearch/library/weekly/aa100599.htm>. Another recent and widely-reported typo-pirating instance involved an individual who registered typo-based variations of domains owned by World Wrestling Federation Entertainment, Inc. WWF commenced an arbitration and obtained a decision directing the registrant of the names to return the names to it. *See World Wrestling Federation Entertainment, Inc. v. Matthew Bessette,* WIPO Arbitration and Mediation Center Case No. D2000-0256 (Admin. Panel Decision filed Jun. 7, 2000) <http://arbiter.wipo.int/domains/decisions/html/d2000-0256.html>.

6. Pub. L. No. 106-113, 113 Stat. 150 (106th Cong. Nov. 18, 1999) <http://www.law.berkeley.edu/institutes/bclt/pubs/swbook/cybersquat-law.html>.

7. *See* Bob Sullivan, *Nike.com Hijacked by Protesters*, MSNBC.com (Jun. 21, 2000) <http://www.msnbc.com/news/423820.asp>; Matt Richtel, *Protesters Hack Nike Web Site*, N.Y. Times on the Web (Jun. 22, 2000) <http://www.nytimes.com/library/tech/00/06/biztech/articles/22nike.html>; *Hackers Take Over Nike Web Site,* Associated Press special to CNET News.com (Jun. 21, 2000) <http://news.cnet.com/0-1007-200-2122747.html>.

8. *See* Jeffrey Goldfarb, *Federal News – Electronic Commerce: Online Impersonator of NYSE Chairman Sued by Exchange for Stock Tip Postings*, 32(32) Sec. Reg. & Law Rep. (BNA) 1101 (Aug. 14, 2000).

9. *See* State of California Business, Transportation and Housing Agency Department of Corporations, *Department of Corporations Files Internet Market Manipulation Action*, News Release 00-11 (Jun. 20, 2000) http://www.corp.ca.gov/pressrel/nr0011.htm.

10. *See Protecting Internet Address of National Banks, supra* n.2.

11. For a summary of some of the many automated monitoring systems freely available on the Web, *see* Blake A. Bell, *Searching the Internet: The Smart Way*, LLRX.com (May 1, 2000) <http://www.llrx.com/features/smart.htm>.

12. *See* The Internet Corporation for Assigned Names and Numbers, *Uniform Domain-Name Dispute-Resolution Policy* (updated Jun. 17, 2000) http://www.icann.org/udrp/udrp.htm.

13. *See* Office of the Comptroller of the Currency, *Infrastructure Threats – Intrusion Risks*, OCC Bulletin 2000-14 (May 15, 2000).