

WHITEPAPER

Examining the Costs of Threats
Associated With Your
Internet Presence

Target Audience: Financial Institutions

Authored By:

**Kevin Joy, Vice President, Marketing
BD-BrandProtect**

June 6, 2007

Table of Contents

Introduction	3
Mapping the Regulatory Environment	4
Quantifying the Costs of Internet Risks.....	8
Conclusion.....	12
About BD-BrandProtect	12
About the Author.....	13

Introduction

Anyone who has tried to quantify the size of the U.S. Internet banking market knows that definitive statistics are hard to come by. According to Forrester Research, 41 million U.S. households were already banking online in 2005; that number is expected to climb to 72 million U.S. households by 2011.¹ For its part, comScore, a global Internet information provider, found that the U.S. online banking population grew 9.5% in 2006, compared to 2005.² In recent years, countless other research firms also have released their growth projections for the industry, with varying degrees of accuracy.

Yet, a number that is less frequently cited is the 150 million U.S. consumers who claim they do not bank online for fear of becoming the next victim of identity theft. This statistic was released earlier this year in a study conducted by Javelin Strategy & Research, which also found that 88 million U.S. online banking customers would change banks or reduce their online service usage if their financial institution was compromised by a data breach.³

Clearly, the risks associated with Internet banking rise each year. Today, consumer confidence is threatened and customers are increasingly at risk from an expanding range of Internet incidents aimed at financial institutions, such as:

- Phishing attacks, where Internet criminals attempt to dupe customers into releasing their personal financial data in order to commit identity theft
- Weblinking infractions, where customers click on links that appear legitimate, only to be diverted to unrelated and potentially offensive sites
- Brand protection incidents that target an organization's brand and misuse it to claim an unauthorized association, divert Web traffic or commit fraud, and Domain infractions, where Internet fraudsters "hijack" Web domains while attempting to find ways to profit from them

¹ **US Online Banking: Five-Year Forecast, North American Consumer Technographics®, March 19, 2007** by Catherine Graeber, found at www.forrester.com/Research/Document/Excerpt/0,7211,41159,00.html on May 24, 2007

² **2006 Online Banking Study, comScore, April 16, 2007**, found at www.comscore.com/press/release.asp?press=1394 on May 24, 2007

³ **TriCipher Consumer Online Banking Study, by Javelin Strategy & Research (Pleasanton, California), found at www.banktech.com/show/Article.jhtml?articleID=199203700 on May 24, 2007**

Far from being merely a nuisance, these emerging threats are rapidly exposing financial institutions to a range of unprecedented financial, legal, strategic, reputation, operational and transactional risks. In today's heightened regulatory environment, financial institution executives and boards can no longer ignore the challenges related to Internet banking. As the FFIEC (Federal Financial Institutions Examination Council) has noted, these challenges "... increase threats to the institution's reputation, confidentiality of information, system and data integrity, system availability, and regulatory compliance."⁴

In light of these risks, financial institutions increasingly need strategies for assessing – and mitigating – the threats associated with maintaining an Internet presence.

Mapping the Regulatory Environment

As one of the most tightly regulated industries in the world, the financial services sector is no stranger to the need for comprehensive risk management practices. To be sure, financial organizations have long invested significant effort and resources to manage credit and liquidity risks. Yet, in recent years, regulators have made it clear that financial institutions are increasingly expected to broaden their risk management framework to consider a range of new threats – including those posed by Internet technologies.

In legislation, regulations and guidelines, agencies across the country are indicating an intention to hold financial organizations to a higher standard of responsibility in protecting both corporate and customer information assets from reasonably foreseeable threats:

- Section 501(b) of the Gramm Leach Bliley Act (GLBA) mandates federal regulators (OCC, OTS, FRB, FDIC, NCUA, FTC, SEC) to implement guidelines that financial services organizations must follow to: safeguard the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to, or use of, such records that could result in substantial harm or inconvenience to any customer. The subsequent

⁴ **FFIEC Information Technology Examination Handbook, E-Banking Booklet, found at http://www.ffiec.gov/ffiecinfobase/html_pages/ebanking_book_frame.htm**

interagency guidance then requires financial institutions to create, implement and maintain a comprehensive information security program that contains a risk assessment process. Among other things, this risk assessment process should enable financial institutions to identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information; and it should consider the potential damage of such a threat, taking into consideration the sensitivity of the information to be protected.

While not specifically articulated, there is little doubt that Internet threats such as phishing and other related infractions could compromise the security and confidentiality of customer records and information. Given the increasing pervasiveness of phishing activities aimed at financial institutions (see the next section of this paper for details), it makes sense for organizations to gain an understanding of their vulnerability to such infractions as part of their risk assessment process.

