Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW.
Washington, DC 20429
Comments@FDIC.gov

September 18, 2006

Re: Comments: RIN 3064–AD00: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; 12 CFR Parts 334 and 364; ACTION: Joint notice of proposed rulemaking.[1] (NPR)

Dear Mr. Feldman,

We appreciate the opportunity to provide comments on the joint notice of proposed rulemaking (NPR) in the Federal Register dated July 18, 2006.

A directory of our issues and recommendations is in Appendix A, pages 67-69.

Executive Summary: Our analysis and comments focus on corporate identity theft risks within the NPR that (1) enable 45% of phishing attacks, which are federal crimes, and (2) pose financial, operational, compliance, reputation and litigation risks to the safety and soundness of IP (intellectual property) owners. Operational risks, per the recent Basel II NPR, are defined as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition of operational risk includes legal risk – which is the risk of loss (including litigation costs, settlements, and regulatory fines) resulting from the failure of the bank to comply with laws, regulations, prudent ethical standards, and contractual obligations in any aspect of the bank's business – but excludes strategic and reputational risks."[2] Influencing our recommendations are (1) phishing metrics from the Anti-Phishing Working Group, (2) recent observations by David A. Thomas of the FBI's Cyberterrorism Unit, (3) recent views on identity fraud and related Suspicious Activity Reports by the UK's Serious Organized Crime Office, (4) Basel II's focus on operational risks and losses, (5) a 6/12/06 speech by a Member of the Board of Governors of the US Federal Reserve System on enterprise risk management, and (6) domestic federal laws and supervisory guidances that focus on duty of care and adequate internal controls to safeguard brands, reputations and customers from fraudulent web sites. Applying existing standards and regulations for safeguarding corporate identities with the same vigor and intensity that banks encourage consumers to safeguard consumer identities will minimize systemic risks for corporate brands and related operational risks that are being exploited by cyber criminals. Allocating a small percentage of a firm's marketing budget from the last 3 years will minimize corporate identity risk exposures that are fueling the growth

of fraudulent web sites, including phishing risks. “Consumer confidence in internet banking is fragile,”[3] states the UK banking regulator, FSA, in January 2006. For this investment, banks will (A) minimize operational risks and (B) generate a positive ROI with reduced identity theft expenses and increased consumer confidence and usage of the low-cost internet channel. IP owners and their Board of Directors need to take ownership of safeguarding their brands, reputation and consumers from fraudulent web sites and in the process reduce corporate identity theft for all stakeholders, including law enforcement. In developing and managing an effective Identity Theft Program, that is synchronized with IP governance standards from an Information Security Program and current federal regulations, a board should receive monthly or quarterly independent IP governance audits focused on (1) measuring and minimizing exposure to corporate identity theft and related operational risks and (2) reaffirming the accuracy of their disclosure statements indicating compliance with federal standards and regulations. Example 1: Boards should select and manage to a strategic risk exposure for corporate identity theft ranging from “F” rating (significant exposures) to “A” rating (minimal exposure). Example 2: Boards should reaffirm the accuracy of “confidential and security” statements that often state, "We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.” In summary, leadership from boards in setting the tone at the top by applying existing regulatory standards combined with regular independent IP governance reports will minimize corporate identity theft, related operational risks and build effective Identity Theft and Information Security Programs.

Fresh FFIEC Resources: Our analysis draws upon 3 documents issued by the FFIEC subsequent to 7-18-06 and the Red Flag NPR that provide fresh information, insights and standards for identity theft. These include the (A) updated FFIEC Information Security Handbook dated 7-27-06[4], (B) Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual dated 7-28-06[5], and (C) “FFIEC Guidance on Authentication in an Internet Banking Environment” dated 8-15-06[6]. Highlights include from (A) 11 supervisory guidances on safeguarding bank brands and domains (only 2 are listed in the NPR), (B) a quote that “Terrorists generally finance their activities through both unlawful and legitimate sources”…that include “identity theft”[7], and (C) multifactor authentication is not required. Specifically, the last one states that, “the guidance does not call for the use of multifactor authentication. The use of multifactor authentication is one of several methods that can be used to mitigate risk as discussed in the guidance. However, the guidance identifies circumstances under which the Agencies would view the use of single-factor authentication as the only control mechanism as inadequate and conclude that additional risk mitigation is warranted.”[8] In light of these developments, our objective is to revisit current regulatory standards and show how these all should be applied, as part of the FDIC’s layered information security strategy, to minimize corporate identity theft and related operational risks and losses. The FDIC’s layered information

strategy for safeguarding bank brands and domain names along with additional authentication options is defined within the FIL 103-2005, "FFIEC Guidance Authentication in Internet Banking Environment."[9]

Growth of cybercrime is among top global threats to security, says FBI:[10]
"'In today's increasingly uncertain world there is only one certainty. Your security will be breached; it's just a case of when' said David Thomas, deputy assistant director, FBI Cyberdivision, at the recent (July, 2006) BCS sponsored World Wide Web Conference in Edinburgh. During a talk highlighting criminal trends worldwide David explained that cybercrime has become so endemic that Robert Mueller, head of the FBI, now regards the Cyberdivision as the third most important after terrorism and foreign intelligence operations. Identity theft is becoming increasingly popular, with fake credit cards selling for between £1 and £100 depending on the card type and fraudster. Personal details are big business. US spammer Jeremy Jaynes made £13m selling personal details before he was caught. And the Mafia made £360m in seven years through e-crime, said Thomas."[11]

The UK's Serious Organized Crime Office (SOCA), established April, 2006:
Lessons learned from the UK's experience in defining issues and allocating resources relating to personal and corporate identity theft could help similar initiatives underway in the US, such as the Agencies involved with the Red Flag NPR and the President's Identity Theft Task Force. SOCA has focused 10% of its resources for identity theft,[12] which it defines as one of the major forms of Organized Crime.

"Fraud is also committed against individuals and companies, in a wide variety of ways, and often by organised gangs. It is here that SOCA will operate. Some examples of such frauds include:

- against banks, often involving false or stolen identities;
- investment and advance fee frauds, in which individuals are enticed to pay over money against false promises of returns; and
- forms of e-fraud exploiting the use of the internet by banks and commerce.

Much fraud goes unreported, and despite the fact that frauds can cause companies and individuals significant damage, it is sometimes, mistakenly, seen as victimless. As well as generating money that can be used for future crimes, fraud means that everyone pays for more goods and services. In addition, it can cause significant personal difficulties and distress."[13]

Basel II - Operational Risks and Losses: The Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters. Over recent years, it has developed increasingly into a standard-setting body on all aspects of banking supervision. Members from the US include Board

of Governors of the Federal Reserve System, OCC, FRB-NY and FDIC.[14] In June 2006, the committee released the "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version".[15] On September 5, 2006, the FRB, FDIC, OCC and OTS issued the Notice of Proposed Rule Making for the American version of Basel II, i.e., "Risk-Based Capital Standards: Advanced Capital Adequacy Framework".[2] Operational risks and operational losses are common features within each of the Basel II drafts. Each Basel II draft has a similar definition of "Operational Risk". The US definition is featured in our Executive Summary. The June 2006 definition is nearly identical.[16] "Operational Loss" in the June 2006 draft includes the following descriptions and chart that would be relevant for capturing identity theft losses arising from restitution payments to customers, litigation settlements and/or regulatory fines. "Operational loss" in the US version has similar language, i.e., "The proposed rule defines operational loss events as events that result in loss and are associated with internal fraud; external fraud; employment practices and workplace safety; clients, products, and business practices; damage to physical assets; business disruption and system failures; or execution, delivery, and process management."[17] We cite the Basel II efforts to define operational risk and operational losses as these could be relevant regulatory factors for evaluating the effectiveness of the Identity Theft and Information Security Programs as it relates to corporate identity theft and its role in enabling federal crimes such as phishing.

Operational Losses (Annex 9: BIS)[18]

Level 1	Level 2	Level 3
External Fraud	Systems, Security	Theft of information (Monetary Loss); Hacking Damage
Clients, Products & Business Practices	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations; Suitability / disclosure issues (KYC, etc.); Retail customer disclosure violations; Breach of privacy;
Execution, Delivery, Process Management	Monitoring & Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)

Federal Reserve Member Speech: "A supervisor's perspective on enterprise risk management"[19] dated 6-12-06 addresses Sarbanes-Oxley and information security. On the latter topic, the transcript states, "**Information security.** Issues involving information security and *identity theft* have received quite a bit of attention from the federal government over the past several years. In fact, just recently, President Bush signed an executive order that created an Identity Theft Task Force for the purpose of strengthening federal efforts to protect against identity theft. The heads of the federal bank regulatory agencies are designated members of this task force; and as supervisors of financial institutions, I believe we can offer a unique perspective on this issue."

"As you have probably noticed, cyber attacks and security breaches involving nonpublic customer information appear in the headlines almost every week. These events have cost the financial services industry millions of dollars in direct losses and have done considerable reputational damage. The cost of identity theft to affected consumers is also significant."[20]

President's Identity Theft Task Force: On May 10, 2006, President Bush signed an Executive Order for "Strengthening Federal Efforts to Protect Against Identity Theft". A report is due within 180 days or early November. One of the objectives is to "address how the private sector can take appropriate steps to protect personal data and educate the public about identity theft."[21]

Overlap of NPRs on Operational Risks: Four of the Agencies participating in the Red Flag NPR, i.e., FRB, FDIC, OCC and OTS, are also participating in the Basel II NPR released 9-05-06. Each of the NPR's are focused on addressing operational risks with the Red Flag NPR seeking to define and establish programs to prevent, detect and mitigate identity theft risks that give rise to potential litigation and operational risks as well as reputation risks. Definitions and/or internal controls established under the final Red Flag Rules will likely be rolled up and/or cited in subsequent efforts to define potential litigation and operational risks under the Basel II NPR. As a result, we are taking a broad, global view on the issue of corporate identity theft and seeking clarity, consistency and coordination amongst the Red Flag NPR Agencies on definitions for corporate identity theft, related internal controls, operational risks and measurement models per existing regulations and supervisory guidances.

NPR's definition of Identity Theft with a focus on Corporate Identity Theft:
The following are quotes from pages within the NPR.[22]

40790	**4. *Identity Theft***. The proposed definition of ''identity theft'' states that this term has the same meaning as in 16 CFR 603.2(a). Section 111 of the FACT Act added several new definitions to the FCRA, including ''identity theft.'' However, section 111 granted authority to the FTC to further define this term. The FTC exercised this authority and issued a final rule, which became effective on December 1, 2004, that defines ''identity theft'' as ''a fraud committed or attempted using the identifying information of another person without authority." The FTC's rule defines ''identifying information'' to mean any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, such as a name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, or employer or taxpayer identification number. This definition of ''identity theft'' in the FTC's rule would be applicable to the Red Flag Regulations. Accordingly, ''identity theft'' within the meaning of the proposed Red Flag Regulations includes both.

40790	"…in addition to individuals, various types of entities (*e.g.*, small businesses) can be victims of identity theft."
40790	5. *Red Flag.* The proposed definition of a ''Red Flag'' is a pattern, practice, or specific activity that indicates the possible risk of identity theft. This definition is based on the statutory language. Section 114 states that in developing the Red Flag Guidelines, the Agencies must identify patterns, practices, and specific forms of activity that indicate ''the possible existence'' of identity theft. In other words, the Red Flags identified by the Agencies must be indicators of ''the possible existence'' of ''a fraud committed or attempted using the identifying information of another person without authority.'' Section 114 also states that the purpose of the Red Flag Regulations is to identify ''possible risks'' to account holders or customers or to the safety and soundness of the institution or ''customer'' from identity theft. The Agencies believe that a ''possible risk'' of identity theft may exist even where the ''possible existence'' of identity theft is not necessarily indicated. For example, electronic messages to customers of financial institutions and creditors directing them to a fraudulent website in order to obtain their personal information (''phishing''), and a security breach involving the theft of personal information often are a means to acquire the information of another person for use in committing identity theft. Because of the linkage between these events and identity theft, the Agencies believe that it is important to include such precursors to identity theft as Red Flags. Defining these early warning signals as Red Flags will better position financial institutions and creditors to stop identity theft at its inception. Therefore, the Agencies have defined ''Red Flags'' expansively to include those precursors to identity theft which indicate ''a possible risk'' of identity theft to customers, financial institutions, and creditors.

NPR Industry Impact: Corporate identity theft is a risk for every organization operating on the Internet including all of those covered by the scope of the NPR. The following section defines the organizations covered by the NPR by Agency.

OCC 40809	**Subpart J—Identity Theft Red Flags § 41.90 Duties regarding the detection, prevention, and mitigation of identity theft.** (a) *Purpose and scope.* This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are national banks, Federal branches and agencies of foreign banks, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).
FRB 40812	**Subpart J—Identity Theft Red Flags § 222.90 Duties regarding the detection, prevention, and mitigation of identity theft.** (a) *Purpose*

	and scope. This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are member banks of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and Agencies of foreign banks (other than Federal branches, Federal Agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations.
FDIC 40815	**Subpart J—Identity Theft Red Flags § 334.90 Duties regarding the detection, prevention, and mitigation of identity theft.** (a) *Purpose and scope.* This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are insured state nonmember banks, insured state licensed branches of foreign banks, or subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).
OTS 40818	**Subpart J—Identity Theft Red Flags § 571.90 Duties regarding the detection, prevention, and mitigation of identity theft.** (a) *Purpose and scope*. This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are either savings associations whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, federal savings association operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).
NCUA 8021	**Subpart J—Identity Theft Red Flags § 717.90 Duties regarding the detection, prevention, and mitigation of identity theft.** (a) *Purpose and scope.* This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are Federal credit unions.
FTC 40823	**§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.** (a) *Purpose and scope.* This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).
Scope of FTC 40806	**Small Entities To Which the Proposed Rule Will Apply:** Section 114: As discussed in the PRA section of this Notice, given the broad scope of section 114's requirements, it is difficult to determine with precision

	the number of financial institutions and creditors that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the proposed regulations implementing section 114 will affect over 3500 financial institutions and over 11 million creditors subject to the FTC's jurisdiction, for a combined total of approximately 11.1 million affected entities.
40788-40799	[6]The Agencies note, however, that some creditors covered by the proposed Red Flag Guidelines are not financial institutions subject to Title V of the GLBA and, therefore, are not required to have an information security program under the GLBA.

9 Issues to be addressed from the NPR: Our analysis and recommendations address the following 9 issues related to corporate identity theft:

Page	NPR Request for Comments
Issue 1 NPR Pages 40789-40790	3. *Customer.* Section 114 of the FACT Act refers to ''account holders'' and ''customers'' of financial institutions and creditors without defining either of these terms. For ease of reference, the Agencies are proposing to define ''customer'' to encompass both ''customers'' and ''account holders.'' Thus, ''customer'' means a person that has an account with a financial institution or creditor. The proposed definition of ''customer'' is broader than the definition of this term in the Information Security Standards. The proposed definition applies to any ''person,'' defined by the FCRA as any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity. The Agencies chose this broad definition because, in addition to individuals, various types of entities (*e.g.*, small businesses) can be victims of identity theft. Although the definition of ''customer'' is broad, a financial institution or creditor would have the discretion to determine which type of customer accounts will be covered under its Program, since the proposed Red Flag Regulations are risk-based. The Agencies solicit comment on the scope of the proposed definition of ''customer.''
Issue 2 40790	5. Red Flag. "The Agencies request comment on the scope of the definition of ''Red Flags'' and, specifically, whether the definition of Red Flags should include precursors to identity theft."
Issue 3 40791	1. Identification and Evaluation of Red Flags; i. Risk-Based Red Flags: "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft. The Agencies request comment on whether the enumerated sources of Red Flags are appropriate."
Issue 4	E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules: "The Board is unable to identify any federal statutes or

40804, 40807	regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred."
Issue 5 40793	4. Oversee Service Provider Arrangements: "The Agencies invite comment on whether permitting a service provider to implement a Program, including policies and procedures to identify and detect Red Flags, that differs from the programs of the individual financial institution or creditor to whom it is providing services, would fulfill the objectives of the Red Flag Regulations. The Agencies also invite comment on whether it is necessary to address service provider arrangements in the Red Flag Regulations, or whether it is self-evident that a financial institution or creditor remains responsible for complying with the standards set forth in the Regulations, including when it contracts with a third party to perform an activity on its behalf."
Issue 6 40793	5. Involve the Board of Directors and Senior Management: "The Agencies request comment regarding the frequency with which reports should be prepared for the board, a board committee, or senior management. The Agencies also request comment on whether this paragraph properly allocates the responsibility for oversight and implementation of the Program between the board and senior management."
Issue 7 40808	H. Community Bank Comment Request: "The Agencies invite your comments on the impact of this proposal on community banks. The Agencies recognize that community banks operate with more limited resources than larger institutions and may present a different risk profile. Thus, the Agencies specifically request comment on the impact of the proposal on community banks' current resources and available personnel with the requisite expertise, and whether the goals of the proposal could be achieved, for community banks, through an alternative approach."
Issue 8 40806-40807	FTC: Projected Reporting, Record keeping and Other Compliance Requirements. The Commission does not expect that there will be any significant legal, professional, or training costs to comply with the Rule. Although it is not possible to estimate small businesses' compliance costs precisely, such costs are likely to be quite modest for most small entities. Nonetheless, because the Commission is concerned about the potential impact of the proposed Rule on small entities, it specifically invites comment on the costs of compliance for such parties. In particular, although the Commission does not expect that small entities will require legal assistance to meet the proposed Rule's requirements, the Commission requests comment on whether small entities believe

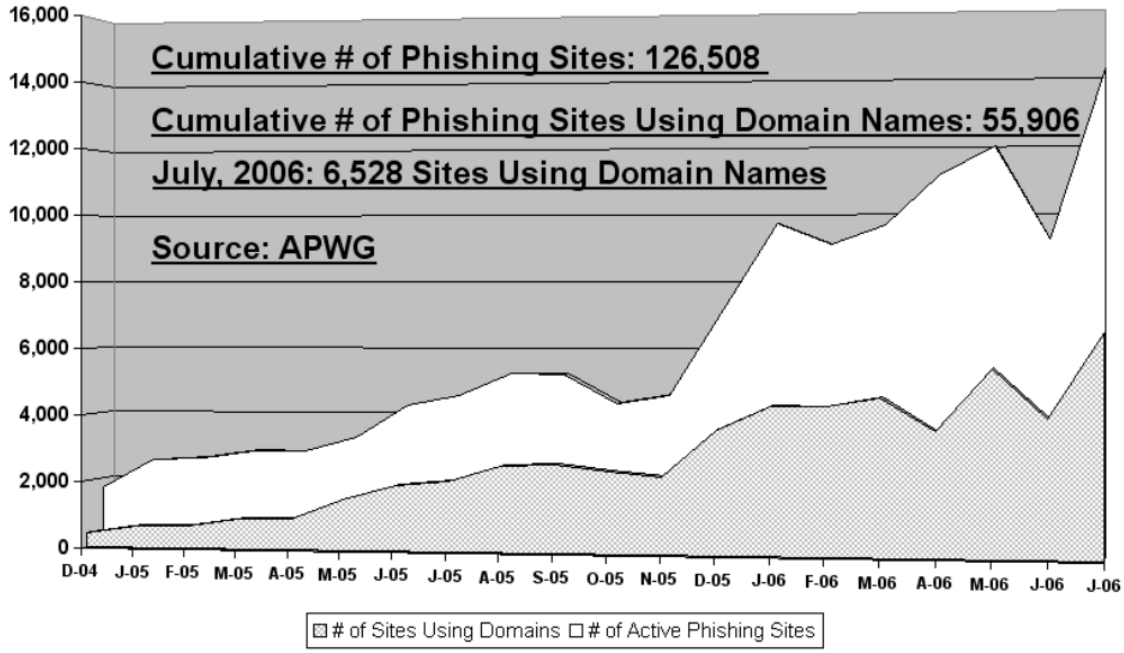
	that they will incur such costs and, if so, what they will be.
Issue 9 40807	FTC: Projected Reporting, Record keeping and Other Compliance Requirements. The Commission requests comment on the costs, if any, of training relevant employees regarding the proposed requirements.

Map of Complementary Programs: The NPR states, "A financial institution or creditor may wish to combine its program to prevent Identity Theft with its Information Security Program, as these programs are complementary in many ways."[23] In light of this, a map of the foregoing issues centered on corporate identity theft is provided in Addendum B. This shows the full spectrum of intellectual property risks that contribute to corporate identity theft. It also facilitates a side-by-side comparison between the regulations and supervisory guidances for safeguarding corporate identities that exist for Information Security Programs but are omitted from the Red Flag NPR. Applying the omitted supervisory guidances will help build an effective Identity Theft Program as well as coordinate common issues between each of the Complementary Programs.