- The Interagency Guidelines Establishing Standards for Safeguarding Customer Information were issued in response to GLBA section 501(b). According to these Guidelines, financial institutions are expected to manage and control identified risks by considering whether specific security measures are appropriate for their circumstances. Among the security measures listed, the Guidelines encourage banks to review their: access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals; monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, customer information systems; and response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems.
 - For its part, last year the FFIEC issued its IT Examination Handbook, which contains a series of 12 booklets applicable to U.S. financial institutions. In its E-Banking Booklet, the FFIEC lists a series of risks examiners should consider when reviewing both informational and transactional websites. Among the risks enumerated are the potential for:
-

- Negative public perception if the institution's on-line services are disrupted or if its website is defaced or otherwise presents inappropriate or offensive material
 - Liability for unauthorized transactions
 - Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or credit on-line
 - Weblinking risks, including consumer confusion about whose website they are viewing, and
 - Reputation risk as a result of (among other things) disclosure or theft of confidential customer information to unauthorized parties (e.g. hackers).
-
- Similarly, the FFIEC Information Security Booklet calls for financial institutions and their technology service providers to maintain effective information security programs tailored to the complexity of their operations. As part of these programs, financial institutions are expected to assess both potential threats and vulnerabilities to customer non-public and corporate proprietary information and the systems used to collect, process, transmit, and store the information. The importance of these actions cannot be over-stated. As the FFIEC notes, "Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services."⁵
-
- In the Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment, issued on August 15, 2006, FFIEC member agencies note that financial institutions are expected to consider the following threats as part of their risk assessment processes: phishing, pharming, malware, reputation risk, harm to the customer, transaction risk and other reasonably foreseeable threats.⁶
-
- A series of FDIC Financial Institution Letters also speak to the importance of monitoring Internet threats to control risk. For instance, FIL-64-2005 provides "Guidance on how financial institutions can protect against pharming attacks".

⁵ FFIEC Information Technology Examination Handbook, Information Security Booklet, found at http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm

⁶ Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment, August 15, 2006, found at <http://www.federalreserve.gov/boarddocs/srletters/2006/SR0613a1.pdf>

Among the protective measures enumerated, the FDIC indicates that financial institutions are expected to diligently manage their domain names and investigate anomalies that might suggest their domain has been hijacked.

FIL-77-2000: Protecting Internet Domain Names notes "Internet domain names have been used to perpetrate fraud and have led to both public confusion and legal disputes". Some of the potential risks cited include phishing, traffic diversion and "cybersquatting", where Internet fraudsters attempt to sell desirable domain names to companies at exorbitant prices.

FIL-26-2004: Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes speaks to the ongoing importance of protecting against phishing attacks. In addition to the serious risks customers face as potential victims of identity theft, the FDIC notes that phishing can also result in "[p]otential negative publicity regarding an institution's business practices [which] may cause a decline in the institution's customer base, a loss in confidence or costly litigation."⁷ To address these risks, financial institutions are urged to enhance their incident response programs by, among other things, increasing suspicious activity monitoring and taking steps to shut down fraudulent websites.

Additionally, in FIL-30-2003: Weblinking, financial institutions are encouraged to prevent the reputation and compliance risks that may arise from weblinking activities by periodically reviewing and testing weblinks to ensure they function properly and present appropriate content. Similar weblinking guidance has also been issued by the OTS and NCUA.

- Finally, in December 2002, the National Credit Union Association (NCUA) issued a Letter to Credit Unions entitled Protection of Credit Union Internet Addresses. In this guidance, NCUA outlines the risks and associated threats that may arise if credit union members fail to reach the intended website (due to traffic diversion or other related domain infractions). As NCUA notes, in this event credit unions (and, by extension, other financial institutions) could face:

⁷ **FDIC FIL-26-2004: Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes**, found at <http://www.fdic.gov/news/news/financial/2004/fil2704a.html>

- Transaction risk, if customers are lured to disclose confidential information that could enable the commission of identity theft
- Strategic risk, if the credit union's domain is hijacked and used to reduce the effectiveness of the organization's branding efforts, or if retention rates suffer due to the traffic diversion
- Compliance risk, if members experience substantial harm due to the lack of an adequate security program, and
- Reputation risk, if any of the above-mentioned situations occurred, or if members were directed to a site containing offensive material

As the regulatory environment continues to evolve, one thing is clear: financial institutions must make greater efforts to measure, monitor and control Internet-related vulnerabilities and threats. The potential risks of non-compliance, ranging from fines and sanctions to more severe penalties, are simply too steep to ignore. Similarly, as the next section of this paper explains, the financial risks associated with Internet threats are also mounting at an alarming rate. That said, financial institutions can put a few relatively simple and cost-effective strategies into place to address these threats.