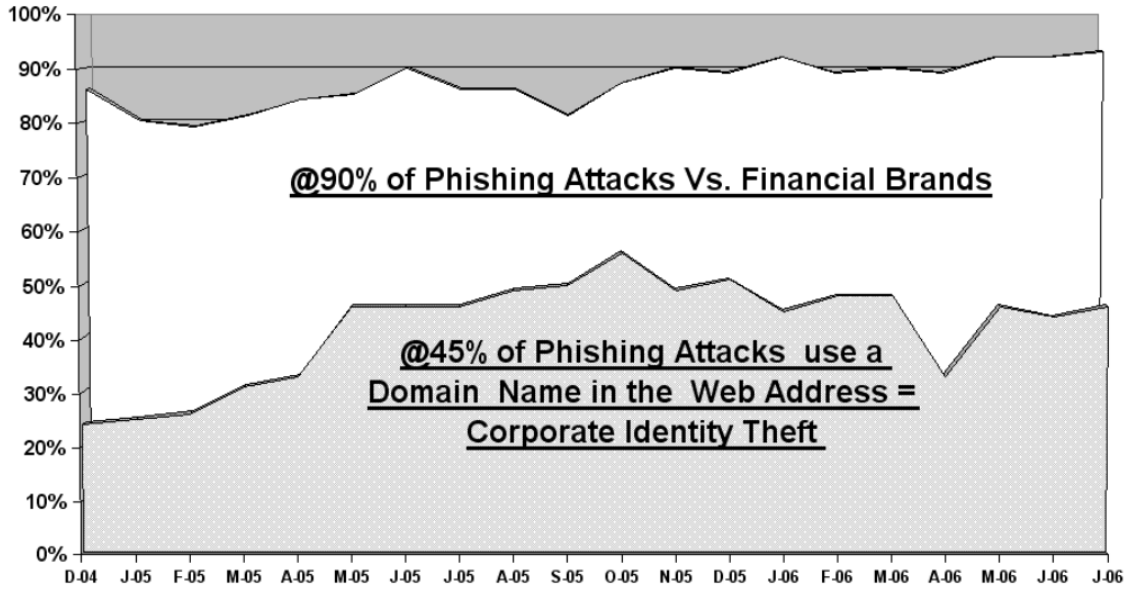
Metrics from the Anti-Phishing Working Group (APWG): The monthly statistics from APWG, over the last 20 months, show current regulatory, technology and law enforcement efforts at preventing phishing fail to slow the accelerating growth of phishing and the related use of infringing domain names, a central source of corporate identity theft.

Key trends from APWG monthly reports[24], covering Dec. '04 to July '06, are that:

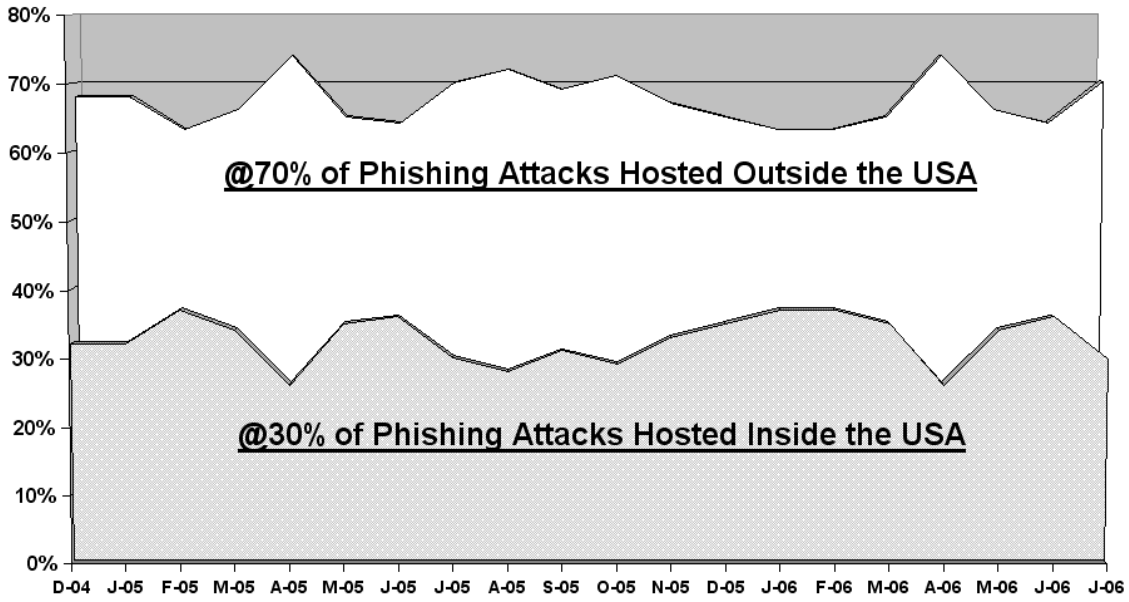
The total number of monthly phishing attacks has accelerated since November 2005, with the recent number of unique site attacks reaching 14,191 attacks in July 2006. This is 206% greater than the 4,630 attacks in November 2005. In July 2006, 46% or 6,528 of the 14,191 attacks used infringing domain names in the web address as a strategy to increase the apparent legitimacy of the phishing email. This is a record level and it is part of a troubling trend. The overall trend for the last 20 months since December 2004 shows rapidly accelerating growth despite current regulatory, technology and law enforcement efforts at preventing phishing and the fraudulent use of corporate identities, i.e., domain names. A revised strategy, focused on operational risks, operational losses and related IP governance issues per current regulations and supervisory guidances for safeguarding bank brands, is one of our core themes in an effort to minimize corporate identity theft in it's earliest stages.



Approximately 90% of the phishing attacks are against financial services providers and about 45% of all phishing attacks use a domain name that is confusingly similar to financial services providers' trademark or service mark. The use of infringing domain names in fraudulent web sites and related phishing attacks is a corporate identity theft risk. Supervisory guidances issued since 2000 outline clear steps for preventing, detecting, remediating and reporting these acts of corporate identity theft to law enforcement and Boards of Directors through Suspicious Activity Reports.



Corporate identity theft and phishing are an international problem with approximately 70% of phishing attacks originating in foreign countries[25] that are beyond US jurisdiction and that have different standards for enforcing intellectual property rights.[26] Analyzing the top 9 countries hosting phishing sites in April, May and June 2006, based on the Property Rights Ranking of the Heritage Foundation/Wall Street Journal, reveals IP owners are exposed to cyber criminals operating in countries that have a low regard for property rights. This helps cyber criminals delay law enforcement efforts to shut down fraudulent web sites thus maximizing time online to defraud consumers. As a countermove, IP owners should implement current IP governance standards to minimize exposure to corporate identity theft and related operational risks.



Full Spectrum of Intellectual Property Risks – Corporate Identity Theft: The following table is extracted from Addendum B to show the full spectrum of intellectual property risks, including domain name risks that contribute to the growth of corporate identity theft and related fraudulent web sites and phishing attacks.

(IP) Intellectual Property Governance					IT Governance	
External, Beyond IT Perimeter Risks					Internal System Risks	
Metrics on IP Governance					Metrics from APWG	
Brands	TM's/®	Domain Names	Fraudulent Web Sites (App. J: 24,25)	Phishing Sites	Pharming Attacks	Spyware, Trojans
IP Owned By Firm			Layered Information Security Solution: FDIC FIL-103-2005			
			Red Flag Risks: Fraudulent Access to Customer Information Bank Secrecy Act / Anti-Money Laundering Examination Manual (8/06) "Terrorists generally finance their activities through both unlawful and legitimate sources"…that include "identity theft"… (12 of 367)[7]			

Defining Red Flag Precursors	Corporate Identity Theft	IT Solutions
The Agencies *request comment* on the scope of the definition of ''Red Flags'' and, specifically, whether the definition of Red Flags should include precursors to identity theft. (40790)	**Phishing Risks** 40790 | 40799	(7-18-06) Multi-Factor Authentication (MFA) Agencies 40799 | OCC 40802 | OTS 40805 OCC 40802 | OTS 40805
Prevent, Detect, Mitigate	**Ref: Footnote 40 (40799)**	
Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft. The Agencies *request comment* on whether the enumerated sources of Red Flags are appropriate. (40791)	OCC. Bulletin. "Risk Mitigation and Response Guidance for Web Site Spoofing Incidents". Bulletin 2005-24. 1 July 2005.[28] OTS. Letter. "Phishing and E-mail Scams" CEO Letter #193. 3 March 2004.[33] FFIEC's Information Security Handbook **Omitted Supervisory Guidances**	National banks and savings associations complying with the ''Interagency Guidelines Establishing Information Security Standards''56 and guidance recently issued by the FFIEC titled ''Authentication in an Internet Banking Environment'' 57 already will have policies and procedures in place to detect attempted and actual intrusions into customer information systems. (8-15-06) FFIEC FAQ's on Multifactor Authentication

Law Enforcement Challenges/Hurdles with Phishing Sites Located in Other Countries: The Internet and the phishing problem is not a U.S. problem, it is a global problem. It is a rare scenario where the criminal, the evidence and the victims of phishing schemes are all located within the United States.

Companies engaging business on the Internet do so to increase exposure to their customers and reduce processing costs. A persistent business risk is the protection of their intellectual property rights.

When US law enforcement approaches a foreign country to obtain evidence, records, details of criminal action, arrests and extraditions, they must respect the property rights for those countries (in addition, to the mutual legal processing between nations.)

To examine the extent of how countries regard property rights (although not necessarily an accurate depiction of the legal structures within each country), presented below is a relative grade by country for property rights.[27] This study is part of the Heritage Foundation's 2006 Index of Economic Freedom.

The average property rights rating across the World is 3.2, which puts intellectual property holders in a negative environment for protection of their trademarks. On

the Internet, criminals leverage their ability to hide in these countries and across international borders to leverage the absence of order to their advantage. As a countermove, IP owners should implement current IP governance standards to minimize exposure to international corporate identity theft.

Top Nine Countries Hosting Phishing Sites (Non-USA)	% Of Phishing Sites (May-June, 2006)	Property Rights Rating (Definitions Provided Below) (Heritage Foundation)
China	17.07%	4
Korea (North)	8.51%	5
Italy	1.72%	3
India	1.12%	3
Malaysia	.86%	3
Brazil	.57%	3
Romania	.57%	4
Subtotal	30.42%	
France	3.94%	2
Germany	3.29%	1
Japan	2.63%	2
Canada	2.37%	1
Netherlands	.50%	1
Subtotal	12.72%	

Heritage Foundation Property Rights Grading Scale[28]

1 - Very high Private property guaranteed by government; court system efficiently enforces contracts; justice system punishes those who unlawfully confiscate private property; corruption nearly nonexistent, and expropriation highly unlikely.

2 - High Private property guaranteed by government; court system suffers delays and is lax in enforcing contracts; corruption possible but rare; expropriation unlikely.

3 - Moderate Court system inefficient and subject to delays; corruption may be present; judiciary may be influenced by other branches of government; expropriation possible but rare.

4 - Low Property ownership weakly protected; court system inefficient; corruption present; judiciary influenced by other branches of government; expropriation possible.

5 - Very low Private property outlawed or not protected; almost all property belongs to the state; country in such chaos (for example, because of ongoing war) that property protection nonexistent; judiciary so corrupt that property not effectively protected; expropriation frequent.[28]

Legal Barriers to International Law Enforcement Increases the Need for IP Owners to Safeguard their IP: "The FTC works to shut down illegal spammers through civil actions. But a loophole in federal law prevents its investigators from sharing information with other countries. That makes it tough for the agency to punish spammers and spyware distributors who have gone global, setting up homes, bank accounts and servers in separate countries. We have got to be able to work with our sister agencies in other countries," said FTC Commissioner Jon Leibowitz at a conference in Washington, D.C. "We can't give them information. We're not allowed to." In addition, he said, consumer protection agencies in other countries are reluctant to provide confidential investigative information to the FTC because it would be available to the public through Freedom of Information Act."

"The Senate passed a bill in March that would solve both problems, but it has been stuck in a House subcommittee since April. The bill, called the U.S. SAFE WEB Act, would allow information-sharing among the FTC and agencies abroad and would protect the foreign information from public disclosure. Rep. Cliff Stearns, R-Fla., chairman of a House subcommittee that handles consumer protection issues, said he wants the panel to take up the antispam bill this fall."[29]

Recommendation A – IP Owner's Role: That IP owners step forward in this war against cyber criminals and implement current IP governance standards within existing regulations and supervisory guidances to minimize exposure to corporate identity theft (45% of phishing attacks) that pose challenges for law enforcement when phishing sites are located in foreign jurisdictions (70% of phishing cases). See Recommendations 4 to 4j1.

Impact of Phishing Risks on Consumer Confidence and Reputation Risks: Surveys from relatively neutral parties, when matched against the monthly phishing trends from APWG, show consumers are losing confidence in financial brands (reputation risk) and reducing their use of the low-cost internet channel at a rate that matches the growth of phishing risks. As of January 2006, the UK's Financial Services Authority released the results of their survey showing "Consumer confidence in internet banking is fragile."[30]

Surveys: Reputation Risks & Fragile Consumer Confidence	
6-05	Gartner Study Finds Consumer Confidence in Online Commerce Waning[31]
8-05	American Banker: Big Names Losing Ground with Consumers
9-05	BITS Consumer Confidence Toolkit: Data Security and Financial Services -"Potential Crisis in Consumer Confidence"[32]
1-06	Financial Services Authority: "Consumer confidence in internet banking is fragile"[30]
4-06	Deloitte: Financial Services industry fears risk to Reputation in battle against ID theft[33]

Primary Objective: Restoring and rebuilding consumer confidence and usage of internet brands by applying current regulations and supervisory guidances for IP

Owners in safeguarding corporate identities is our primary objective with our analysis and recommendations.

9 Issues to be addressed from the NPR: Our analysis and recommendations are directed to 9 issues within the Red Flag NPR as noted below.

Page	NPR Request for Comments
Issue 1 40789-40790	3. *Customer.* Section 114 of the FACT Act refers to ''account holders'' and ''customers'' of financial institutions and creditors without defining either of these terms. For ease of reference, the Agencies are proposing to define ''customer'' to encompass both ''customers'' and ''account holders.'' Thus, ''customer'' means a person that has an account with a financial institution or creditor. The proposed definition of ''customer'' is broader than the definition of this term in the Information Security Standards. The proposed definition applies to any ''person,'' defined by the FCRA as any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity. The Agencies chose this broad definition because, in addition to individuals, various types of entities (*e.g.*, small businesses) can be victims of identity theft. Although the definition of ''customer'' is broad, a financial institution or creditor would have the discretion to determine which type of customer accounts will be covered under its Program, since the proposed Red Flag Regulations are risk-based. The Agencies solicit comment on the scope of the proposed definition of ''customer.''

Recommendation 1 – Scope – Include Data Brokers and Credit Reporting Agencies: That organizations controlling consumer "identifying information" per the FTC's definition[34] and subject to GLBA, such as data brokers, credit reporting agencies, be subject to the corporate identity safeguarding requirements of the final NPR. We did not see data brokers or credit reporting agencies listed in the organizations subject to the Red Flag NPR and we are not sure if the proposed definition of "customer" includes these industries that own and profit from consumer identifying information. It makes sense to include these industries in light of similar industries that are referenced in this NPR statement, i.e., "The Agencies expect that the final Red Flag Regulations will apply to a wide-variety of financial institutions and creditors that offer many different products and services, from credit cards to certain cell phone accounts." (40791)

2 Pivotal Issues: The next two issues are pivotal in our analysis and recommendations.

Issue 2 40790	**Pivotal Issue: "**5. Red Flag." "The Agencies request comment on the scope of the definition of ''Red Flags'' and, specifically, whether the definition of Red Flags should include ***precursors*** to identity theft."

40790	As context for this issue, we quote the entire section addressing "***precursors*** to identity theft form the NPR. 5. *Red Flag.* The proposed definition of a ''Red Flag'' is a pattern, practice, or specific activity that indicates the possible risk of identity theft. This definition is based on the statutory language. Section 114 states that in developing the Red Flag Guidelines, the Agencies must identify patterns, practices, and specific forms of activity that indicate ''the possible existence'' of identity theft. In other words, the Red Flags identified by the Agencies must be indicators of ''the possible existence'' of ''a fraud committed or attempted using the identifying information of another person without authority.'' Section 114 also states that the purpose of the Red Flag Regulations is to identify ''possible risks'' to account holders or customers or to the safety and soundness of the institution or ''customer'' from identity theft. The Agencies believe that a ''possible risk'' of identity theft may exist even where the ''possible existence'' of identity theft is not necessarily indicated. For example, electronic messages to customers of financial institutions and creditors directing them to a fraudulent website in order to obtain their personal information (''phishing''), and a security breach involving the theft of personal information often are a means to acquire the information of another person for use in committing identity theft. Because of the linkage between these events and identity theft, the Agencies believe that it is important to include such ***precursors*** to identity theft as Red Flags. Defining these early warning signals as Red Flags will better position financial institutions and creditors to *stop identity theft at its inception*. Therefore, the Agencies have defined ''Red Flags'' expansively to include those ***precursors*** to identity theft which indicate ''a possible risk'' of identity theft to customers, financial institutions, and creditors.

The noun "precursor" is defined by *Merriam-Webster's Medical Dictionary as* "(1) one that precedes and indicates the onset of another and (2) a substance, cell, or cellular component from which another substance, cell, or cellular component is formed especially by natural processes." By applying this definition and combining it with (A) the objective per the NPR, i.e., "Defining these early warning signals as Red Flags will better position financial institutions and creditors to stop identity theft *at its inception*" and (B) the foregoing metrics from the Antiphishing Working Group that state approximately 45% of phishing attacks use domain names within the fraudulent web sites, then to be consistent with the objective of stopping corporate identity theft at its inception, we submit the following recommendation.

Recommendation 2 – Red Flag Risks #24 and #25: That the revised Red Flag Risks per Appendix J, #24 and #25 for the NPR be changed by replacing "fraudulent web sites" with the earliest stage of corporate identity theft, i.e., "infringing domain names." Infringing domain names are confusingly similar and violate trademark rights (common law or federal) of an IP owner. Infringing domain names are further defined as domain names likely to be awarded to an IP owner based on comparable risks and arbitration cases in the Uniform Domain Name Dispute Resolution Policy or other country-based domain name dispute resolution standards." Applying this revised definition of a Red Flag Risk recognizes that domain names are the first building block or stage in building fraudulent web sites and corporate identity theft. This is also consistent with supervisory guidances from the FFIEC Information Security Handbook that are omitted from the NPR whereby IP owners are directed to prevent, detect and report infringing domain name risks to Boards and Law Enforcement per Suspicious Activity Reports.

(IP) Intellectual Property Governance					IT Governance	
External, Beyond IT Perimeter Risks					Internal System Risks	
Metrics on IP Governance					Metrics from APWG	
Brands (Global)	TM's/® (Global)	Domain Names (Global)	Fraudulent Web Sites (App. J: 24,25)	Phishing Sites	Pharming Attacks	Spyware, Trojans
			Red Flag Risks per NPR			
		Revised Red Flag Risks (Recommendation 2)				

Next Pivotal Issue: For the following NPR request for comment (Issue 3), we also refer to Addendum B and cite Red Flag Risks #24 and #25 from Appendix J.

Issue 3 40791	1. Identification and Evaluation of Red Flags; i. Risk-Based Red Flags: "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft. The Agencies request comment on whether the enumerated sources of Red Flags are appropriate."

We agree with the overall premise of this comment that "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft." We, however, disagree with the application of this responsibility as drafted within Appendix J and the Red Flag Risks #24 and #25 (see below) whereby the responsibility for detecting and reporting fraudulent web sites (subject to modification to include infringing

domain names per Recommendation 2) rests with Customers and not the IP owners.

Notice From Customers or Others Regarding Customer Accounts (Appendix J)						
24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.						
25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent Web site that looks very similar, if not identical, to the Web site of the financial institution or creditor.						
	OCC 40811	FRB 40814	FDIC 40817	OTS 40820	NCUA 40823	FTC 40826

In existing supervisory standards, IP owners are obligated to prevent, detect and report infringing domain names to law enforcement and boards of directors through Suspicious Activity Reports (SAR). We acknowledge that the NPR includes "notifying law enforcement and filing SARs" as a Red Flag obligation in Appendix J but for clarity and consistency of responsibility in reporting Red Flag Risks per Recommendation 2, we submit the following recommendation:

Recommendation 3 – Red Flag Risks #24 and #25: That the primary responsibility for preventing, detecting and reporting corporate identity theft risks that include infringing domain name risks, fraudulent web sites and phishing sites (Recommendation 2) rests with the IP owner and not the customer as currently drafted in the NPR. Red Flag Risks #24 and #25 in Appendix J should be changed accordingly to reflect this Recommendation 3. (See Recommendation 4e1b – Litigation Risks Arising from Operational Risks.)

The impact of Recommendations 2 and 3 on the map of complementary programs (Appendix B) is shown in the following section.

(IP) Intellectual Property Governance						IT Governance
External, Beyond IT Perimeter Risks						Internal System Risks
Metrics on IP Governance						Metrics from APWG
Brands	TM's/®	Domain Names	Fraudulent Web Sites (App. J: 24,25)	Phishing Sites	Pharming Attacks	Spyware, Trojans
			Customers Report Fraudulent Web Sites (Red Flags 24, 25)	Red Flag Risk 40790 40799		
		Recommendation 2 Infringing Domain Names defined as				

		a corporate identity theft risk and Red Flag Risk.				
		Recommendation 3 IP Owners are responsible for preventing, detecting and reporting infringing domain name risks as Red Flag Risks. (Recommendation 2) (App. J: 24,25)				
IP Owned By Firm		Layered Information Security Solution: FDIC FIL-103-2005				

Issue addressed below:

Issue 4 40804, 40807	E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules: "The Board is unable to identify any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred."

Issue 4 is positioned in this analysis to build upon the foregoing domestic and international corporate identity theft risks and matching Recommendations A and 1 - 3. The map is repeated for ease of reference. This identifies relevant supervisory guidance included in the NPR from each Program as well as omitted from the Information Security Program as it relates to corporate identity theft.

Information Security Program (GLBA) 40780 | 40789 | 40804			Identity Theft Prevention Program The program must address financial, operational, compliance, reputation, and litigation risks. (40790)			
40788	Combine Information Security and Identity Theft Programs					40804
40780	Scope of Organizations Covered by the NPR					40790
(IP) Intellectual Property Governance						IT Governance
External, Beyond IT Perimeter Risks						Internal System Risks
Metrics on IP Governance						Metrics from APWG
Brands (Global)	TM's/® (Global)	Domain Names	Fraudulent Web Sites (App. J: 24,25)	Phishing Sites	Pharming Attacks	Spyware, Trojans
IP Owned By Firm			Layered Information Security Solution: FDIC FIL-103-2005			
			Red Flag Risks: Fraudulent Access to Customer Information Bank Secrecy Act / Anti-Money Laundering Examination Manual (8/06)			

	legitimate sources"…that include "identity theft"… (12 of 367)	
Defining Red Flag Precursors The Agencies *request comment* on the scope of the definition of ''Red Flags'' and, specifically, whether the definition of Red Flags should include precursors to identity theft. (40790) Prevent, Detect, Mitigate Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft. The Agencies *request comment* on whether the enumerated sources of Red Flags are appropriate. (40791)	Corporate Identity Theft **Phishing Risks** 40790 | 40799 **Ref: Footnote 40 (40799)** OCC. Bulletin. "Risk Mitigation and Response Guidance for Web Site Spoofing Incidents". Bulletin 2005-24. 1 July 2005.[28] OTS. Letter. "Phishing and E-mail Scams" CEO Letter #193. 3 March 2004.[33] FFIEC's Information Security Handbook **Omitted Supervisory Guidances**	IT Solutions (7-18-06) Multi-Factor Authentication (MFA) Agencies 40799 | OCC 40802 | OTS 40805 OCC 40802 | OTS 40805 National banks and savings associations complying with the ''Interagency Guidelines Establishing Information Security Standards''A56 and guidance recently issued by the FFIEC titled ''Authentication in an Internet Banking Environment''A57 already will have policies and procedures in place to detect attempted and actual intrusions into customer information systems. (8-15-06) FFIEC FAQ's on Multifactor Authentication
Identification of Duplicative, Overlapping, or Conflicting Federal Rules 40804 | 40807 Omitted Regulations	The Board *seeks comment* regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred. (FFIEC "Privacy of Consumer Financial Information") — "We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information." Sarbanes-Oxley — Internal controls to detect fraud. Trademark Law — Rights & obligations for brands. Trade Secret Law — Rights & obligations for business secrets. SEC Disclosures — Representations for Investors.	

The top portion of the map is repeated below in order to focus on the concept in the Red Flag NPR that organizations subject to the Identity Theft Program may want to combine that Program with the complementary Information Security Program. By so doing and building upon the 3 supervisory guidances for corporate identity theft cited in Footnote #40, organizations impacted by the NPR should be aware that there are additional supervisory guidances from the FFIEC's Information Security Handbook and E-Banking Handbook on infringing domain name risks that are omitted from the Red Flag NPR but are directly relevant for the Identity Theft and Information Security Programs. These are cited in Appendix C[35] of the FFIEC's Information Security Handbook (updated 7-27-06) and are referenced in the table below:

Information Security Program (GLBA) 40780 | 40789 | 40804		Identity Theft Prevention Program The program must address financial, operational, compliance, reputation, and litigation risks. (40790)
40788	Combine Information Security and Identity Theft Programs	40804
40780	Scope of Organizations Covered by the NPR	40790
(IP) Intellectual Property Governance		IT Governance
External, Beyond IT Perimeter Risks		Internal System Risks

Metrics on IP Governance					Metrics from APWG	
Brands	TM's/®	Domain Names	Fraudulent Web Sites (App. J: 24,25)	Phishing Sites	Pharming Attacks	Spyware, Trojans
IP Owned By Firm		Layered Information Security Solution: FDIC FIL-103-2005				
		Red Flag Risks: Fraudulent Access to Customer Information Bank Secrecy Act / Anti-Money Laundering Examination Manual (8/06) "Terrorists generally finance their activities through both unlawful and legitimate sources"…that include "identity theft"… (12 of 367)[7]				

Footnote 40: Applicable Supervisory Guidance (IP Governance) (40799)
OCC. Bulletin. "Risk Mitigation and Response Guidance for Web Site Spoofing Incidents". Bulletin 2005-24. 1 July 2005.[36]
OTS. Letter. "Phishing and E-mail Scams" CEO Letter #193. 3 March 2004.[37]
FFIEC's Information Security Handbook[35]
Applicable Supervisory Guidance: Omitted in Footnote 40 (IP Governance)
Source: Appendix C of the FFIEC's Information Security Handbook (7-27-06)[35]
FDIC. Bank Technology Bulletin. "Protecting Internet Domains". FIL-77-2000. 8 November 2000.[38]
FDIC. Financial Institution Letter. "Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes". FIL-27-2004. 12 March 2004.[39]
FDIC. Financial Institution Letter. Identity Theft Study on "Account Hijacking" Identity Theft and Suggestions for Reducing Online Fraud, FIL-132-2004. 14 December 2004.[40]
FDIC. Financial Institution Letter. "Pharming Guidance on How Financial Institutions Can Protect Against Pharming Attacks". FIL-64-2005. 18 July 2005.[41]
FDIC. Financial Institution Letter. FFIEC Guidance Authentication in an Internet Banking Environment, FIL-103-2005. 10 October 2005.[42]
OCC. Alert. "Protecting Internet Addresses of National Banks". Alert 2000-9.19 July 2000.[43]
OCC. Alert. "Customer Identity Theft: E-Mail-Related Fraud Threats". Alert 2003-11. Sept. 2003.[44]
NCUA. Letter. "Protection of Credit Union Internet Addresses" Letter 02-CU-16. December 2002.[45]
NCUA. Letter. "Fraudulent Newspaper Ads, Websites by Entities Claiming to be Credit Union" Letter 03-CU-12.[46]
NCUA. Letter. "E-Mail and Internet Related Fraudulent Schemes Guidance" Letter 04-CU-06.[47]
NCUA. Letter. "Phishing Guidance for Credit Unions And Their Members" Letter 05-CU-20.[48]
Applicable Supervisory Guidance: Omitted in Footnote 40 (IP Governance)
FFIEC's E-Banking Handbook[49]

The common theme within these omitted supervisory guidances is that IP owners are directed to prevent, detect and report infringing domain names through Suspicious Activity Reports and the Information Security Program. This includes registering available matching domain names, scanning for infringing uses and reporting infringing uses through Suspicious Activity Reports to law enforcement (FINCEN for banks) and Board of Directors. This is consistent with the 3 supervisory guidances included in footnote #40 (see map) as well as the requirement in the proposed Identity theft prevention and mitigation section of Subpart J that organizations are to report infringing domain names through Suspicious Activity Reports.

Recommendation 4 – Inclusion of Omitted Supervisory Guidances: In regards to the identification of duplicative, overlapping, or conflicting federal rules and supporting supervisory guidances on corporate identity theft risks for the

development and implementation of either the Identity Theft Program or the Information Security Program per Subpart J-Identity Theft Red Flags, it is recommended that the foregoing omitted supervisory guidances be incorporated as supervisory guidances in defining Red Flag Risks for each of the Agencies per their respective pages in the NPR. This is consistent with and reinforces earlier Recommendations A, 1, 2, and 3.

Subpart J: (d) Development and Implementation of Program: Supervisory Guidance (1) Identification and evaluation of Red Flags					
OCC 40809	FRB 40812	FDIC 40815	OTS 40818	NCUA 40821	FTC 40824

Recommendation 4a – Incorporating and Synchronizing: Incorporating and synchronizing these supervisory guidances for safeguarding domain names across all Agencies in either of the Complementary Programs will eliminate regulatory gaps between Agencies (systemic risk) that are exploited by cyber criminals. This will also provide common and consistent definitions of corporate identity theft risks across all Agencies when assessing operational risks under the Basel II NPR. Example, the FRB has not issued any supervisory guidances addressing the safeguarding of domain names but the FRB regulates the majority of the banks that will be subject to the proposed operational risks under the Basel II NPR. (Ref: Industry Impact). On September 5, 2006, the FRB, FDIC, OCC and OTS issued the Basel II NPR "proposing a new risk-based capital adequacy framework that would require some and permit other qualifying banks to use an internal ratings-based approach to calculate regulatory credit risk capital requirements and advanced measurement approaches to calculate regulatory operational risk capital requirements."[50] "Operational risk means the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events (including legal risk but excluding strategic and reputational risk)."[51] Operational risk is a central risk in the Identity Theft Prevention Program as noted on page 40815 of the Red Flag NPR: "(c) Identity Theft Prevention Program. Each financial institution or creditor must implement a written Identity Theft Prevention Program (Program). The Program must include reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, including financial, ***operational***, compliance, reputation, and ***litigation risks***, in the manner discussed in paragraph (d) of this section." For all of these reasons, we recommend a consistent application and inclusion of the foregoing supervisory guidances on domain name risks from the Red Flag NPR in the Final Rule for all of the NPR Agencies

Recommendation 4a1 – Operational Risk – A Defined Term: That Operational Risk in the Red Flag NPR be a defined term using the definition from the September 5, 2006 "Joint Notice of Proposed Rulemaking. Risk-Based Capital Standards: Advanced Capital Adequacy Framework", i.e., "Operational risk

means the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events (including legal risk but excluding strategic and reputational risk)."[51]

A detailed list of supervisory guidances from the foregoing omitted guidances that should be incorporated as internal controls in the final Red Flag rules for all Agencies is noted below.

Recommendation 4b – Layered Information Security Program: That a layered Information Security Program include the safeguarding of domain names plus additional authentication per the supervisory guidance in the FDIC's FIL-132-2004[40], dated 14 December 2004 and FIL-103-2005[42], dated 10 October 2005.

Recommendation 4c – Domain Name Board Report: That "the effectiveness of an insured institution's Internet domain name protection program should be addressed in periodic risk assessments and status reports presented to the institution's board of directors." This supervisory guidance, omitted from the NPR, is from the FDIC's FIL-64-2005[41], dated 18 July 2005. This is consistent with the requirements of the Red Flag NPR that periodic reports be submitted to the Board of Directors on the effectiveness of the Identity Theft Program as well as with the requirement under SARS for reporting a summary of SAR activity to Boards of Director.

Recommendation 4d – FFIEC's E-Banking Request Letter: That, as part of developing and maintaining an effective Identity Theft Program and Information Security Program, audits of corporate identity risks need to address and include the following supervisory guidances per the FFIEC's E-Banking Request Letter[52], dated August, 2003 that were omitted from the Red Flag NPR, i.e.,

4d1	Objective 1 – Determine the scope for the examination of the institution's e-banking activities consistent with the nature and complexity of the institution's operations.[52]
4d1a	A list of URLs for all financial institution-affiliated websites.[52]
4d1b	Copies of recent monitoring reports that illustrate trends and experiences with intrusion attempts, successful intrusions, fraud losses, service disruptions, customer complaint volumes, and complaint resolution statistics.[52]
4d1c	Copies of findings from, and management/board responses to, the following: • Internal and external audit reports. • Annual tests of the written information security program as required by GLBA.[52]
4d2	Objective 2 – Determine the adequacy of board and management oversight of e-banking activities with respect to strategy, planning,

	management reporting, and audit.[52]
4d2a	Internal or external audit schedules, audit scope.[52]
4d2b	Descriptions of e-banking-related training provided to employees including date, attendees, and topics.[52]
4d2c	Insurance policies covering e-banking activities such as blanket bond, errors and omissions, and any riders relating to e-banking.[52]
4d3	Objective 4 – Determine if the institution has appropriately modified its information security program to incorporate e-banking risks.[52]
4d3a	Samples of e-banking-related security reports reviewed by IT management, senior management, or the board including suspicious activity, unauthorized access attempts, outstanding vulnerabilities, fraud or security event reports, etc.[52]
4d3b	Documentation related to any successful e-banking intrusion or fraud attempt.[52]
4d4	Objective 6 – Assess the institution's understanding and management of legal and compliance issues associated with e-banking activities.[52]
4d4a	Policies and procedures related to e-banking consumer compliance issues including website content, disclosures, BSA, financial record keeping, and the institution's trade area.[52]
4d4b	A list of any pending lawsuits or contingent liabilities with potential losses relating to e-banking activities.[52]
4d4c	Copies of, or publicly available weblinks to, privacy statements, consumer compliance disclosures, security disclosures, and e-banking agreements.[52]

Future Applications: In looking ahead, listing and quantifying contingent liabilities, associated with remediation of infringing domain names from Recommendation 4d4b, fits in with periodic reports to the Board per Recommendation 4c, with internal controls per Sarbanes-Oxley (upcoming topic) and with an operational risk quantification system for litigation risks under the Basel II NPR.[53]. Additionally, analyzing the quality and accuracy of disclosure statements per Recommendation 4d4c fits in with the periodic reports to the Board per Recommendation 4c, with internal controls per Sarbanes-Oxley (upcoming topic) and with Board Policy on Disclosures under the Basel II NPR.[54]

Continuation of Issue 4 (Repeated below):

Issue 4 40804, 40807	E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules: "The Board is unable to identify any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent

	identity theft or mitigate identity theft that has occurred."

Issue 4e - Litigation Risk: The Red Flag NPR cites "litigation risk" 9 times within the context of the development and implementation of the Program on the following pages:

NPR Page	Section	Reference
40790	Section ll.90(c) Identity Theft Prevention Program	Proposed paragraph §ll.90(c) describes the primary objectives of the Program. It states that each financial institution or creditor must implement a written Program that includes reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, in the manner described in §ll.90(d). The program must address financial, operational, compliance, reputation, and ***litigation risks***.
40790		The risks of identity theft to a customer may include financial, reputation and litigation risks that occur when another person uses a customer's account fraudulently, such as by using the customer's credit card account number to make unauthorized purchases. The risks of identity theft to the safety and soundness of the financial institution or creditor may include: compliance, reputation, or ***litigation risks for failure to adequately protect customers from identity theft***; operational and financial risks from absorbing losses to customers who are the victims of identity theft; or losses to the financial institution or creditor from opening an account for a person engaged in identity theft. Addressing identity theft in these circumstances would not only benefit customers, but would also benefit the financial institution or creditor, and any person (who has no relationship with the financial institution or creditor) whose identity has been misappropriated.

OCC	FRB	FDIC	OTS	NCUA	FTC
40809	40812	40815	40818	40821	40824

"Subpart J—Identity Theft Red Flags § 41.90 Duties regarding the detection, prevention, and mitigation of identity theft. (c) Identity Theft Prevention Program."

"Each financial institution or creditor must implement a written Identity Theft Prevention Program (Program). The Program must include reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, including financial, operational, compliance, reputation, and ***litigation risks***, in the manner discussed in paragraph (d) of this section."

(d) Development and implementation of Program. (1) Identification and evaluation of Red Flags. (i) Risk-based Red Flags. At a minimum, the Program must incorporate any relevant Red Flags from: (A) Appendix J to this part; (B) Applicable ***supervisory guidance;***

Subpart J: (d) Development and Implementation of Program: (2) Identity theft prevention and mitigation: **Suspicious Activity Reports**

OCC	FRB	FDIC	OTS	NCUA	FTC
40810	40813	40815	40819	40821	40824

Litigations risks arising from corporate identity theft and its permutations, such as phishing, are separated into two distinct groups but are connected, we believe, by a duty of care and/or fiduciary responsibility of the Board and its senior

management to safeguard its intellectual property. The first group, Issue 4e1a, consists of legal actions and penalties that can be brought against the perpetrators or cyber criminals who initiate phishing risks, 45% of which use infringing domain names. The second group, Issue 4e1b, consists of legal actions and penalties that can be brought against a firm through civil law suits, regulatory fines and/or shareholder lawsuits for failing to safeguard its intellectual property with adequate internal controls per regulations and duty of care standards. Each group will be analyzed with a special focus on the role played by corporate identity theft as a lightning rod for litigation, in either group.

Issue 4e1a - Litigation Risks Applicable to Parties Committing Phishing:

U.S. Federal Criminal Statutes Applicable to Parties Committing Phishing: These are quoted from a presentation by Jonathan J. Rusch, Special Counsel for Fraud Prevention, US Department of Justice dated August 6, 2004.[55]

Identity Theft – 18 U.S.C. 1028(a)(7):

Elements:

- Knowingly using or transferring another (real) person's "Means of identification". "Means includes name, SSN, DOB, driver's license, passport number, unique biometric data, unique EIN, address, or routing code; or access device (e.g., credit card or financial account number).
- With Intent to commit/aid or abet any unlawful activity that constitutes a federal violation or state of local felony.

Penalties:

- Imprisonment (Maximum)
  - Fraud-Related Violation – 15 years imprisonment if, as a result of offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period.
  - Basic Violation – 3 years imprisonment
- Fine – maximum $250,000 for individuals
- Forfeiture – Any personal property used or intended to be used to commit offense.

Wire Fraud – 18 U.S.C. 1343

Elements:

- Scheme or artifice to defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises
- Transmits (or causes transmission of) by means of wire communication in interstate or foreign commerce.
- Writing, signs, signals, pictures, sounds for purpose of executing scheme or artifice.

Penalties:
- Imprisonment (Maximum)
  - 30 years imprisonment if violation affects a financial institution (e.g., bank or savings and loan).
  - 20 years imprisonment in other cases.
- Fine – Maximum $250,000 for individuals
- Forfeiture

Examples of Section 1343 Offenses
- Initial e-mails to prospective victims
- Victim response to bogus website or window
- Criminal's transmission of victim's personal and financial data to other computers across state or international borders.

Bank Fraud – 18 U.S.C. 1344

Elements:
- Knowingly executing, or attempting to execute scheme or artifice to defraud institutions, or to obtain money, funds, etc under financial institutions custody by means of false or fraudulent pretenses, representations, or promises.

Penalties:
- Imprisonment (Maximum) – 30 years imprisonment
- Fine – Maximum $250,000
- Forfeiture

Computer Fraud and Abuse – 18 U.S.C. 1030

Elements of Section 1030(a)(2)(c) Offense
- Intentionally accessing computer without authorization or exceeding authorization, and
- Thereby obtaining information from any protected computer if conduct involved interstate or foreign communication.

Penalties
- Imprisonment (Maximum)
  - Felony – 5 years if offense or attempt to commit offense committed for private financial gain, in furtherance of any criminal or tortuous action in violation of U.S. Constitution or U.S. federal or state law.
  - Basic offense – 1 year for first offense or attempt.
  - Fine.

Other federal laws are listed within the presentation dated 8-6-04.[55] Featuring the foregoing federal statutes shows the penalties for parties who commit phishing crimes, 45% of which are enabled by the fraudulent use of corporate identities.

Tennessee Law, Anti-Phishing Act of 2006, enacted July 1, 2006.
This law states: "It shall be unlawful for any person to represent oneself, either directly or by implication, to be another person, without the authorization or permission of such other person, through the use of the Internet, electronic mail messages or any other electronic means, including wireless communication, and to solicit, request, or take any action to induce a resident of this state to provide identifying information or identification documents."[56]

Penalty: $500,000 for a person who violates this law.

Valuation Implications: Trademark owners operating in Tennessee may seek to recover the greater of actual damages or five hundred thousand dollars ($500,000) per incident or trademark infringement.[56]

Recommendation 4e1a1 – Enforcement – Tennessee Banks: That the 225 banks operating in Tennessee, per the FDIC's deposit market share database, proactively apply their right to sue for trademark violations within phishing cases under the Anti-Phishing Act of 2006, and report the suspicious use of their infringing domain name, with a valuation of $500,000 (damages to be won), in Box 35u of the Suspicious Activity Report.

Recommendation 4e1a2 – New State Legislation: That the other 49 states enact similar legislation as the Tennessee Anti-Phishing Act of 2006[56] with the understanding that 70% of phishing sites are hosted outside of the USA.

Issue 4e1b - Litigation Risks Arising from Operational Risks: The second group of litigation risks consist of legal actions and penalties that can be brought against a financial firm through civil law suits, regulatory fines and/or shareholder lawsuits for failing to safeguard its intellectual property with adequate internal controls per regulations and duty of care standards.

Issue 4e1b1: Suspicious Activity Reports: Each of the Agencies reference SARS in the Red Flag NPR in a perfunctory manner without providing a discussion or analysis on the relevance of SARS for identity theft, litigation risks, or operational risks when in fact SARS fulfill 2 vital roles in the development and management of an effective Identity Theft and Information Security Program. The 2 roles are (A) information sharing with law enforcement and the Board of Directors and (B) either an indemnity shield or lightning rod for litigation. As an incentive to cooperate with law enforcement, firms that regularly submit SARS are immune from civil litigation and/or regulatory fines through the Safe Harbor provision.[57] Conversely, financial firms that fail to implement adequate internal controls per supervisory guidances, including the submission of SARS, are subject to civil litigation and/or regulatory penalties. This represents a litigation and operational risk.

Subpart J: (d) Development and Implementation of Program: (2) Identity theft prevention and mitigation: **Suspicious Activity Reports**					
OCC 40810	FRB 40813	FDIC 40815	OTS 40819	NCUA 40821	FTC 40824

Litigation Risk Exposures – Corporate Identity Theft: As background, each of the foregoing supervisory guidances on corporate identity theft (Issue 4 and Recommendation 4) state the relevant financial firms are to prevent, detect and report infringing domain names and related fraudulent web sites through SARS to FINCEN and their Board of Directors as a routine set of internal controls. It is also a fiduciary and duty of care issue for senior management to have adequate internal controls to detect, prevent and report fraud through Suspicious Activity Reports.[58] (Notice the FRB has no supervisory guidances on corporate identity theft; hence Recommendation 4a that all supervisory guidances be incorporated and synchronized between the Agencies.) It is also important to note 3 years ago, on July, 2003, FINCEN included box 35U for "identity theft" in its revised Suspicious Activity Report[57] following the release of supervisory guidances on identity theft (see above). And one month later, the FFIEC's E-Banking Handbook Request Letter[52] asked auditors to review suspicious activity reports to the Board of Directors (See Recommendation 4d3a). Detailed legal requirements for submitting SARS are listed under "FDIC Law, Regulations, Related Acts; Suspicious Activity Reports"[59] and in the current SARS report[57] released July 2003.

A pattern of failure to comply with the reporting requirements of SARS exposes a firm to civil litigation risks and regulatory penalties (operational risks per Basel II). Conversely, the filing of SARS provides a Safe Harbor indemnity from civil litigation and regulatory penalties as confirmed from this section in the current SARS form.[57] "**Safe Harbor** Federal law (31 U.S.C. 5318(g)(3)) provides complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to this report's instructions or are filed on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure".[57]

For more information on the Safe Harbor provision, please read the Interagency Advisory, "Federal Court Reaffirms Protections for Financial Institutions Filing Suspicious Activity Reports."[60]

Recommendation 4e1b1 - Reporting of SARS for Corporate Identity Theft and Phishing – Valuation Issues & Benchmarks: That submitting Suspicious Activity Reports for infringing domain names is required by the foregoing supervisory guidances cited in Issue 4 and Recommendation 4. The failure to do so exposes a bank to the possibility of civil litigation and/or regulatory fines, deprives law enforcement and Board of Directors of vital fraud information for an Information Security Program and/or Identity Theft Program that could lead to damages for shareholders, and it enables an infringing domain name to remain in the custody of an unauthorized party for future use. Based on the current SARS reporting requirements, infringing domain names are to be reported as Identity Theft in Box 35U under one of 3 conditions and valuation hurdles. These are noted below along with our description and analysis of the actual terms in the SARS report.[57]

$0	Section 2 of SARs for Phishing Sites where consumers reveal sensitive customer information in fraudulent web sites.
$5,000	Section 1b for infringing domain names where the identity of the perpetrator is known per the whois domain name records.
$25,000	Section 1c for infringing domain names where the identity of the perpetrator is not known per the whois domain name records.

Importance and Value of Domain Names:

Current valuation data points for infringing domain names include:

- the Tennessee Law, Anti-Phishing Act of 2006[56], which sets the minimum damages to be won by a trademark owner at $500,000 per phishing site (@45% of phishing sites use an infringing domain name).
- the FDIC, in it's supervisory guidance, FIL 64-2005, states "**Financial institution domain names are critical and valuable financial institution property** that should be protected. Financial institutions and their Internet banking customers may be vulnerable to data and financial loss if domain names are misused or otherwise redirected. Practices to monitor and protect domain names should be regularly reviewed and updated as part of a financial institution's ***information security program***."[41]
- the significant sums invested in marketing budgets each year by each financial institution to build brand awareness. While these sums do not appear, under current accounting rules, on the balance sheet for intellectual property, i.e., for brands and trademarks, marketing budgets play a direct role in building demand for brands. In fact, our research shows a direct correlation between the size of a firm's marketing budget and exposure to corporate identity fraud in those cases where firms have failed to enact the supervisory guidances per Issue 4 and Recommendation 4.

- A range of historical damages won by trademark owners, beginning in 2000, based on an infringing domain name is set forth below. Notice the rising trend in valuations from 2001 to 2003 for cybersquatting violations, a common risk amongst infringing domain names.

$25,000	'01 Damages for ernestandjuliogallo.com (holding it as real estate): E. and J. Gallo Winery v. Spider Webs Ltd., et al.[61]
$50,000	'02 Damages for pinehurstresort.com (dilution and cybersquatting): Pinehurst v. Wick[62]
$100,000	'03 Damages for gmatplus.com (dilution, cybersquatting): GMAT v. Raju[63]
$100,000 per domain	'00 Damages. Plaintiff owned the trademarks EB and ELECTRONICS BOUTIQUE, and operated a popular online store at "ebworld.com" and "electronicsboutique.com." Defendant registered the domain names with the misspellings "electronicboutique.com," "eletronicsboutique.com," "electronicbotique.com," "ebwold.com," and "ebworl.com," and operated websites at those names, all of which "mousetrapped" users with numerous pop-up advertising windows. The court ordered defendant to transfer the disputed domain names and enjoined defendant from using any domain name "substantially similar" to plaintiff's marks. Additionally, the court awarded plaintiff $500,000 in statutory damages. In justifying the maximum award of $100,000 per infringing domain name, the court noted that: (1) defendant admittedly earned between $800,000 and $1,000,000 annually from his cybersquatting activities, and (2) defendant "boldly thumb[ed] his nose at the rulings of this court and the laws of our country" by continuing his cybersquatting even after this court in another case enjoined him and assessed statutory damages and attorney's fees. Finally, the court awarded plaintiff over $30,000 in attorney's fees and costs. Elecs. Boutique Holdings Corp. v. Zuccarini[64]
$166,666	'02 Damages for watchreplica.com (counterfeiting, infringement, dilution, and cybersquatting). Louis Vuitton Malletier v. Veit[65]
$337,280	'02 Damages for entrepreneurpr.com. Plaintiff, owner of the registered mark ENTREPRENEUR for magazines, operated websites at the domain names "entrepreneur.com" and "entrepreneurmag.com." Among other claims, plaintiff sued defendant for trademark infringement (entrepreneurpr.com), unfair competition, and counterfeiting. The district court granted plaintiff's motion for summary judgment on its trademark-infringement and unfair-competition claims, awarded plaintiff $337,280 in damages, and enjoined defendant from using any marks confusingly similar to "Entrepreneur." Entrepreneur Media, Inc. v. Smith , 279 F.3d 1135[66]
$400,000	'04 Damages for medpets.com (dilution, infringement, unfair competition, cybersquatting). Petmed Express, Inc. v. Medpets.com, Inc.[67]
$500,000	'06 Damages per phishing site and infringing trademark or domain name for trademark owners operating in Tennessee per Anti-Phishing Act of 2006[56].
$500,000 (Rolex) $100,000 (Polo)	'00 Damages for Rolex and Polo. Defendant sold counterfeit watches and shirts bearing plaintiffs' trademarks ROLEX and POLO through his websites including "knockoffalley.com" and "replica4u.com." Noting the willful violations by defendant, the magistrate judge recommended statutory damages for trademark counterfeiting of $500,000 for Rolex and $100,000 for Polo. The court distinguished this case from storefront counterfeiting cases in which only $25,000 was awarded per trademark violation because those amounts "would plainly be inadequate to compensate the plaintiffs" here "[i]n view of the virtually limitless number of customers available to [defendant] through his Web sites." The magistrate judge also recommended awarding attorney's fees based on

	defendant's willful infringement and defendant's conduct that increased plaintiff's legal costs. Rolex Watch U.S.A., Inc. v. Jones , 2000 U.S. Dist. LEXIS 15082[68]
$2,500,000 per trademark	'06 Damages. Defendants used plaintiffs' trademarks in the metatags of their websites, and purchased the marks "Australian Gold" and "Swedish Beauty" as search keywords. The plaintiff-manufacturers sued for trademark infringement, false advertising, and unfair competition, and plaintiff ETS sued for interference with its distribution contracts. After a trial, the jury returned a verdict in favor of plaintiffs on trademark infringement and false advertising. The jury awarded: (1) plaintiffs Australian Gold and Advanced Technology Systems damages of $325,000 and $125,000, respectively, for infringement, and $35,000 and $15,000, respectively, for false advertising; (2) damages of $500,000 to ETS for its tortious interference claim, and (3) punitive damages to ETS of more than $4,000,000 on its tortious interference/conspiracy claims. Australian Gold, Inc. v. Hatfield , 436 F.3d 1228 (10th Cir. 2006)[69]
$28,945,515	'05 Damages for yesmoke.com (Sale of gray-market cigarettes): Philip Morris USA, Inc. v. Otamedia Ltd[70]

Issue: $0 Dollar Limit for Phishing Sites:

$0	Section 2 of SARs for Phishing Sites where consumers reveal sensitive customer information in fraudulent web sites.

Under Section 2 of the SARS report[57], released July 2003, a set of conditions could be interpreted to mean no dollar limits are required to submit a SARS in the event of a phishing attack using an infringing domain name of the bank to gain access to sensitive data of bank customer. Section 2, Computer Intrusion, states, "For purposes of this report, "computer intrusion" is defined as gaining access to a computer system of a financial institution to (b) Remove, steal, procure or otherwise affect critical information of the institution including customer account information. For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institutions that provide no access to institution or customer financial or other critical information."[57] In a case involving a phishing web site that uses infringing domain names of bank information security and intellectual property systems to gain access to customer financial or other critical information, then we believe a SARS should be reported in this situation with no dollar limits as required under Section 2.

Support for this position is provided in FINCEN's SAR Review Issue #9[71] whereby no dollar limits are being used in reporting corporate identity theft cases through SARS. This report also identifies a trend whereby many banks failed to report all phishing cases through SARS to FINCEN. FINCEN and the FBI also acknowledge, in this report, that ***spoofing involves trademark and other intellectual property violations***. The report states, "A dramatic change in the population occurred in the second quarter of 2004 as overall filing volume increased and the "Identity Theft" violation type appeared on the Suspicious Activity Report form. Reports using the "Identity Theft" violation type began with

216 filings in the second quarter of 2004, possibly indicating an association between computer intrusion and identity theft. This positive association between computer intrusion and identity theft continued into the first half of 2005. The addition of "Identity Theft" to the violation type field appeared to help better define computer intrusion as a violation. This adjustment also eliminated filings related to employee misconduct and fraudulently negotiated checks as computer intrusions. The drop in filings, coupled with important changes in observed activity, signifies a pivotal development driving the filing volume in 2004."[72]

"**Violation Amounts.** Generally, institutional filers were most likely to indicate that violation amounts involved in each occurrence equaled zero ($0); however, in the fourth quarter of 2003 and throughout the first two quarters of 2005, filers indicated violation amounts within the range of $1 to $9,999 more commonly than violation amounts equal to zero ($0). This clearly indicates an emerging trend in actual losses reported by institutional filers. Interestingly, the timing of this trend in violation amounts corresponded to the emergence of identity theft and debit card fraud as leading violations in early 2004. Further review of these violations indicated they typically occurred in the presence of spoofing/phishing attacks.[13] ([13] According to the Federal Bureau of Investigation, "Spoofing or phishing frauds attempt to make Internet users believe that they are receiving email from a specific, trusted source, or that they are securely connected to a trusted web site, when that is not the case. Spoofing is generally used as a means to convince individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. ***Spoofing also often involves trademark and other intellectual property violations.")*** The emergence of filers reporting financial loss and the emergence of identity theft and debit card fraud may support the theory that a new pattern of vulnerability involving spoofing/phishing attacks was on the rise throughout 2004 and into 2005.[73]

"The strong association between the FINCEN data and Anti-Phishing Working Group open source data allowed a model of activity to be developed for this institution based on the launch of the phishing email and the time of detection. This model identified that the average filing lead time for an incident of phishing/spoofing normally exceeded 60 days. The incident of phishing/spoofing typically: was identified after a customer reported an account as compromised; exceeded 25 days from date of the phishing/spoofing email; and occurred within either one week before or after the first of each month (i.e., August 24 through September 7). While the 2004 phishing/spoofing attacks reported by the Anti-Phishing Working Group identified attacks against large banking organizations, only a few were filers of computer intrusion-related Suspicious Activity Reports. Narrative analysis revealed that only two of the large banks actively and consistently reported phishing/spoofing attacks."[74]

Recommendation 4e1b1a - Reporting of SARS for Corporate Identity Theft and Phishing – Synchronized with the UK's Standards Implemented April 1, 2006: That the Agencies modify the current dollar reporting limits for SARS in relation to infringing domain names to match the guidelines within the UK's

Suspicious Activity Report (SAR) system, established April 1, 2006. British banks are to report individual and private sector fraud through SARs to the Serious Organised Crime Agency, with no £0[75], based on the following guidelines:

> "Fraud involves the obtaining of other people's money or assets by deception. A lot of fraud is committed directly against the Government and against the tax and the benefits systems. Her Majesty's Revenue and Customs and the Department of Work and Pensions respectively and not SOCA are responsible for responding to those threats, although SOCA will support them.
>
> Fraud is also committed against individuals and companies, in a wide variety of ways, and often by organised gangs. It is here that SOCA will operate. Some examples of such frauds include:
>
> - against banks, often involving false or stolen identities;
> - investment and advance fee frauds, in which individuals are enticed to pay over money against false promises of returns; and
> - forms of e-fraud exploiting the use of the internet by banks and commerce.
>
> Much fraud goes unreported, and despite the fact that frauds can cause companies and individuals significant damage, it is sometimes, mistakenly, seen as victimless. As well as generating money that can be used for future crimes, fraud means that everyone pays for more goods and services. In addition, it can cause significant personal difficulties and distress."[76]

Benefits from this modification include removing a USA regulatory hurdle that (1) probably causes confusion for US and British banks operating in the US, and (2) hinders the reporting of corporate identity theft risks to US Law Enforcement and Boards of Directors. Synchronizing the reporting of corporate identity theft through Suspicious Activity Reports, using the UK's SOCA model as the most conservative, will also eliminate any potential distortions or advantages when calculating operational risk exposures under Basel II.

Recommendation 4e1b1b – Remediation Responsibility for Corporate Identity Theft: That concurrently with the filing of SARS, IP owners of infringing domain names commence remediation efforts to eliminate the infringing domain names as corporate identity theft and Red Flag risks (Recommendations 2 and 3) consistent with Recommendations A and 4 to 4j1 thus eliminating ongoing and/or repeat infringing uses that enable phishing cases, which are federal crimes. Measurement of remediation efforts and resulting exposure to corporate identity theft risks should be part of an effective Identity Theft Program and

Information Security Program given the goal of preventing identity theft at it's earliest stage per the Red Flag NPR.

Recommendation 4e1b2 – IP Owners: Primary responsibility for the remediation of the infringing domain name risks should not fall to law enforcement but rather to the IP owner. Why? 70% of the phishing risks are hosted in foreign jurisdictions that pose the foregoing cross-border legal hurdles for US law enforcement. Additionally, IP owners are directed by the foregoing supervisory guidances to safeguard their intellectual property and they have the best legal standing to defend and litigate intellectual property risks. Boards of Directors also have a Duty of Care and Fiduciary responsibility to safeguard their intellectual property. This is consistent with Recommendation 3 where we recommend the IP owner, rather than the customer, have the primary responsibility under Red Flag Risks #24 and #25 to prevent, detect and report corporate identity theft risks.

Recommendation 4e1b3 – Trademark Enforcement: That a litigation risk analysis and a program to develop and implement an Identity Theft and Information Security program include an independent assessment of the internal controls to (A) safeguard intellectual property rights, specifically trademarks, brands and domain names and to (B) detect, report and litigate trademark infringements. Quantifying trademark infringement risks as it relates to corporate identity theft risks and related operational risks (Basel II) should be an integral part of developing, implementing and managing an effective Identity Theft Program and Information Security Program. Omitted from the NPR, as it relates to corporate identity theft risks, is any reference to trademark law and how it obligates trademark owners to detect, prevent and mitigate trademark infringements or risk abandonment of exclusive use and related value of its trademarks. Within the context of corporate identity theft risks, we repeat the reference by FINCEN in its SARS Review #9[71] where it quoted from the FBI as follows: According to the Federal Bureau of Investigation, "Spoofing or phishing frauds attempt to make Internet users believe that they are receiving email from a specific, trusted source, or that they are securely connected to a trusted web site, when that is not the case. Spoofing is generally used as a means to convince individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. ***Spoofing also often involves trademark and other intellectual property violations.")***

Under Trademark Act Section 43, a trademark owner is entitled to stop newcomers from using indicia of origin that are confusingly similar to its trademark or service mark in ways that are likely to cause confusion, to cause mistake, or to deceive. Under Trademark Act Section 45, 15 U.S.C. 1127, indicia of origin can include words, names, symbols or devices or combinations thereof. Domain names fall within the scope of this definition. Consequently, under the Anti-Cybersquatting Consumer Protection Act, Trademark Act Section 43(d), 15 U.S.C. 1125(d), a trademark owner is entitled to stop newcomers from registering or using with an intent to profit a domain name that is confusingly similar to its trademark or service mark. Likewise, under ICANN Uniform Domain Name

Dispute Resolution Policy Paragraph 4(a), a trademark owner is entitled to seek transfer of a domain name that is confusingly similar to its trademark or service mark provided the current owner has no rights or legitimate interests in the domain name and provided further the domain name has been registered and is being used in bad faith. Despite the availability of these tools, trademark owners are not held meaningfully accountable for corporate identity theft. Consequently, it is exceedingly easy for criminals to steal a corporate identity and use it to facilitate phishing. Corporate identity theft is nearly the perfect crime.

Proactive steps to minimize the unauthorized use of corporate identities are as follows: First, a trademark owner should purchase available domain names, in each country of operation, that are confusingly similar to its trademarks or service marks so that they cannot be used to facilitate phishing. Second, a trademark owner should obtain through legal process or negotiation domain names owned by others that are confusingly similar to its trademarks or service marks. Third, a trademark owner should regularly search for, identify and secure domain names that are confusingly similar to its trademarks or service marks. (See foregoing supervisory guidances on corporate identity theft.) Scanning for infringing uses of domain names is part of the layered information security program, that includes multifactor authentication, as recommended by the FDIC in its Financial Institution Letter 103-2005, "FFIEC Guidance Authentication in an Internet Banking Environment."[42] And finally, senior management (i.e. business managers, financial officers and other personnel entrusted with business asset management) should make corporate identity an important part of an organization's overall business strategy.

As the number of domain names held by a trademark owner increases, phishing will decrease as criminals, finding it increasingly difficult to trick individuals into disclosing personal identifying information, choose to target the customers of less proactive trademark owners. Lost sales, damage to reputation, loss of trademark rights and unauthorized disclosure of confidential information due to infringement will be reduced. If the corporate identity of a trademark owner is more secure, then the personal identity of its customers is more secure, which will presumably result in increased business for the trademark owner. Trademark owners and especially, financial service providers, must be obliged to build protection from consumer and corporate identity theft into their practices, systems, and policies.

Recommendation 4e1b4 – Independent Counsel & Attorney-Client Privilege: A litigation risk audit needs to be conducted by independent trademark and trade secret counsel, under attorney-client privilege, with assistance from IP forensic auditors, in order to conduct an accurate analysis between historical SARs reports, that are highly sensitive trade secrets subject to regulatory protection, and current exposures to corporate identity theft risks that are reportable SARS events per the foregoing supervisory guidances. A failure to file Suspicious Activity Reports exposes a financial firm to regulatory fines and civil

litigation. Identifying and quantifying potential litigation risk is a central part of operational risks under the Basel II NPR. A supervisory guidance, omitted from the Red Flag NPR, addresses, as of January 20, 2006, the highly sensitive information within SARS plus recommendations on "Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies."[76] Additional reasons for an independent audit by counsel are to overcome 2 systemic risks. One is created by Sarbanes-Oxley whereby the auditor of the financial statements is prohibited from auditing intellectual property, unless special approval is granted by the Audit Committee. The other systemic risk is plausible deniability whereby company counsel avoids independent audits of IP assets to avoid knowledge of infringements because, with such knowledge, lawyers are ethically obligated to act. Independent counsel experienced with all of these issues in addition to Sarbanes-Oxley would be the ideal party to lead the development and implementation of the Identity Theft Program and Information Security programs as it relates to intellectual property issues.

Recommendation 4e1b5 – Public Policy Priorities: A reassessment of public policy priorities by federal regulators and law enforcement is recommended in the fight against anti-money laundering and identity theft as little attention, and possibly resources, has been given to corporate identity theft. Example #1: Regulators and FINCEN have cited numerous banks for failures to implement adequate internal controls in the fight against Anti-Money Laundering but no similar fines have been levied against banks on corporate identity theft risks despite the foregoing supervisory guidances on corporate identity theft. Banks fined by FINCEN since 2003 for failing to submit SARS, in the case of anti-money laundering cases[77], include: Liberty Bank of New York ($600,000 Civil Money Penalty)[78], BankAtlantic ($10,000,000 Civil Money Penalty)[79], Metrobank ($150,000 Civil Money Penalty)[80], ABN AMRO ($30,000,000 Civil Money Penalty)[81], AmSouth ($10,000,000 Civil Money Penalty)[82], Riggs ($25,000,000 Civil Money Penalty)[83], Banco de Chile ($3,000,000 Civil Money Penalty)[84], Korea Exchange Bank ($1,100,000 Civil Money Penalty)[85], and Western Union ($8,000,000 fine to NY State Department of Banking).[86] The similarities in risk profiles (NPR term: risk profile: page 40808) between anti-money laundering cases and banks with poor IP (intellectual property) governance are as follows, i.e., lack of adequate internal controls, independent audits, senior management involvement, centralized risk management, staff training and submission of Suspicious Activity Reports. Example #2: Annual reports due to Congress, under Section 526(b)[87] of GLBA or 15 USC, Subchapter II, Sec. 6826(b), by the FTC and Attorney General on the number and disposition of all enforcement actions taken, reveal 2 phishing prosecutions for the FTC during the 4 years ending 3-30-04, i.e., *FTC v. C.J.*, Civ. No. 03-5275[88] and *FTC v. Zachary Keith Hill*, Civ. Action No. H 03-5537[89]. No additional annual reports, under Section 526(b) of GLBA, could be found for the FTC for the period after 3-30-04. No annual reports, under Section 526(b) of GLBA, to Congress from the Attorney General or from the federal banking regulators could be found for 2000 to 2005. Policy

Issue: Administrative enforcement responsibilities under GLBA for prosecuting "fraudulent access to financial information" are vested and divided amongst the functional federal regulators as confirmed by links from the FFEIC[90] and FTC[91] under "15 USC, Subchapter II, Sec. 6822.[91] Members of the President's Identity Theft Task Force, including the Agencies involved with the current NPR, hold the Congressional mandate to enforce GLBA. These members have a unique opportunity to apply and align current public policy so that the private sector plays its original and natural role in safeguarding its IP in the battle against identity theft.

Recommendation 4e1b5a – Public Policy Priorities - UK: That priorities established by the UK's Serious Organized Crime Agency's in April, 2006, that includes dedicating 10% of its operational efforts for individual and private sector fraud, be considered as a benchmark for US priorities in addressing similar identity theft risks.[92]

Recommendation 4e1b6 – State Banking Departments: To be included in a litigation risk assessment is the possibility that individual banks exposed to corporate identity theft risks may also face examinations and regulatory fines from state banking departments following the Western Union case and the NY Department of Banking. In this case, an audit of Western Union for Anti-Money Laundering violations by the NY State Banking Department resulted in an $8,000,000 fine paid to the State of NY. Other state banking departments, concerned about reputation and compliance risks associated with the foregoing supervisory guidances on preventing, detecting and reporting corporate identity theft risks as part of an Information Security Program under GLBA since 2000, may also commence audits of banks for their exposure to and role in enabling identity theft risks for consumers.

Recommendation 4e1b7 – Clarification of Internal Controls: That the definition of "controls" within the Red Flag NPR be expanded and clarified, for the purpose of operational risk and litigation risk audits, to include (A) internal controls for detecting, preventing, and reporting trademark risks (infringing domain names) and trade secret risks (management and reporting of SARS reports) per the supervisory guidances in Recommendation 4, (B) the Recommendations 4d to 4d4c from the FFIEC E-Banking Handbook, (C) the control risks cited by FINCEN in their Anti-Money Laundering investigations, and (D) Sarbanes-Oxley. Example, banks fined by FINCEN in the Anti-Money Laundering cases, per Recommendation 4e1b5, exhibited the following risk profile, i.e., lack of adequate internal controls, independent audits, senior management involvement, centralized risk management, staff training and submission of Suspicious Activity Reports. Control risks fit within the Basel II NPR for Operational Risk, which is defined as: "Operational risk means the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events (including legal risk but excluding strategic and

reputational risk)."[93] The term "controls" is featured in the Red Flag NPR in 2 sections, i.e.,

40788	*B. Proposed Red Flag Regulations* 1. Overview The Agencies are proposing Red Flag Regulations that adopt a flexible risk based approach similar to the approach used in the ''Interagency Guidelines Establishing Information Security Standards'' 3 issued by the Federal banking agencies (FDIC, Board, OCC and OTS), the ''Guidelines for Safeguarding Member Information'' issued by the NCUA,4 and the "Standards for Safeguarding Customer Information'' 5 issued by the FTC, (collectively, Information Security Standards), to implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801. Under the proposed Red Flag Regulations, financial institutions and creditors must have a written Program that is based upon the risk assessment of the financial institution or creditor and that includes *controls to address the identity theft risks identified.*
FDIC 40804	Under the proposed rule, financial institutions and creditors must have a written program that includes *controls* to address the identity theft risks they have identified. With respect to credit and debit card issuers, the program also must include policies and procedures to assess the validity of change of address requests. Users of consumer reports must have reasonable policies and procedures with respect to address discrepancies. The program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities, and be flexible to address changing identity theft risks as they arise. A financial institution or creditor may wish to combine its program to prevent identity theft with its information security program, as these programs are complementary in many ways.

Recommendation 4e1b7a - Internal Controls – Inclusion of Sarbanes-Oxley:
That Sarbanes-Oxley, which is not referenced in the Red Flag NPR, be applied as it relates to banks with assets or $1 billion or more[94], when assessing potential litigation and operational risks as well as in developing and implementing the Identity Theft and Information Security Programs for safeguarding a firm's intellectual property, including trademarks and trade secrets, i.e., customer information and Suspicious Activity Reports. Financial firms are already directed by the following supervisory guidances, omitted from the Red Flag NPR, to comply with Sarbanes-Oxley subject to exceptions for small firms:

FDIC. Financial Institution Letter. CORPORATE GOVERNANCE, AUDITS, AND REPORTING REQUIREMENTS; Effect of the Sarbanes-Oxley Act of 2002 on Insured Depository Institutions. FIL-17-03. March 5, 2003.[95]
FRB, OCC, OTS. Statement on Application of Recent Corporate Governance Initiatives to Non-Public Banking Organizations. SR 03-8. May 5, 2003.[96]

Sarbanes-Oxley, when applied to material assets such as intellectual property, directs that adequate internal controls be in place at the Board and CEO/CFO levels to detect fraud, impaired valuations and compliance with applicable laws and regulations. Quantifying the foregoing trademark litigation risks plus the cost of remediation for infringing trademarks are valuations needed by CEO's and CFO's to determine their materiality when (1) certifying, per Sarbanes-Oxley, that a firm has adequate internal controls to detect and report fraud on material assets and that there are no material events that would negatively impact a firm's stock price and (2) assessing operational risks per the Basel II NPR. False certifications carry significant penalties (litigation and operational risks) for the CEO and CFO.

Applying Sarbanes-Oxley to intellectual property assets is consistent with:

- the objectives of the FFIEC's E-Banking Handbook, omitted from the Red Flag NPR, and the related Recommendations 4d to 4d4c,
- Ernst & Young's presentation: "The Impact of SOX on Intellectual Property Management",[97] and
- the principles set forth in the following books, i.e.,
  - "Sarbanes-Oxley and Trademark Portfolio Management: Establishing Internal Controls for Compliance & Preventing Infringement"[98], by Paul W. Kruse, Esq. This book captures the essential ideas within the supervisory guidances (Recommendations 4 - 4d4c) for preventing, detecting, reporting and correcting corporate identity theft risks against the backdrop of Sarbanes-Oxley.
  - "Trade Secret Asset Management; An Executive's Guide to Information Asset Management, Including Sarbanes-Oxley Accounting Requirements for Trade Secrets"[99], by R. Mark Halligan and Richard F. Weyand. "Customer Information" is a trade secret[100] thus increasing the duty of care responsibilities for a Board of Directors in safeguarding a firm's intellectual property.

Additionally, in remarks by Governor Susan Schmidt Bies of the Federal Reserve on June 12, 2006 on the topic of "A Supervisor's Perspective on Enterprise Risk Management"[101], insight is provided on the relevance and importance of Sarbanes-Oxley as it relates to material weaknesses in internal controls.

"Section 404 of the Sarbanes-Oxley Act of 2002 requires each annual report of a public company to include a report by management on the company's internal control over financial reporting. Restatements by banking organizations alone resulted in the revision of a number of material weaknesses in internal control for the 2004 reporting period, fifty-two from the thirty-seven originally reported. This increase implies a significant amount of operational risk associated with the accounting process.

"Generally, examiners review the Sarbanes-Oxley 404 process to determine whether the organization has a clear understanding of the roles of the audit committee, management, internal audit, and the external auditor and whether the organization has implemented an effective plan to achieve the objectives and requirements of Sarbanes-Oxley 404. Examiners also review the Sarbanes-Oxley 404 process to determine whether the organization has an effective follow-up strategy for the remediation of significant deficiencies and material weaknesses. Examiners are encouraged to utilize the results of the Sarbanes-Oxley 404 process, where possible, in their overall assessment of the organization's risk-management and control process and in the risk scoping of safety-and-soundness examinations and inspections."[101]

The very next point addressed by Governor Susan Schmidt Bies is "Information Security" where she states **"***Issues involving information security and identity*

theft have received quite a bit of attention from the federal government over the past several years. In fact, just recently, President Bush signed an executive order that created an Identity Theft Task Force for the purpose of strengthening federal efforts to protect against identity theft. The heads of the federal bank regulatory agencies are designated members of this task force; and as supervisors of financial institutions, I believe we can offer a unique perspective on this issue."[101]

The relevancy of Sarbanes-Oxley is also addressed in a January 2006 report by the Federal Reserve Bank of New York on "Industry Sound Practices for Financial and Accounting Controls at Financial Institutions."[102] This includes, "Section 2 Existing Laws, Regulatory Requirements, and Supervisory Guidance", which states, "Extensive laws, regulations, and supervisory guidance exist that stress the importance of accounting and financial controls. Among the laws are the Federal Deposit Insurance Corporation Act of 1991 (FDICIA) and the Sarbanes-Oxley Act of 2002 (SOX). Various regulatory agencies, including the Securities and Exchange Commission (SEC), the Board of Governors of the Federal Reserve System (FRB), and the PCAOB have promulgated rules and regulations and issued guidance concerning accounting and financial controls under these and other laws. In addition, private entities, such as the American Institute of Certified Public Accountants (AICPA) and other non-governmental entities, have issued guidance on this topic. In general, the laws, regulations and guidance emphasize the need for strong financial controls and require companies to devise and maintain an adequate system of internal accounting controls. However, none of the existing laws, regulations or guidance specifically identifies comprehensive sound practices for accounting or financial controls. In this section, we briefly review FDICIA and SOX on accounting and financial controls, and the regulatory and guidance structure that supports those laws."[102]

In regards to Sarbanes-Oxley Section 404, the report states, in Section *2.2 SOX – Section 404, "*SOX enhanced and expanded regulatory requirements for corporate internal controls over financial reporting to include all public companies, not only banks, while also adding requirements beyond what FDICIA called for in terms of enhanced documentation and testing. In particular, Section 404 of SOX (SOX 404) requires the management of a public company to assess and report on the effectiveness of internal controls over financial reporting and requires the company's external audit firm to express an opinion on management's assessment and to perform its own audit on the effectiveness of internal controls over financial reporting. SOX 404 has resulted in additional work for banking institutions to comply with the rules, such as end-to-end processes reviews, enhanced documentation, and an increase in testing. SOX 404 guidance describes the deliverables but is not specific on how to design financial controls or what constitutes sound practice for effective accounting and financial controls."[102]

The FRB report concludes in "Section 4.11 Boards/Audit Committees and senior management exercise effective oversight of financial controls" with these comments: "Law, regulation and guidance task Boards, through their Audit Committees, with exercising oversight over an institution's financial controls. In most cases, the Audit Committee reviews and evaluates financial performance and ensures that senior finance and accounting staff have appropriate knowledge and skills. Boards and Audit Committees are kept informed of current and emerging issues in accounting and financial reporting and regularly discuss their impact on the organization. Senior management is responsible for developing policies and implementing policies and practices to ensure that financial statements are accurate and internal controls over financial reporting are effective. It gives close attention to accounting control issues and approves corporate-wide policies that define the accounting control framework for the institution. Under Section 302 of SOX, the CEO and the CFO are required to attest that the quarterly financial statements are accurate, and they may be held personally liable if issues are uncovered or the financial statements are restated. As noted above, under SOX 404, senior management is also required to attest to the adequacy of controls over financial reporting."[102]

Sarbanes-Oxley: Section 906: Criminal Penalties: "Section 906 of Sarbanes-Oxley sets forth serious criminal penalties for certifying false financial statements. These penalties include fines up to $1,000,000 and jail terms up to ten years for knowingly certifying a false report, and fines up to $5,000,000 and jail terms up to twenty years for willfully certifying a false report. The act thus requires certification by CEO's and CFO's, while providing significant penalties for false certifications. Congress clearly intended that Sarbanes-Oxley be taken seriously."[103]

Recommendation 4e1b7b - Internal Controls – Sarbanes-Oxley – Accounting Gap Risks for Intellectual Property: That Boards of Directors and CEO's/CFO's engage independent counsel, under attorney-client privilege, with assistance from independent forensic IP accounting firms, per Recommendation 4e1b4, to develop and implement an Identity Theft Program and Information Security Program, with adequate internal controls, as it relates to intellectual property and specifically corporate identity theft risks in order to overcome systemic accounting gap risks for intellectual property, i.e.,

- auditors of financial statements apply industrial-age accounting standards for tangible assets and acquired intangible assets under FASB 141 and 142[103] but they do not audit, in the digital age, home-grown intellectual property.
- auditors of the financial statements are prevented, under Sarbanes-Oxley, from conducting non-audit fee-based consulting services[104] such as IP Governance audits.

Recommendation 4e1b7c – SOX 409 Disclosure: That Boards of Directors and CEO's/CFO's consider a disclosure, for the initial risks discovered from

Recommendation 4e1b7a, under Section 409 of the Sarbanes-Oxley Act, "on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer . . . as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest."[105]

Recommendation 4e1b8 – Disclosure of Security Breaches: That a litigation risk audit consider the findings of the 2005[106] and 2006[107] CSI/FBI Computer Crime and Security Surveys. These address a disclosure problem for Boards of Directors, CEO's and CFO's, shareholders, consumers and law enforcement whereby the majority of firms, in the surveys, failed to disclose information security breaches to law enforcement and legal counsel for fear of the negative impact on a firm's reputation and stock price. A key finding from the 2006 report is that "The percentage of organizations reporting computer intrusions to law enforcement [and legal counsel] has reversed its multi-year decline, standing at 25% as compared to 20% in the previous two years."[108] The predominant reason given for not reporting…" was the perception that resulting negative publicity would hurt their organization's stock and/or image". *(This is consistent with recent research by Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou ("The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market,"* Journal of Computer Security, *Vol. 11, No. 3, 2003, pp. 431-448) that found reports of security breaches can adversely affect a firm's stock price.)*[109]

Recommendation 4e1b9 – Duty of Care & Fiduciary Responsibilities: That a litigation risk audit consider whether a financial firm has dutifully protected its intellectual property, more specifically its trademark rights and sought for the benefit of shareholders all potential damages arising from current infringements of its intellectual property. The foregoing supervisory standards outline the steps financial firms are to follow in regard to safeguarding its brands and domain names from fraudulent uses. Boards of Directors have a special obligation under the Duty of Care standard and fiduciary responsibilities to prevent wasting of intellectual property, to have adequate internal controls to prevent and detect fraud and to apply best market practices in safeguarding its intellectual property. Notable legal cases defining these standards include:

- TJ Hooper. "The court found that the defendants breached their duty of care even though they were following industry practice."[110] "The court determined that the defendant tugboat operator had failed to use reasonable prudence, due to its failure to equip its tugs with radios capable of receiving storm warnings. This, despite the fact that use of such radios was not a standard industry practice at the time." [111]
- George v. Celotex Corp., "Similarly, in George v. Celotex Corp., the U.S. Court of Appeals for the Second Circuit held that a manufacturer, as an expert in its field, has a duty to stay informed of advances in scientific knowledge related to its field. As a result, the court found that an asbestos

manufacturer should have acted upon a research report, which concluded that levels of worker exposure to asbestos, once considered safe, were not."[111]

- Kline v. 1500 Massachusetts Avenue Apartment Corp., In this case, "the U.S. Court of Appeals for the District of Columbia Circuit ruled that a landlord has an obligation to take protective measures to ensure that his or her tenants are protected from foreseeable criminal acts in areas "peculiarly under the landlord's control."[111]
- RSA Security ("RSA") "faced a shareholder lawsuit for failing to protect its intangible assets. Although the suit predated SOX, the shareholders alleged that RSA failed to maintain and protect its patents overseas, thus breaching a duty of care to protect against patent infringers. In 2001, RSA settled the lawsuit with its shareholders. The seven-figure settlement also resulted in a consent decree in which RSA would establish an internal control system to properly protect its intellectual property. Additionally, the shareholders received attorney's fees for the action."[112]
- Caremark International, Inc. "In 1994, Caremark has been charged with multiple felonies relating to violations of federal and state health care statutes. At issue in the shareholder derivative action was the scope of the fiduciary duty owed by the board of directors to shareholders. The suite claimed that the directors allowed a situation to develop and continue that exposed the corporation to enormous legal liability and that, in so doing, they violated a duty to be active monitors of corporate performance, The discussion portion of the Caremark decision noted that the board of directors has a fiduciary duty to ensure that it is reasonably informed about the corporation's activities and to exercise good faith efforts to ensure that adequate systems are in place to receive accurate and timely information so it can intervene to protect the interests of shareholders and the corporation."[113]

Continuation of Issue 4 (Repeated below):

Issue 4 40804, 40807	E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules: "The Board is unable to identify any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred."

Recommendation 4f - Information Security Standards – Credit Card Industry: That the final NPR rules on safeguarding corporate identity, including all of the foregoing Recommendations, be applied to the members of the credit card industry. The current information security standards of the credit card

industry only address traditional IT security issues and omit references to the concepts embedded in the foregoing supervisory guidances in Issue 4 and Recommendation 4 for preventing, detecting and reporting corporate identity theft risks. Examples: the original Payment Card Industry Data Security Standard, Version 1.0[114], and the new Payment Card Industry Data Security Standard, Version 1.1, issued in September 2006,[115] do not address corporate identity fraud risks for the brands of the issuing credit card companies.

Recommendation 4g - False Advertising or Misuse of Names to Indicate Federal Agency: That the federal banking agencies in the Red Flag NPR include as a relevant regulation "18 U.S.C. Section 709: False Advertising or Misuse of Names to Indicate Federal Agency"[116] This statute covers false advertising or representations, misuse or unauthorized use of words such as "national", "Federal", "United States", "reserve", "Deposit Insurance", federal deposit, or misuse of names such as FDIC, to convey the impression of Federal agency affiliation. The May, 2005 GAO report to Congress, "INFORMATION SECURITY Emerging Cybersecurity Issues Threaten Federal Information Systems" states, "Many agencies have not fully addressed the risks of emerging cybersecurity threats as part of their agencywide information security programs (including periodic risk assessments; security controls commensurate with the identified risk; security awareness training; and procedures for detecting, reporting, and responding to security incidents). For example, 17 of the 24 agencies indicated that they have not assessed the risk that the agency name or the name of any of its components could be exploited in a phishing scam."[117] Additionally, the report states, "our analysis of the incident-response plans or procedures provided by all 24 agencies showed that none specifically addressed spyware or phishing. Further, one agency indicated that spyware is not considered significant enough to warrant reporting it as a security incident."[118] The few cases of infringing domain names in violation of this statute and/or general trademark rights recovered through the Uniform Domain Name Dispute Resolution Policy since 1999 are as follows: (1) fedlineadvantage.com: D2004-0918 – Federal Reserve Banks[119], (2) fannimae.com: 114620 - Federal National Mortgage Association[120], (3) freddiemac.biz: 116767 - Federal Home Loan Mortgage Corporation[121], (4) freddymae.com: 128653 - Federal Home Loan Mortgage Corporation[122], (5) freddiemac.info: 154102 - Federal Home Loan Mortgage Corporation[123], (6) homesteps.info: 155173 - Federal Home Loan Mortgage Corporation[124], and (7) freddiemacmortgages.com, freddiemacmortgages.net, freddiemacmortgages.org, freddymacmortgages.com, freddiemacarms.com, freddiemacarms.net, freddiemacarms.info, freddymacloans.com, freddymacloans.net: 566605 - Federal Home Loan Mortgage Corporation.[125]

Continuation of Issue 4 (Repeated below):

Issue	E. Identification of Duplicative, Overlapping, or Conflicting Federal

4 40804, 40807	Rules: "The Board is unable to identify any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred."

Issue 4h - Accurate Confidentiality and Security Statements - Conflict with the Agencies' Privacy Regulations and related Disclosures: The Red Flag NPR is another positive step by the Agencies to address information security and identity theft risks that threaten the privacy and security of consumer financial information. The NPR references on page 40789 the Agencies' privacy regulations, which are defined in footnote 9. [Footnote 9- 12 CFR 40.3(i)(1) (OCC)[126]; 12 CFR 216.3(i)(1) (Board)[127]; 12 CFR 332.3(i)(1) (FDIC)[128]; 12 CFR 573.3(i)(1) (OTS)[129]; 12 CFR 716.3(j) (NCUA)[130]; and 16 CFR 313.3(i)(1) (FTC)[131]] We have added the URLs for each of these privacy notices in the corresponding footnotes. The privacy regulations for the FDIC, OCC, OTS, NCUA and FRB are based upon the final rules "Privacy of Consumer Financial Information"[132], published in the Federal Register on June 1, 2000 pursuant to section 504 of GLBA. The introduction to the Final Rules explains the purpose and objective of the Privacy disclosure regulations, i.e., "*Section* I*.4 Initial Privacy Notice to Consumers Required* The GLB Act requires a financial institution to provide an initial notice of its privacy policies and practices in two circumstances. For customers, the notice must be provided at the time of establishing a customer relationship. For consumers who are not customers, the notice must be provided prior to disclosing nonpublic personal information about the consumer to a nonaffiliated third party. The proposed rule implemented these requirements by mandating that a financial institution provide the initial notice to an individual prior to the time a customer relationship is established and the opt out notice prior to disclosing nonpublic personal information to nonaffiliated third parties. *These disclosures were required under the rule to be clear and conspicuous and to accurately reflect the institution's privacy policies and practices*."[133]

It further defines in "*H. Information Described in the Initial and Annual Notices" that* the initial and annual notices must include an accurate description of the following four items of information"…with the fourth one being…"Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information." Additionally, it states, "For each of these items of information above, you may use a sample clause from Appendix A. ***The Agencies emphasize that you may use a sample clause only if that clause accurately describes your actual policies and practices***." (Page 35187). In Appendix A, it provides the relevant example as follows: "**A–7—Confidentiality and security (all institutions)** You may use this clause, as applicable, to meet

the requirement of § 216.6(a)(8) to describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. *Sample Clause A–7:* ***We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information***."[134]

Over time, financial firms have modified the foregoing "Confidentiality and Security" clause to disclose for consumers 1 of 5 different "Privacy and Security" standards for their compliance or lack of compliance with federal standards to guard a consumer's nonpublic information, i.e.,

Our physical, electronic, and procedural safeguards *meet or exceed federal standards* regarding the protection of customer information.	We maintain physical, electronic, and procedural safeguards that *comply with federal standards* to guard your personal information.	(1) We maintain physical, electronic and procedural safeguards to guard information. (2) Using industry standard security techniques ensures that your personal financial information remains confidential.	Although our bank has taken reasonable precautions to assure account security, we reserve the right to disclaim responsibility/ liability for a breach of security that occurs for reasons outside our control.	"SampleBank is also not liable to you or any third party for any occurrences or damages directly or indirectly related to any phishing, pharming or other attacks or fraud committed against SampleBank, SampleBank.com, and SampleBank.com's URL, DNS or IP address, or a third party's ability to tap into your Internet connection via phone line, DSL, cable connection, or otherwise."
Privacy Security Rating #1	Privacy Security Rating #2	Privacy Security Rating #3	Privacy Security Rating #4	Privacy Security Rating #5

Recommendation 4h – Accurate Confidentiality and Security Statements Verified By Boards of Directors: That the Board of Directors, as part of developing and implementing an effective Information Security and/or Identity Theft Program, obtain an independent risk assessment of it's firms compliance with all relevant information security regulations and supervisory guidances, including the foregoing supervisory guidances on corporate identity theft, and then select one of the foregoing "Privacy and Security" statements that ***accurately*** describes its information security practices under GLBA 504. This recommendation is consistent the standard detailed in the Basel II NPR that

states: ”Each bank holding company is required to have a formal disclosure policy approved by the board of directors that addresses its approach for determining the disclosures it makes. The policy must address the associated internal controls and disclosure controls and procedures. The board of directors and senior management must ensure that appropriate verification of the disclosures takes place and that effective internal controls and disclosure controls and procedures are maintained.[135]

Identifying each of the Privacy and Security statements with a corresponding Privacy Security Rating will help all stakeholders conduct a peer review on the standards approved by a Board of Directors for safeguarding their customer’s identifying information.

Issue 4i – Litigation Risks from State Laws: Omission from the NPR of the potential for litigation risks filed pursuant to state laws that provide greater protections than are provided by Title V of GLBA. In the final rules, “Privacy of Consumer Financial Information”, published in the Federal Register on June 1, 2000 pursuant to section 504 of GLBA, it states on “Section I.17, Relation to State Laws, Section 507 of the GLB Act that Title V does not preempt any State law that provides greater protections than are provided by Title V. Determinations of whether a State law or Title V provides greater protections are to be made by the Federal Trade Commission (FTC) after consultation with the agency that regulates either the party filing a complaint or the financial institution about whom the complaint was filed, and may be initiated by any interested party or on the FTC’s own motion.”[136] California’s AB1950 is cited, in a 12-31-05 10-K from Friedman, Billings, Ramsey Group, Inc., as one such privacy law.“[137]

Regulatory Developments.
In recent years, federal and state legislators and regulators adopted a variety of new or expanded regulations, particularly in the areas of privacy and consumer protection. We summarize these regulations below.
Privacy
The federal Gramm-Leach-Bliley financial reform legislation imposes additional obligations on us to safeguard the information we maintain on our borrowers. Also, several states are considering even more stringent privacy legislation. California has passed legislation known as the California Financial Information Privacy Act and the California On-Line Privacy Protection Act. Both pieces of legislation became effective July 1, 2004, and impose additional notification obligations on us and place additional restrictions upon information sharing with non-affiliated third parties. The more stringent information provisions of these laws are not pre-emptied by existing federal laws. In addition, the California Information Safeguard Law AB1950 imposes the obligation on businesses to establish procedural and electronic safeguards to protect customer personal information. If other states choose to follow California and adopt a variety of inconsistent state privacy legislation, our compliance costs could substantially increase.[137]

California AB 1950 was cited in Congressional testimony on March 23, 2006 as a 3rd major Information Security Requirement Applicable to U.S. Businesses following GLBA and HIPAA. “A third information security requirement applicable to many U.S. businesses is found in California AB 1950 and its analogs in other

states, such as Arkansas and Texas. AB 1950 requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect the information from unauthorized access, destruction, use, modification or disclosure. The law also requires businesses that disclose personal information to nonaffiliated third parties to require by contract that those third parties maintain reasonable security procedures."[138]

"Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide". "Businesses can comply with A.B. 1950 by performing a risk management analysis and borrowing security standards from the federal Gramm-Leach-Bliley and the Health Insurance Portability and Accountability Acts."[139]

Risk of Civil Litigation for not complying with GLBA's Information Security Program: California resident's experiencing a privacy breach due to a failure of a business operating in California to maintain an adequate information security program per GLBA standards may institute a civil action to recover damages.[140]

Recommendation 4i- Due Diligence for California Businesses: That firms operating in California subject to GLBA carefully review their compliance with GLBA's Information Security Program including all of the supervisory guidances in Appendix C of the FFIEC's Information Security Booklet, especially those supervisory guidances addressing corporate identity theft risks, to understand their exposure to potential litigation risks arising from deficient Information Security Programs and fraudulent web sites. California resident's experiencing an Identity Theft arising from fraudulent web sites may be able to bring a civil law suit against the bank for failing to implement the supervisory guidances from Appendix C of the Information Security Booklet[30] that address corporate identity theft.

Continuation of Issue 4 (Repeated below):

Issue 4 40804, 40807	E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules: "The Board is unable to identify any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred."

Issue 4j - Conflict with Supervisory "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer

Notice"[141] dated March 29, 2005: In the context of complying with existing regulations and guidances on identity theft, the Red Flag NPR includes response programs on page 40799 and footnote #40 (see below) but it omits reference to the FFIEC's guidance noted above on "response programs" dated March 29, 2005. As background, the supervisory guidances directing banks to prevent, detect and report corporate identity theft risks have been addressed above. For this issue, the objective is to review and compare (a) the 3-29-05 Response Program which states banks are not obligated to disclose loss of sensitive customer information by consumers within fraudulent web sites with (b) the intent and goals of the NPR to minimize reputation risks for banks.

Issue 4i 40799	The NPR states "the Agencies believe that many financial institutions and creditors already have implemented some of the requirements of the proposed regulations implementing section 114 as a result of having to comply with other existing regulations and guidance, such as the regulations implementing section 326 of the USA PATRIOT Act, 31 U.S.C. 5318(l),38 the Information Security Standards that implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801, and section 216 of the FACT Act, 15 U.S.C. 1681w,39 and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and ***response programs***.40 (see Footnote 40 below)
40799	Footnote 40: *See*, *e.g.*, 12 CFR part 30, supp. A to app. B (national banks); 12 CFR part 208, supp. A to app. D–2 and part 225, supp. A to app. F (state member banks and holding companies); 12 CFR part 364, supp. A to app. B (state non-member banks); 12 CFR part 570, supp. A to app. B (savings associations); 12 CFR 748, app. A and B (credit unions); Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Booklet (the ''IS Booklet'') *available at http://www.ffiec.gov/guides.htm*; FFIEC ''Authentication in an Internet Banking Environment'' *available at http://www.ffiec.gov/pdf/authentication_guidance.pdf*; Board SR 01–11 (Supp) (Apr. 26, 2001) *available at: http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm*; ''Guidance on Identity Theft and Pretext Calling,'' OCC AL 2001–4 (April 30, 2001); ''Identity Theft and Pretext Calling,'' OTS CEO Letter #139 (May 4, 2001); NCUA Letter to Credit Unions 01–CU–09, ''Identity Theft and Pretext Calling'' (Sept. 2001); OCC 2005–24, ''Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents,'' (July 1, 2005); ''Phishing and E-mail Scams,'' OTS CEO Letter #193 (Mar. 8, 2004); NCUA Letter to Credit Unions 04–CU–12, ''Phishing Guidance for Credit Unions'' (Sept. 2004).

To begin, the 3/29/05 "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"[141] directs banks to respond in the following way to the loss of sensitive customer information in fraudulent web sites: "This final Guidance also applies to ''customer information,'' meaning any record containing ''nonpublic personal information'' (as that term is defined in § __.3(n) of the Agencies' Privacy Rules) about a financial institution's customer, whether in paper, electronic, or other form, *that is maintained by or on behalf of the institution*.7 Consequently, *the final Guidance applies only to information that is within the control of the institution and its service providers, and would not apply to information directly disclosed by a customer to a third party, for example, through a fraudulent Web site*."[141] We accept that this is now standard industry practice but it is also one obvious factor

contributing to consumers losing confidence with online banking and the proliferation of fraudulent web sites.

Recommendation 4j – Attempt to Reconcile: That the Agencies involved with the Red Flag NPR revisit the omitted supervisory guidance "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" and attempt to reconcile the current disclosure standards for the loss of sensitive information by a consumer in a fraudulent web site, i.e., no disclosure requirement by a bank to a customer, with the apparently conflicting objectives of the NPR and related proposed Red Flags. Notice on page 40790 of the NPR where it states: "5. *Red Flag.* The proposed definition of a ''Red Flag'' is a pattern, practice, or specific activity that indicates the possible risk of identity theft. This definition is based on the statutory language. Section 114 states that in developing the Red Flag Guidelines, the Agencies must identify patterns, practices, and specific forms of activity that indicate ''the possible existence'' of identity theft. In other words, the Red Flags identified by the Agencies must be indicators of ''the possible existence'' of ''a fraud committed or attempted using the identifying information of another person without authority.'' Section 114 also states that the purpose of the Red Flag Regulations is to identify ''possible risks'' to account holders or customers or to the safety and soundness of the institution or ''customer'' from identity theft. The Agencies believe that a ''possible risk'' of identity theft may exist even where the ''possible existence'' of identity theft is not necessarily indicated. For example, electronic messages to customers of financial institutions and creditors directing them to a fraudulent website in order to obtain their personal information (''phishing''), and a security breach involving the theft of personal information often are a means to acquire the information of another person for use in committing identity theft. Because of the linkage between these events and identity theft, the Agencies believe that it is important to include such precursors to identity theft as Red Flags. Defining these early warning signals as Red Flags will better position financial institutions and creditors to stop identity theft at its inception. Therefore, the Agencies have defined ''Red Flags'' expansively to include those precursors to identity theft which indicate ''a possible risk'' of identity theft to customers, financial institutions, and creditors."

Recommendation 4j1 – Additional Disclosure: If it is not possible to reconcile this disclosure issue with the NPR, then disclosing this fact, i.e., banks are not obligated to disclose the release of sensitive customer information by consumers in fraudulent web sites, alongside the Confidentiality and Security disclosure (see Recommendation 4h) will alert consumers to the full risk of fraudulent web sites. The additional disclosure will minimize potential litigation risk for not fully and prominently disclosing this risk for consumers.

Conclusion for Recommendations 4 to 4j1: Applying existing standards and regulations for safeguarding corporate identities with the same vigor and intensity

that banks encourage consumers to safeguard consumer identities will minimize systemic risks for corporate brands, reputations and customers that are being exploited by cyber criminals.

Issue 5 40793	4. Oversee Service Provider Arrangements: "The Agencies invite comment on whether permitting a service provider to implement a Program, including policies and procedures to identify and detect Red Flags, that differs from the programs of the individual financial institution or creditor to whom it is providing services, would fulfill the objectives of the Red Flag Regulations. The Agencies also invite comment on whether it is necessary to address service provider arrangements in the Red Flag Regulations, or whether it is self-evident that a financial institution or creditor remains responsible for complying with the standards set forth in the Regulations, including when it contracts with a third party to perform an activity on its behalf."

Recommendation 5 – Measuring Effectiveness – Service Providers: Assuming that a service provider already complies with all relevant regulations and supervisory guidances for the benefit of its banking clients, the service provider is probably best suited to deliver timely, sophisticated services in a more-cost effective manner for a small financial institution than if the same institution sought comparable services on a stand-alone basis in its community. Measuring the effectiveness of the solution from the service provider is, however, the same issue to be addressed by a Board of Directors for any institution subject to the NPR per Issue 3, which is repeated below.

Issue 3 40791	1. Identification and Evaluation of Red Flags; i. Risk-Based Red Flags: "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to *effectively* detect, prevent, and mitigate identity theft. The Agencies request comment on whether the enumerated sources of Red Flags are appropriate."

And as the NPR states, ultimately, the Board of Directors is responsible for developing, implementing and approving the Program. Measuring the effectiveness of the solution is thus an issue for all interested parties, especially the Board of Directors. For this reason, there needs to be a set of standards and metrics to gauge the effectiveness and to provide accountability in managing corporate identity risks within the Identity Theft and Information Security Programs.

Issue 6 40793	5. Involve the Board of Directors and Senior Management: "The Agencies request comment regarding the frequency with which reports should be prepared for the board, a board committee, or senior management. The Agencies also request comment on whether this paragraph properly allocates the responsibility for oversight and

	implementation of the Program between the board and senior management."

Issue 6 – Role of Board of Directors: This an appropriate stage in the analysis to address the role of the Board of Directors and Senior Management in fulfilling their obligations in developing and implementing an ***effective*** Identity Theft and Information Security Program. "Effective" is the key word in the NPR. It is defined by *Random House Unabridged Dictionary* as "adequate to accomplish a purpose; producing the intended or expected result". Effective and its derivatives, effectiveness and effectively, are cited in the following sections of the NPR as it relates to a describing the relative quality of the program:

40790 to 40791	Section ll.90(c) Identity Theft Prevention Program. Thus, to ensure the Program's *effectiveness* in addressing the risk of identity theft to customers and to its own safety and soundness, each financial institution or creditor must monitor, evaluate, and adjust its Program, including the type of accounts covered, as appropriate.
40793	5. Involve the Board of Directors and Senior Management. Proposed §ll.90(d)(5) highlights the responsibility of the board of directors and senior management to develop and implement the Program. The board of directors or an appropriate committee of the board must approve the written Program. The board, an appropriate committee of the board, or senior management is charged with overseeing the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation. In addition, persons charged with overseeing the Program must review reports that must be prepared at least annually by staff regarding compliance by the financial institution or creditor with the Red Flag Regulations. The reports must discuss material matters related to the Program and evaluate issues such as: The ***effectiveness*** of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for changes in the Program. This report will indicate whether the Program must be adjusted to increase its ***effectiveness***.
40793 to 40794	*C. Proposed Red Flag Guidelines: Appendix J*. The proposed list in Appendix J is not meant to be exhaustive. Therefore, proposed §ll.90(d)(1) of the Red Flag Regulations also provide that each financial institution and creditor must have policies and procedures to identify additional Red Flags from applicable supervisory guidance that may be issued from time-to-time, incidents of identity theft that the financial institution or creditor has experienced, and methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks. Ultimately, the financial institution or creditor is responsible for implementing a Program that is designed to ***effectively*** detect, prevent and mitigate identity theft.

OCC 40809 to 40810	FRB 40812 to 40813	FDIC 40815 to 40816	OTS 40818 to 40819	NCUA 40821 to 40822	FTC 40823 to 40825
Subpart J—Identity Theft Red Flags § 41.90 Duties regarding the detection, prevention, and mitigation of identity theft.	Subpart J—Identity Theft Red Flags§ 222.90 Duties regarding the detection, prevention, and mitigation of identity theft.	Subpart J—Identity Theft Red Flags § 334.90 Duties regarding the detection, prevention, and mitigation of identity theft.	Subpart J—Identity Theft Red Flags § 571.90 Duties regarding the detection, prevention, and mitigation of identity theft.	Subpart J—Identity Theft Red Flags § 717.90 Duties regarding the detection, prevention, and mitigation of identity theft.	PART 681—IDENTITY THEFT RULES 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(d) *Development and implementation of Program.*

(5) *Involvement of board of directors and senior management.*

(i) *Board approval*. The board of directors or an appropriate committee of the board must approve the

	written Program.
	(ii) *Oversight by board or senior management.* The board of directors, an appropriate committee of the board, or senior management must oversee the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation, and reviewing annual reports prepared by staff regarding compliance by the financial institution or creditor with this section.
	(iii) *Reports.*
	(A) *In general.* Staff of the financial institution or creditor responsible for implementation of its Program must report to the board, an appropriate committee of the board, or senior management, at least annually, on compliance by the financial institution or creditor with this section.
	(B) *Contents of report.* The report must discuss material matters related to the Program and evaluate issues such as: the ***effectiveness*** of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for changes in the Program.

Metrics from the Anti-Phishing Working Group show current regulatory, technology and law enforcement efforts at preventing phishing for the last 20 months fail to slow the rapid growth of this cyber crime, including corporate identity theft.

Recommendation 6 – Measuring Effectiveness – Board: That measuring the effectiveness of the policies and procedures of the Identity Theft and Information Security Programs must be a central issue for regulators, IP owners, ISP's, shareholders and consumers, alike especially as it relates to quantifying potential litigation and operational risks for the Complementary Programs as well as for the Basel II NPR (See Recommendation 6a10). In April 2006, the National Science and Technology Council released the "Federal Plan for Cyber Security and Information Assurance Research and Development".[142] It recommends that federal agencies "develop and apply new metrics to assess cybersecurity and information assurance".[143] It states further that, "Metrics can be defined as tools designed to facilitate decision making and improve performance and accountability, such as through the collection, analysis, and reporting of performance data. Operators can use such quantifiable, observable, and measurable data to apply corrective actions and improve performance. Regulatory, financial, and organizational factors drive the requirement to measure IT security performance. A number of laws, rules, and regulations require IT performance measurement in general and IT security assessment in particular. These laws include the Information Technology Management Reform Act (also known as the Clinger-Cohen Act), the Government Performance and Results Act, the Government Paperwork Elimination Act, the Federal Information Security Management Act, and the Healthcare Insurance Portability and Accountability Act. Other drivers are the national and homeland security implications of IT infrastructure vulnerabilities.

Potential security metrics cover a broad range of measurable features, from security audit logs of individual systems to the number of systems within an organization that were tested over the course of a year. Security metrics measure diversified multidimensional data collected in real time and analyzed. Effective security metrics should be used to identify security weaknesses,

determine trends to better utilize security resources, and measure the success or failure of implemented security solutions. Ultimately, the metrics should help characterize an organization's overall security posture from risk/threat/vulnerability, budgetary, and regulatory standpoints."[145]

Recommendation 6a - Omitted Factors to be Included for a Board: Factors omitted from the NPR that need to be considered by a Board of Directors in developing and implementing an effective Identity Theft Program and Information Security Program, include:

6a1	COSO: Internal Control - Integrated Framework (1994). This states, "Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations."[146]
6a2	FDIC: Risk Management Manual of Examination Policies. This states, "Bank management is responsible for preventing and detecting fraud and insider abuse: The primary responsibility to prevent fraud and insider abuse rests with the board of directors and senior management. To properly execute their fiduciary duties, management must implement internal controls and other safeguards to prevent fraud and theft whether internally or externally perpetrated. However, even the best safeguards can be circumvented; therefore, systems also must be designed to detect suspicious activities. Once detected, suspicious activities must be reported."[147]
6a3	FDIC Financial Institution Letter dated July 18, 2005 (FIL-64-2005). This states, "The effectiveness of an insured institution's Internet domain name protection program should be addressed in periodic risk assessments and status reports presented to the institution's board of directors."[148]
6a4	Duty of care and fiduciary responsibilities of Boards of Directors include safeguarding intellectual property. Failure to safeguard IP exposes a firm to shareholder lawsuits.
6a5	Boards of Directors for banks and credit unions are required to receive a summary of all Suspicious Activity Reports (SARS) submitted on infringing domain names. The failure of a bank or credit union to submit SARS exposes that firm to regulatory fines plus civil litigation.
6a7	Sarbanes-Oxley, when applied to material assets such as intellectual property, directs adequate internal controls be in place at the Board and CEO/CFO levels to detect fraud, impaired valuations and compliance with applicable laws and regulations.
6a8	Gramm-Leach-Bliley Act (GLBA) directs that a Board approve and maintain oversight of the firm's Information Security Program. In the

	Proposed Rules on Identity Theft Red Flags, a recommendation is made that "financial institutions may wish to combine its program to prevent identity theft with its information security program for compliance with GLBA as these programs are similar in many ways."[149]
6a9	Boards of Directors also need to address, in addition to the defined issues in the Red Flag NPR, these related risks • Intellectual property governance issues that cut across compliance, duty of care, fiduciary responsibility, and regulatory boundaries, • All disclosure statements, including forward-looking risks, about a firm's compliance and/or exposure to federal and state regulations on privacy and data security regulations, • Adequacy of internal controls for safeguarding intellectual property; and • Cyber insurance risks. These additional risks complement the core defined risks in the Red Flag NPR, which are as follows: "The risks of identity theft to the safety and soundness of the financial institution or creditor may include: compliance, reputation, or litigation risks for failure to adequately protect customers from identity theft; operational and financial risks from absorbing losses to customers who are the victims of identity theft; or losses to the financial institution or creditor from opening an account for a person engaged in identity theft."[149]
6a10	Operational risks within the context of the Basel II NPR will require a measurement analysis. As background, the Basel NPR includes two measurement approaches, i.e., "These approaches include the internal ratings-based (IRB) approach for credit risk and the advanced measurement approaches (AMA) for operational risk (together, the advanced approaches). The IRB framework uses risk parameters determined by a bank's internal systems in the calculation of the bank's credit risk capital requirements. The AMA relies on a bank's internal estimates of its operational risks to generate an operational risk capital requirement for the bank."[150] Additional information on the AMA for operational risk is quoted as follows: "2. The AMA for operational risk The proposed rule also includes the AMA for determining risk-based capital requirements for operational risk. Under the proposed rule, operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition of operational risk includes legal risk – which is the risk of loss (including litigation costs, settlements, and regulatory fines) resulting from the failure of the bank to comply with laws, regulations, prudent ethical standards, and contractual obligations in any aspect of the bank's

	business – but excludes strategic and reputational risks. Under the AMA, a bank would use its internal operational risk management systems and processes to assess its exposure to operational risk. Given the complexities involved in measuring operational risk, the AMA provides banks with substantial flexibility and, therefore, does not require a bank to use specific methodologies or distributional assumptions. Nevertheless, a bank using the AMA must demonstrate to the satisfaction of its primary Federal supervisor that its systems for managing and measuring operational risk meet established standards, including producing an estimate of operational risk exposure that meets a one-year, 99.9th percentile soundness standard. A bank's estimate of operational risk exposure includes both expected operational loss (EOL) and unexpected operational loss (UOL) and forms the basis of the bank's risk based capital requirement for operational risk. The AMA allows a bank to base its risk-based capital requirement for operational risk on UOL alone if the bank can demonstrate to the satisfaction of its primary Federal supervisor that the bank has eligible operational risk offsets, such as certain operational risk reserves, that equal or exceed the bank's EOL. To the extent that eligible operational risk offsets are less than EOL, the bank's risk-based capital requirement for operational risk must incorporate the shortfall."[151]

Recommendation 6b – FFIEC Standards to be Included by a Board: That Boards of Directors adopt and apply the following standards, in the development, implementation and ongoing management of the Identity Theft and Information Security Programs based on the relevant standards included in the FFIEC's Information Security Handbook and E-Banking Handbook, i.e.,

6b1	Include a "*Multidisciplinary and Knowledge Based Approach*—A consensus evaluation of the risks and risk mitigation practices requires the involvement of users with a broad range of expertise and business knowledge. Not all users may have the same opinion of the severity of various attacks, the importance of various controls, and the importance of various data elements and information system components. Management should apply a sufficient level of expertise to the assessment."[152]
6b2	"Acceptable Methodologies" for gathering necessary information, identifying information and information systems, analyzing the information and assigning risk ratings.[153]
6b3	"Review the website content for inclusion of …security disclosures"[154]
6b4	"Financial institutions should comply with all legal requirements relating to e-banking, including the responsibility to provide their e-banking customers with appropriate disclosures and to protect customer data.

	Failure to comply with these responsibilities could result in significant compliance, legal, or reputation risk for the financial institution."[155]
6b5	"Financial institutions should exercise care in selecting their website name(s) in order to reduce possible confusion with those of other Internet sites. Institutions should periodically scan the Internet to identify sites with similar names and investigate any that appear to be posing as the institution. Suspicious sites should be reported to appropriate criminal and regulatory authorities."[156]
6b6	Independent Audits. Independent individuals or companies conducting the audits without conflicting e-banking or network security roles."[157]

Recommendation 6c – Omitted Concepts By FFIEC to be Included by a Board: That Boards of Directors understand the FFIEC handbooks include the foregoing supervisory guidances on corporate identity theft but currently omit relevant intellectual property issues and concepts that must be included when addressing corporate identity theft risks, i.e.,

6c1	FFIEC Information Security model focuses on software, hardware, protocols and controls[158] but omits from its Glossary[159] and model these IP risks, i.e., phishing, domain names, brands and intellectual property.
6c2	FFIEC's E-Banking model focuses on "the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. This definition includes delivering services and products such as: account information, access to funds and business transactions and transfers through a public or private network"[160] This model, however, omits from its Glossary[162] and scope of services these IP risks, i.e., phishing, domain names, brands and intellectual property.

Recommendation 6d – Independent IP Governance Audits & Ratings: That Boards of Directors, in the development, implementation and ongoing management of the Identity Theft and Information Security Programs, obtain ongoing independent IP Governance audits, from industry experts, addressing the following interrelated issues, i.e.,

6d1: Audit Risks	Independent audits of trademarks and trade secrets led by independent counsel under attorney-client privilege. Engagements are led by a law firm, specializing in trademarks and Sarbanes-Oxley, under attorney-client privileges and are resourced with IP forensic auditors and insurance attorneys all of whom are free of conflicts. Independent IP audits are recommended to overcome audit gap risks, conflicts of interest, plausible deniability claims and to obtain unbiased information when designing either an Identity Theft or Information Security Program for

	corporate identity theft. Special attention needs to be given for litigation risks which are addressed below.
6d2: Litigation Audit Risk	That any firm and their Board of Directors when developing, implementing and managing their Identity Theft program needs to include a litigation risk audit that analyzes their exposure to civil litigation and regulatory fines for failing to have adequate internal controls to prevent, detect and report corporate identity theft risks per the foregoing supervisory guidances and SARs reporting requirements. A conservative litigation risk audit, in the spirit of the NPR's Section ll.90(c) Identity Theft Prevention Program that seeks to minimize operational, reputational and litigation risks from corporate identity theft, will assume all infringing domain name risks are eligible for SARS. Methodology for measuring exposure to litigation involves open source tools (available for consumers, state banking examiners, federal banking regulators, and shareholders – all potential sources of litigation) for identifying trademarks and domain names owned by a firm as well as confusingly similar domain names owned by and available for registration by infringing parties. Comparing infringing domain names to UDRP claims won by banks since 1999 establishes a universe of infringing domain names eligible for SARS reports and successful remediation through UDRP arbitration. Quantifying potential lost income from infringing domains from the combination of a lost revenue model and potential damage awards is the first valuation analysis. Estimating the cost of remediation to minimize corporate identity theft risks is the second valuation analysis. Each of these valuations should be reported to senior management and the Board of Directors as part of ongoing internal controls and operational risk assessments for safeguarding intellectual property.
6d3: Insurance Risk Audit	A special review of cyber insurance exposures is included in the IP Governance audit. Liability from the failure to file SARs reports or to comply with other government regulations may not be fully covered, or may not be covered at all, under many standard form insurance policies. The same is true for civil litigation related to cyber-specific threats, which often results in both a direct loss to the bank and third-party liability that very often is not covered by many of traditional insurance policies purchased by banks. Insurance industry insiders report that 36% or less of vulnerable banks have adequate cyber-insurance protection. For the most part, the standard form insurance

	policies held by banks may not cover losses such as damage to software and other computer system components, third-party liability from cyber crime and other related forms of loss. Further, it may not even be possible to obtain coverage for other types of loss, which may include regulatory fines and penalties. An independent review of cyber insurance policies is recommended, especially given the possibility under the Basel II NPR dated 9-5-06 that up to 20% of operational risk exposure may be offset by insurance providing such insurance has no exclusions or limitations based upon regulatory action.[162]
6d4: Direct Trademark and Trade Secret Risks, Remediation Budgets and Ratings	The law firm coordinates a full set of services that include audits of internal controls for detecting, reporting and safeguarding suspicious activity reports on identity theft risks, cyber insurance risk reviews, independent verification of infringing trademark risks, preparation, submission and management of UDRP arbitration cases, and domain name registration. Monitoring for new infringing domain name risks is 24x7 with immediate remediation services if needed. Monthly IP Governance Reports are delivered to the Board of Directors reflecting progress in remediation plus new risk exposures all converted to fresh Online Brand Ratings. An Online Brand Rating is a function of the (a) sum of positive points allocated for trademarks and domain names owned by an IP Owner plus (b) negative points allocated for available, matching domain names plus infringing domain names divided by (c) the number of unique brands. “F” Ratings indicate significant exposure to corporate identity theft. “A” Ratings indicate minimal exposure to corporate identity theft. Remediation investments are a function of the desired Online Brand Rating, historical investments to safeguard IP, deferred maintenance on IP infringements plus historical marketing budgets that attract consumers and cyber criminals. We use the term investments as funds are applied in remediation to obtain ownership of IP infringements through arbitration. The underlying objective of remediation is to enhance IP values and minimize exposure to corporate identity theft per current and proposed regulations.
6d5: Specialized Trademark Services	Additional trademark services range from establishing new, strong brands for the internet to litigation for damages under the Anticybersquatting Consumer Protection Act as

	well as under the Tennessee Anti-Phishing Act of 2006. Microsoft's recent litigation demonstrates how a proactive litigation stance may serve as a deterrent and earn damages for shareholders.
6d6: IP Governance Risks	IP Governance Audit report addresses, for the benefit of the Board of Directors and for CEO's and CFO's, potential disclosure issues under Sarbanes-Oxley 409 and operational risk assessments. These include IP impairment valuations and related remediation investments, lack of adequate internal controls to detect and prevent fraud per federal standards and regulations, lack of disclosure of suspicious activity events with law enforcement, legal counsel and Boards of Directors, exposure to litigation, lack of insurance and a failure to fulfill the duty of care and fiduciary responsibilities in safeguarding intellectual property.
6d7: Disclosure Risks	An independent review addresses the quality of risk disclosures relating to regulatory compliance issues within Audit or Risk Committee Charters, Privacy and Security Statements per GLBA 504, debt agreements and SEC disclosures.
6d8: Operational Risk Quantification System	One of the issues noted by a June 2006 study on Basel II from the Federal Reserve Bank of Boston is that "the measurement of operational risk faces the challenge of limited data availability."[163] Just the opposite is the case with infringing domain names and related operational risks as open source tools enable the detection of brands, trademarks and infringing domain names. Such tools are used by the cyber criminals to identify confusingly similar domain names available for registration. As noted above, the IP Governance model identifies and measures a range of potential damages, remediation budgets and degrees of exposure (Online Brand Rating) to infringing domain names by financial institution as an operational risk quantification system.
6d9: Operational Losses (Attorney-client privilege).	Identifying under attorney-client privileges legal settlements and/or restitution payments for identity theft (absorbing losses to customers who are the victims of identity theft - 40790) is part of defining operational losses in the development and monitoring of an effective Identity Theft and Information Security Program. Operational losses are a central part of Basel II.
6d10: Metrics and Ratings	The Basel II NPR is "proposing a new risk-based capital adequacy framework that would require some and permit other qualifying banks to use an internal ratings-based

	approach to calculate regulatory credit risk capital requirements and advanced measurement approaches to calculate regulatory operational risk capital requirements."[164] As noted above, the Online Brand Rating model measures operational risk exposure to infringing domain names. The Online Brand Rating for a firm is a function of the (a) sum of positive points allocated for trademarks and domain names owned by an IP Owner plus (b) negative points allocated for available, matching domain names plus infringing domain names divided by (c) the number of unique brands. "F" Ratings indicate significant exposure to corporate identity theft. "A" Ratings indicate minimal exposure to corporate identity theft. One of the primary reasons driving the growth of corporate identity theft is that financial firms have not enacted the regulatory standards and related supervisory guidances for safeguarding their brands and domain names and this is confirmed by the consistent "F" ratings earned by large and small financial firms.
6d12: Transparency of Metrics and Ratings	Stakeholders seeking public information on global phishing trends, the top 10 phishing brands, and an Online Brand Rating for a financial firm may find this information online at: • Antiphishing.org - APWG • McAfee's Top 10 Phishing Brands[165] • OnlineBrandRating.com by IP Governance Task Force.
6d13: Synchronization with Internal Controls and Sarbanes-Oxley 404	Synchronizing the Identity Theft and Information Security Programs with Sarbanes-Oxley 404 is part of the private sector model that should be addressed by external auditors.
6d14: Timing Differences & Competitive Advantages	Proactive banks that minimize their operational risks and losses arising from corporate identity theft and Red Flag Risks, per Recommendations 2 and 3, ahead of current Basel II implementation schedules, i.e., FYE 2007 for international banks and 2009 for US banks, will benefit with stronger brands and fewer risks for their customers, reputation and capital.

Recommendation 6e – Role of Board – Setting the Tone at the Top – 3 Strategic Decisions: Corporate identity theft is fueling the growth of 45% of the phishing cases as shown by the metrics from the APWG. This is occurring despite all of the foregoing supervisory guidances addressing internal controls to detect, prevent, report and correct fraudulent uses of bank brands. Finding a balanced, transparent solution from the private sector based on current

regulations and guidances requires active leadership from Boards of Directors in setting the tone at the top for safeguarding their brands, customers and reputations. To facilitate this, each Board of Director is tasked with making three strategic decisions in the implementation and management of an effective corporate identity theft program, i.e., selecting (A) independent IP counsel aided by IP forensic auditors to develop adequate internal controls to safeguard core intellectual property and minimize operational risks, (B) their desired level of exposure to corporate identity theft on a scale of "F" to "A" and (C) the Privacy and Security statement that accurately describes their compliance with federal standards for safeguarding identifying information of their customers.

On May 8, 2006, the Wall Street Journal included this article, "Checks on Internal Controls Pay Off; Study Shows Share Prices Can Climb if a Company Uncovers, Fixes Problems". The article states, "Critics of a law that requires public companies to prove they have adequate systems in place to prevent accounting mistakes and fraud argue that the cost of complying with the rule is too onerous. But a study to be released this week suggests that shareholders benefit when companies perform checks on their internal controls: These companies whose houses are in order enjoy market-beating gains in their share price. Conversely, the stocks of companies with weak internal controls underperform the market. Further, the process of checking on internal controls - even if the checks turn up problems – can lead companies' shares to outperform if the companies act on the problems, according to the study by research firm Lord & Benoit LLC"[166].

Issue 7 40808	H. Community Bank Comment Request: "The Agencies invite your comments on the impact of this proposal on community banks. The Agencies recognize that community banks operate with more limited resources than larger institutions and may present a different risk profile. Thus, the Agencies specifically request comment on the impact of the proposal on community banks' current resources and available personnel with the requisite expertise, and whether the goals of the proposal could be achieved, for community banks, through an alternative approach."

Recommendation 7 – Remediation Investments: Remediation investments are a function of the desired Online Brand Rating, i.e., "F" to "A", historical investments to safeguard IP, deferred maintenance on IP infringements plus historical marketing budgets that attract consumers and cyber criminals. We use the term investments as funds are applied in remediation to obtain ownership of IP infringements through arbitration. The underlying objective of remediation is to enhance IP values and minimize exposure to corporate identity theft per current and proposed regulations.

Issue 8	FTC: Projected Reporting, Record keeping and Other Compliance Requirements. The Commission does not expect that there will be any

40806-40807	significant legal, professional, or training costs to comply with the Rule. Although it is not possible to estimate small businesses' compliance costs precisely, such costs are likely to be quite modest for most small entities. Nonetheless, because the Commission is concerned about the potential impact of the proposed Rule on small entities, it specifically invites comment on the costs of compliance for such parties. In particular, although the Commission does not expect that small entities will require legal assistance to meet the proposed Rule's requirements, the Commission requests comment on whether small entities believe that they will incur such costs and, if so, what they will be.

Recommendation 8 – Projected Reporting, Record keeping and Other Compliance Requirements: As currently drafted, with the omission of the aforementioned regulations and supervisory guidances on corporate identity theft, the NPR assumptions within Issue 8 are probably fair and accurate. Ultimately, it all depends on the final NPR rules and how the Agencies decide to define identity theft risks and the related Red Flags. Should the Agencies adopt the foregoing recommendations, we then refer to Recommendation 7 for a review of potential remediation investments.

We also offer below the perspective from a CEO of a credit union with 14,423 members and $128,222,919 in assets who has adopted all of the foregoing recommendations:

"As President and CEO with fiduciary responsibilities to safeguard River Valley Credit Union's brands and consumers from identity theft attacks, we are setting the tone at the top by recalibrating our priorities to prevent, detect and correct infringing uses of our brands. Recent remediation efforts have improved our Online Brand Rating from "F" to "B" to "A". Protecting consumers online is part of our mission to earn their trust and online business." John E. Bowen, President and CEO, River Valley Credit Union, Miamisburg, Ohio. September 18, 2006.

Issue 9 40807	FTC: Projected Reporting, Record keeping and Other Compliance Requirements. The Commission requests comment on the costs, if any, of training relevant employees regarding the proposed requirements.

Recommendation 9 – Training Costs – Depends on Final Rules: As currently drafted, with the omission of the aforementioned regulations and supervisory guidances on corporate identity theft, training is probably not a significant issue for any of the Agencies. Ultimately, it all depends on the final rules and how the Agencies decide to define identity theft risks and the related Red Flags. Should the Agencies adopt the foregoing recommendations, then training will be a significant issue for Boards of Directors, C-Level executives, compliance officers, counsel, privacy officers, marketing officers, regulators, and banking associations

as it relates to safeguarding intellectual property within Information Security and Identity Theft Programs.

Setting the Tone at the Top: Ultimately, it is the responsibility of "the Board of Directors and or an appropriate committee of the board to approve the Program. In addition, the board, an appropriate committee of the board, or senior management must exercise oversight over the Program's implementation. Staff implementing the Program must report to its board, an appropriate committee or senior management, at least annually, on compliance by the financial institution or creditor with the Red Flag Regulations." (40789)

Map – Board of Directors: A map of key issues for a Board of Directors in developing and managing an effective Identity Theft and Information Security Program for corporate identity theft risks, with a view towards Basel II, is provided in Appendix C.

In conclusion, we appreciate the opportunity to provide comments on the proposed final rules and we thank the agencies for their efforts to improve the industry standards for safeguarding sensitive customer information due to internet risks.

Respectfully submitted,

Nathan Z. Johns, CISA
Risk & Performance Services
Crowe Chizek and Company, LLC
354 Eisenhower Parkway, Plaza 1
Livingston, New Jersey 07039
973-422-4533

Tom Kellermann
Cyber Security Analyst
4977 Battery Lane
Bethesda MD, 20814
202-415-3955

Paul W. Kruse, Esq.
Bone McAllester Norton PLLC
511 Union Street - Suite 1600
Nashville, Tennessee 37219
615-238-6300

Beckwith B. Miller
TrademarkBots.com, Inc.
5100 Tamiami Trail North, Suite 105
Naples, Florida 34103
239-777-4638

Patrick J. Whalen, Esq.
Spencer Fane Britt & Browne, LLP
1000 Walnut Street, Suite 1400
Kansas City, MO 64106-2140
816-474-8100

Members of the IP Governance Task Force
www.ipgovernance.com

Appendix A: Directory of Issues and Recommendations

Appendix B - Map of Corporate Identity Theft Risks:

This shows the full spectrum of intellectual property risks that contribute to corporate identity theft. It also facilitates a side-by-side comparison between the regulations and standards cited in the NPR for safeguarding brands from each of the two complementary programs, i.e., the Identity Theft Program and the Information Security Program, and those that are omitted but should be included for an effective program.

Note: The five digit numbers beginning with “40” refer to pages in the NPR.

Board of Directors Must Approve each Program

The Agencies ***request comment*** regarding the frequency with which reports should be prepared for the board, a board committee, or senior management. (40793)

The Agencies also ***request comment*** on whether this paragraph properly allocates the responsibility for oversight and implementation of the Program between the board and senior management. (40793)

Information Security Program (GLBA)			Identity Theft Prevention Program
40780	40789	40804	The program must address financial, operational, compliance, reputation, and litigation risks. (40790)

40788	Combine Information Security and Identity Theft Programs	40804
40780	Scope of Organizations Covered by the NPR	40790

(IP) Intellectual Property Governance	IT Governance
External, Beyond IT Perimeter Risks	Internal System Risks
Metrics on IP Governance	Metrics from APWG

Brands	TM's/®	Domain Names	Fraudulent Web Sites (App. J: 24,25)	Phishing Sites	Pharming Attacks	Spyware, Trojans

IP Owned By Firm

Layered Information Security Solution: FDIC FIL-103-2005

Red Flag Risks: Fraudulent Access to Customer Information

Bank Secrecy Act / Anti-Money Laundering Examination Manual (8/06)

"Terrorists generally finance their activities through both unlawful and legitimate sources"…that include "identity theft"… (12 of 367)

Defining Red Flag Precursors

The Agencies *request comment* on the scope of the definition of ''Red Flags'' and, specifically, whether the definition of Red Flags should include precursors to identity theft. (40790)

Prevent, Detect, Mitigate

Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft. The Agencies *request comment* on whether the enumerated sources of Red Flags are appropriate. (40791)

Corporate Identity Theft

Phishing Risks

40790	40799

Ref: Footnote 40 (40799)

OCC. Bulletin. "Risk Mitigation and Response Guidance for Web Site Spoofing Incidents". Bulletin 2005-24. 1 July 2005.[28]

OTS. Letter. "Phishing and E-mail Scams" CEO Letter #193. 3 March 2004.[33]

FFIEC's Information Security Handbook

Omitted Supervisory Guidances

IT Solutions

(7-18-06) Multi-Factor Authentication (MFA)

Agencies 40799	OCC 40802	OTS 40805
	OCC 40802	OTS 40805

National banks and savings associations complying with the ''Interagency Guidelines Establishing Information Security Standards''56 and guidance recently issued by the FFIEC titled ''Authentication in an Internet Banking Environment'' 57 already will have policies and procedures in place to detect attempted and actual intrusions into customer information systems.

(8-15-06) FFIEC FAQ's on Multifactor Authentication

Identification of Duplicative, Overlapping, or Conflicting Federal Rules

40804	40807

The Board *seeks comment* regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred.

Omitted Regulations

(FFIEC "Privacy of Consumer Financial Information")	"We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information."
Sarbanes-Oxley	Internal controls to detect fraud.
Trademark Law	Rights and obligations for brands.
Trade Secret Law	Rights and obligations for business secrets.
SEC Disclosures	Representations for Investors.

Appendix C - Map – Board of Directors:

A map of key issues for a Board of Directors in developing and managing an effective Identity Theft and Information Security Program for corporate identity theft risks, with a view towards Basel II, is provided below.

Board of Directors	
Setting the Tone at the Top	Duty of Care & Fiduciary Responsibilities

Internal Controls & Measuring Effectiveness

IP Governance - Due Diligence Matrix		
Information Security Program (GLBA)	Identity Theft Program (Red Flag)	Advanced Management (Basel II)

Operational Losses (Annex 9: BIS)		
Level 1	Level 2	Level 3
External Fraud	Systems, Security	Theft of information (Monetary Loss); Hacking Damage
Clients, Products & Business Practices	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations; Suitability / disclosure issues (KYC, etc.); Retail customer disclosure violations; Breach of privacy;
Execution, Delivery, Process Management	Monitoring & Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)

Operational Risks			
Operational Risks:	**Brands, Trademarks, Domain Names**	**Disclosures**	**Litigation Risks**
Metrics:	**Enables 45% of Phishing Risks, (Federal Crimes)**	**Accuracy**	**Sarbanes-Oxley 409** (Remediation Budget)
Metrics:	**Online Brand Rating**	**Privacy Security Rating**	**Consumer Confidence**
Options:	**"A" to "F"**	**"1" to "5"**	**Internal Controls & Materiality**

Privacy Security Rating (GLBA 504)		
#1	Very Strong	Our physical, electronic, and procedural safeguards meet or exceed federal standards regarding the protection of customer information.
#2	Strong	We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your personal information.
#3	Mild	We maintain physical, electronic and procedural safeguards to guard information.
#4	Weak	Although our bank has taken reasonable precautions to assure account security, we reserve the right to disclaim responsibility/liability for a breach of security that occurs for reasons outside our control.
#5	Very Weak	SampleBank is also not liable to you or any third party for any occurrences or damages directly or indirectly related to any phishing, pharming or other attacks or fraud committed against SampleBank.

Appendix D - Definitions:

APWG: Anti-Phishing Working Group.

COSO: The Committee of Sponsoring Organizations of the Treadway Commission.

Domain Name: "A combination of letters and numbers that identifies a specific computer or website on the Internet. A domain name usually consists of three parts: a generic "top-level" domain such as ".com" or ".gov" that identifies the type of organization; a second level domain such as nolo or yahoo, which identifies the organization, site or individual; and a third level domain such as "www," [@], [FTP] which is used to identify a particular host server [and/or internet function]. Domain names have various functions. They can serve as an address (whitehouse.com), as a trademark (amazon.com) or as an expression of free speech (presidentbushsucks.com). A domain name owner can stop another business from using the same name for its business or product only if the domain name is being used as a trademark. In other words, if you use your domain name in connection with the sale of goods or services and consumers associate the domain name with your business, you can stop another business from using it. On the flip side, trademark owners can stop others from using a domain name if it conflicts with their existing trademark."[167]

Domain Name System: "A worldwide distributed database that is used to translate worldwide unique domain names such as www.isoc.org to other identifiers"[168] such as Internet Protocol Addresses. A detailed analysis of the Domain Name System [DNS] is available from "Culturally-appropriate Local Environments and a Global Internet Supplemental Information and Readings"[169]

FACT Act: Fair Credit Reporting Act.

FDIC: Federal Deposit Insurance Corporation.

FFIEC: Federal Financial Institutions Examination Council. The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

FASB: Financial Accounting Standards Board.

FINCEN: Financial Crimes Enforcement Network.

GLBA: Gramm-Leach-Bliley Act.

ICANN: Internet Corporation for Assigned Names and Numbers. ICANN is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function.

IP: Intellectual Property.

IP Governance Task Force: www.IPGovernance.com.

NCUA: National Credit Union Administration.

OCC: Office of the Comptroller of the Currency.

Pharming: "The redirection of an individual to an illegitimate Web site through technical means [involving the DNS system]. For example, an Internet banking customer, who routinely logs in to his online banking Web site, may be redirected to an illegitimate Web instead of accessing his or her bank's Web site.[170]

Phishing: Phishing – as in fishing for confidential information – is a scam that encompasses fraudulently obtaining and using an individual's personal or financial information. In a typical case, the consumer receives an e-mail appearing to originate from a financial institution, government agency or other entity that requests personal or financial information. The e-mail often indicates that the consumer should provide immediate attention to the situation described by clicking on a link. The provided link appears to be the Web site of the financial institution, government agency or other entity. However, in "phishing" scams, the link is not to an official Web site, but rather to a phony Web site. Once inside that Web site, the consumer may be asked to provide a Social Security number, account numbers, passwords or other information used to identify the consumer, such as the maiden name of the consumer's mother or the consumer's place of birth. When the consumer provides the information, those perpetrating the fraud can begin to access consumer accounts or assume the person's identity.[170]

UDRP: Uniform Domain Name Dispute Resolution Policy. Defined and explained in the following chapter: "5.6 RESOLUTION OF CONFLICTS OVER DOMAIN NAMES", Signposts in Cyberspace: The Domain Name System and Internet Navigation (2005), The National Academies Press.[171]

URL: Uniform Resource Locators or domain name.

Footnotes:

[1.] Federal Register. “Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy”. Date 18 July 2006. Accessed 3 August 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-6187.pdf

[2.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 23 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[3.] Financial Services Authority. “Banks encouraged to engage consumers in tackling online fraud”. Date 23 January 2006. Accessed 8 August 2006. Available http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/005.shtml

[4.] FFEIC. “Federal Financial Regulators Release Updated Information Security Booklet.” Date 27 July 2006. Accessed 3 September 2006. Available http://www.ffiec.gov/press/pr072706.htm

[5.] FFIEC. “Bank Secrecy Act/Anti-Money Laundering Examination Manual”. Date 28 July 2006. Accessed 3 August 2006. Available: http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf

[6.] FFIEC. “FFIEC Guidance on Authentication in an Internet Banking Environment”. Date 15 August 2006. Accessed 3 September 2006. Available: http://www.fdic.gov/news/news/financial/2006/authentication_faq.pdf

[7.] FFIEC. “Bank Secrecy Act/Anti-Money Laundering Examination Manual”. Date 28 July 2006. 12 of 367. Accessed 3 August 2006. Available: http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf

[8.] FFIEC. “FFIEC Guidance on Authentication in an Internet Banking Environment”. Date 15 August 2006. 2 of 7. Accessed 3 September 2006. Available: http://www.fdic.gov/news/news/financial/2006/authentication_faq.pdf

[9.] FDIC. Financial Institution Letter (FIL-103-2005). “FFIEC Guidance Authentication in an Internet Banking Environment.” 12 October 2005. Accessed 3 September 2006 Available http://www.fdic.gov/news/news/financial/2005/fil10305.html

[10.] Computerweekly.com. “Growth of cybercrime is among top global threats to security, says FBI” Date 11 July 2006. Accessed 13 September 2006. Available:http://www.computerweekly.com/Articles/Article.aspx?liArticleID=216802&PrinterFriendly=true

[11.] British Computer Society (BCS). “The Cybermen fight back” Date 11 July 2006. Accessed: 14 September 2006. Available:http://www.bcs.org/server.php?show=ConWebDoc.5959

[12.] Serious Organized Crime Agency. “SOCA’s Aims”. Accessed 14 September 2006. Available: http://www.soca.gov.uk/aboutUs/aims.html

[13.] Serious Organized Crime Agency. “Organized Crime: Individual & Private Sector”. Accessed 14 September 2006. Available: http://www.soca.gov.uk/orgCrime/sectorFraud.html

[14.] Bank for International Settlements. Basel Committee on Banking Supervisions. Fact Sheet. Accessed 14 September 2006. Available: http://www.bis.org/about/factbcbs.htm

[15.] Bank for International Settlements. “Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version” Date: June 2006. Accessed: 14 September 2006 Available: http://www.bis.org/publ/bcbs128.pdf

[16.] Bank for International Settlements. “Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version” 158 of 347. Date: June 2006. Accessed: 14 September 2006 Available: http://www.bis.org/publ/bcbs128.pdf

[17.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 83 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[18.] Bank for International Settlements. “Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version” 319 of 347. Date: June 2006. Accessed: 14 September 2006 Available: http://www.bis.org/publ/bcbs128.pdf

[19.] Federal Reserve Board. Governor Susan Schmidt Bies. “A supervisor’s perspective on enterprise risk management”. Date 12 June 2006. Accessed 3 September 2006. Available http://www.federalreserve.gov/boardDocs/speeches/2006/200606122/default.htm

[20.] Federal Reserve Board. Governor Susan Schmidt Bies. “A supervisor’s perspective on enterprise risk management”. Date 12 June 2006. Accessed 3 September 2006. Available http://www.federalreserve.gov/boardDocs/speeches/2006/200606122/default.htm

[21.] The White House. “Executive Order: Strengthening Federal Efforts to Protect Against Identity Theft”. Date 10 May 2006. Accessed 3 September 2006. Available http://www.whitehouse.gov/news/releases/2006/05/20060510-3.htm

[22.] Federal Register. “Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy”. Date 18 July 2006. Accessed 3 August 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-6187.pdf

[23.] Federal Register. “Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy”. Date 18 July 2006. 4 of 42. Accessed 3 August 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov

[24.] Anti-Phishing Working Group. “APWG Whitepapers and Reports”. Accessed 8 August 2006. Available http://www.antiphishing.org/resources.html#consumer

[25.] Anti-Phishing Working Group. “APWG Whitepapers and Reports”. Accessed 8 August 2006. Available http://www.antiphishing.org/resources.html#consumer

[26.] The Heritage Foundation. Property Ratings. Accessed 3 September 2006. Available http://www.heritage.org/research/features/index/scores.cfm

[27.] The Heritage Foundation. Property Ratings. Accessed 3 September 2006. Available http://www.heritage.org/research/features/index/scores.cfm

[28.] The Heritage Foundation. Property Ratings. Accessed 3 September 2006. Available http://www.heritage.org/research/features/index/scores.cfm

[29.] Detroit Free Press. “Foreign Spammers Thwart the FTC”. Date 27 August 2006. Accessed 3 September 2006. Available: http://www.freep.com/apps/pbcs.dll/article?AID=/20060827/NEWS07/608270645/1009

[30.] Financial Services Authority. “Banks encouraged to engage consumers in tackling online fraud”. Date 23 January 2006. Accessed 8 August 2006. Available http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/005.shtml

[31.] Gartner. “Gartner Study Finds Consumer Confidence in Online Commerce Waning” Date June 2005. Accessed 3 September 2006. Available http://www.cheaphostingdirectory.com/news-study-finds-consumer-confidence-in-online-commerce-waning-1171.html

[32.] BITS. Financial Services Roundtable. “BITS Consumer Confidence Toolkit: Data Security and Financial Services -“Potential Crisis in Consumer Confidence.” Date September 2005. Accessed 3 September 2006. Available http://www.bitsinfo.org/downloads/Publications Page/bitscons2005.pdf

[33.] Deloitte. “Financial Services industry fears risk to Reputation in battle against ID theft” Date 24 April 2006. Accessed 3 September 2006. Available http://www.deloitte.com/dtt/press_release/0,1014,sid%253D2834%2526cid%253D116358,00.html

[34.] Federal Register. “Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy”. Date 18 July 2006. Page 6 of 42 or 40790 Accessed 3 August 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-6187.pdf

[35.] FFIEC. Information Security Booklet. Appendix C. Date 27 July 2006. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm

[36.] OCC. Bulletin. “Risk Mitigation and Response Guidance for Web Site Spoofing Incidents”. Bulletin 2005-24. Date 1 July 2005. Accessed 8 August 2006. Available http://www.occ.treas.gov/ftp/bulletin/2005-24.doc

[37.] OTS. Letter. “Phishing and E-mail Scams” CEO Letter #193. Date 3 March 2004. Accessed 8 August 2006. Available http://www.ots.treas.gov/docs/2/25193.pdf

[38.] FDIC. Bank Technology Bulletin. “Protecting Internet Domains”. FIL-77-2000. Date 8 November 2000. Accessed 8 August 2006. Available http://www.fdic.gov/news/news/financial/2000/fil0077a.html

[39.] FDIC. Financial Institution Letter. “Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes”. FIL-27-2004. Date 12 March 2004. Accessed 8 August 2006. Available http://www.fdic.gov/news/news/financial/2004/fil2704.html

[40.] FDIC. Financial Institution Letter. Identity Theft Study on “Account Hijacking” Identity Theft and Suggestions for Reducing Online Fraud”. FIL 132-2004. Date 14 December 2004. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/fdi-fil-103-2005.pdf

[41.] FDIC. Financial Institution Letter. “Pharming Guidance on How Financial Institutions Can Protect Against Pharming Attacks”. FIL-64-2005. Date 18 July 2005. Accessed 8 August 2006. Available http://www.fdic.gov/news/news/financial/2005/fil6405.html

[42.] FDIC. Financial Institution Letter. “FFIEC Guidance Authentication in an Internet Banking Environment” FIL-103-2005. Date 10 October 2005. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/fdi-fil-103-2005.pdf

[43.] OCC. Alert. “Protecting Internet Addresses of National Banks”. Alert 2000-9. Date 19 July 2000. Accessed 8 August 2006. Available http://www.occ.treas.gov/ftp/alert/2000-9.txt

[44.] OCC. Alert. “Customer Identity Theft: E-Mail-Related Fraud Threats”. Alert 2003-11. Date 9 September 2003. Accessed 8 August 2006. Available http://www.occ.treas.gov/ftp/alert/2003-11.doc

[45.] NCUA. Letter. “Protection of Credit Union Internet Addresses” Letter 02-CU-16. Date December 2002. Accessed 8 August 2006. Available http://www.ncua.gov/letters/2002/02-CU-16.pdf

[46.] NCUA. Letter. “Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Union” Letter 03-CU-12. Date August 2003. Accessed 8 August 2006. Available http://www.ncua.gov/letters/2003/03-CU-12.pdf

[47.] NCUA. Letter. “E-Mail and Internet Related Fraudulent Schemes Guidance” Letter 04-CU-06. Date April 2004. Accessed 8 August 2006. Available http://www.ncua.gov/letters/2004/04-CU-06.doc

[48.] NCUA. Letter. “Phishing Guidance for Credit Unions And Their Members” Letter 05-CU-20. Date December 2005. Accessed 8 August 2006. Available http://www.ncua.gov/letters/2005/CU/05-CU-20.doc

[49.] FFIEC. “E-Banking Booklet. E-Banking Request Letter.” Date 2003. Accessed 3 August 4 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_03c_exam_letter.html

[50.] Federal Reserve Board. Joint Notice of Proposed Rulemaking. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework.” Date 5 September 2006. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[51.] Federal Reserve Board. Joint Notice of Proposed Rulemaking. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework.” 344 of 501. Date 5 September 2006. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[52.] FFIEC. “E-Banking Booklet. E-Banking