Quantifying the Costs of Internet Risks

There is ample anecdotal evidence that Internet incidents and malicious activities damage corporate reputation, result in lost revenue, lead to deteriorating customer loyalty and threaten brand integrity. Yet the repercussions extend far beyond unquantifiable loss. In recent years, numerous research organizations, advocacy groups and media sources have released figures that measure the cost of Internet infractions in financial terms:

- According to the 2006 E-Crime Watch Survey from CSO Magazine⁸, the financial and operational losses caused by electronic crime incidents are on the rise. This third annual survey of 434 security executives and law enforcement personnel was conducted in cooperation with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center and Microsoft Corp. Among the findings: 63% of respondents report operational losses as a result of e-crime; 40% report financial losses averaging \$740,000 per

⁸ 2006 E-Crime Watch Survey, CSO Magazine, found at <http://www.cert.org/archive/pdf/ecrimesurvey06.pdf> on May 24, 2007

incident; and 23% report harm to their organization's reputation as a result of e-crime. Additionally, 29% of respondents admit to being victims of fraud, 19% report experiencing customer identity theft, 31% were victims of phishing, 40% had their domains hijacked and used to generate illegal spam e-mail, and 14% experienced website defacement.

- According to the Anti-Phishing Working Group (APWG), 55,643 unique phishing websites were detected in April 2007, representing a massive jump of nearly 35,000 from March. As a result, 174 brands faced attack in April, with financial services remaining the most targeted sector at 92.5%.⁹
- Increasingly sophisticated phishing techniques also continue to put financial organizations at risk. In internal testing conducted by TriCipher, a company that develops authentication solutions, it took one person six hours to develop and configure a man-in-the-middle phishing site that could be used to gain unauthorized access to live accounts and/or to modify transactions. In this type of attack, fraudsters intercept the communication between two (or more) computing devices and, by inserting themselves into the "middle" of the communication, they are able to view any unencrypted information that passes between the computers – including account numbers and passwords. In TriCipher's test, once the man-in-the-middle phishing site was active, it took only 45 minutes to attack a financial or e-commerce portal and 45 minutes to attack a major U.S. brokerage site. Using similar tactics, in October 2006, hackers broke into accounts at two large U.S. brokerages to execute fraudulent trades, resulting in losses of \$22 million.¹⁰

"A single high-profile incident that is picked up by the major news media could instantaneously turn a significant number of online banking users back into check-writers who frequent bank branch teller windows. Even worse, the reputation damage could ruin a bank's entire franchise."

– George Tubin, Senior Analyst, TowerGroup, No More Straw Houses: The Fed's Guidance on Online Authentication

⁹ Phishing Activity Trends, April 2007, Anti-Phishing Working Group, found at http://www.apwg.com/reports/apwg_report_april_2007.pdf on May 24, 2007

¹⁰ The Perfect Storm: Man in the Middle Phishing Kits, Weak Authentication and Organized Online Criminals, TriCipher, found at www.antiphishing.org/sponsors_technical_papers/TriCipherMITMWhitepaper.pdf on May 24, 2007

- In June 2003, Gartner Research and Harris Interactive also completed two studies that found that approximately seven million people were victims of identity theft in the previous 12 months. The study revealed that the aftermath of identity theft includes an average of 600 hours per victim to recover from the crime, at a huge cost in lost potential income.¹¹ In the same year, the Gartner Group estimated that direct phishing-related loss to U.S. banks and credit card issuers was \$1.2 billion. Notably, indirect losses were much higher, and included customer service expenses, account replacement costs and higher expenses due to decreased use of online services.¹²

- Needless to say, these trends aren't confined to North America. Weber Shandwick, a global public relations company, found that major triggers of reputation failure include financial irregularity (72%), security breaches (62%) and online attacks or rumors (25%). Significantly, when companies lose reputation after a crisis, the study also found that 60% of business executives blame their CEO.¹³

- In the UK, it is estimated that one in eight Internet surfers – representing 1.7 million people – were victims of online fraud in 2006, with personal losses averaging £875.¹⁴ Even more significantly, it appears that one-third of UK businesses may not report information security crimes and breaches for fear of the reputation damage it may cause. The reason? Many of these businesses are subject to attempted e-crime every day.¹⁵

¹¹ As cited in **Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization**, Symantec, found at www.antiphishing.net/sponsors/technical_papers/symantec_online_fraud.pdf on May 24, 2007

¹² Identity Theft Technology Council (ITTC) **Report on Online Identity Theft Technology and Countermeasures**, found at www.antiphishing.org/Phishing-dhs-report.pdf on May 24, 2007

¹³ **Safeguarding Reputation™**, Weber Shandwick, in partnership with KRC Research, 2006, found at <http://164.109.94.76/Default.aspx/Insights/ThoughtLeadership/ResearchInitiatives/SafeguardingReputationSurvey> on May 24, 2007

¹⁴ **£875: the cost of online fraud**, Webuser, by Ben Camm-Jones, March 26, 2007 citing Get Safe Online's Internet Safety: The State of the Nation report, found at www.webuser.co.uk:80/news/news.php?id=114059-cost on May 24, 2007

¹⁵ **One third of UK firms hush up e-crime: Fear of reputation damage leads firms to keep quiet**, vnunet.com, by Robert Jacques, April 3, 2007, found at www.computing.co.uk/vnunet/news/2187069/third-uk-firms-hush-crime on May 24, 2007

- Similarly, Aon Australia continues to report that brand and reputation risk remain the key risk concerns for Australian businesses. As noted in the firm's 2004/05 Risk Management and Total Cost of Insurable Risk Survey, "Damage to the perception of a brand or product's quality can mean a loss of market share. Incidents can also have an impact on a company's liquidity. Less widely acknowledged is the impact that reputation damage can have on the ability to retain and recruit top talent."¹⁶

As these trends become more widespread and better known, financial services executives will likely face greater scrutiny from regulators, boards of directors and customers. Given the dangers of non-compliance, the potential for financial loss and the heightened reputation, transaction and strategic risks organizations may face as a result of Internet threats, it is incumbent upon financial institutions to take the necessary steps to assess their exposure to threats on the Internet.

Although regulatory guidance does not specifically outline the threats to be assessed as part of this review, it may be helpful for financial institutions to review common areas of potential exposure from significant Internet incidents, such as phishing, weblinking infractions, brand infractions and domain registration infractions.

Some of the steps they can take to address these threats include:

- Identifying significant Internet incidents and malicious activities
- Determining the probability of customers being exposed to each infraction to help assess its potential impact
- Developing a response plan to address each threat in a timely manner

¹⁶ 2004/05 Risk Management and Total Cost of Insurable Risk Survey, by Aon Australia, found at www.riskmanagementmagazine.com.au/articles/a6/0c0357a6.asp on May 24, 2007

Conclusion

As consumers around the world increasingly turn to the Internet to transact business and conduct online banking, regulators will continue to place financial institutions under greater scrutiny than in the past. Already, financial services organizations are expected to comply with a great number of regulations and guidelines designed to protect the integrity of their information systems and safeguard their consumers from potential harm on the Internet. Although there are no hard-and-fast rules that mandate financial institutions to respond to Internet threats in a specific way, there is little doubt that examiners, management and Boards of Directors will expect more rigorous responses than in the past. Rapidly, it is becoming clear that financial institutions require more robust and formal strategies to help them assess and mitigate the threats associated with maintaining an Internet presence.

About BD-BrandProtect

BD-BrandProtect, the leader in online threat protection, empowers organizations to gain control over how they are represented online by uncovering and mitigating the threats that put their reputation at risk and erode customer trust.

BD-BrandProtect is uniquely positioned to provide detailed and actionable reports on the most relevant and highest priority threats by combining advanced technology, round-the-clock monitoring, proven best practices and exhaustive human analysis.

BD-BrandProtect first scours millions of domains, Web pages and Internet links to uncover infractions. It then categorizes and ranks those threats according to their severity. It then initiates proactive and escalating response protocols to effectively mitigate threats when required

BD-BrandProtect has relationships with more than 2,000 Internet Service Providers globally that account more than 85% of the traffic flowing across the Internet. By consistently investing in this network, BD-BrandProtect customers have access to the most coordinated incidence response team ever created.

The company is recognized by many of the world's largest financial institutions as the leader in online threat protection. It serves the needs of a cross-section of organizations, including many of the world's most respected global brands.

BD- BrandProtect was founded in 2001 and is headquartered in Toronto, Canada, with offices in the United States, Singapore and London.

For more information: www.bdbrandprotect.com

About the Author

Kevin Joy, Vice President of Marketing, is responsible for all aspects of global branding and marketing for BD-BrandProtect. Kevin has over 16 years of marketing experience growing leading consumer goods and professional services firms. For the past 7 years, he has led the market strategy and program development of all Deloitte Canada's services and played a major role globally as a member of the firm's marketing, communications and business development council, most notably as a leader of its branding initiative.

Prior to this, he spent eight years with Unilever in Canada and Mexico. In Canada, he built Becel into one of Canada's most successful and trusted household brands and then went on to lead Lipton's food innovation effort. While in Mexico, his experience included being an integral part of a successful new joint venture for Unilever's ice cream business, which included franchise operations. Kevin has also worked in Canada and in the US for a division of Dresser Industries, as a technical marketing representative. Finally, he was a founding member and director of a Canadian biotech startup.

Kevin holds a Bachelor's degree in Chemical Engineering and an MBA in International Business & Marketing.

Kevin Joy
Vice President, Marketing
BD-BrandProtect
Tel: 905.271.3725 ext. 306
kjoy@bdbrandprotect.com

06/06/07 v 03

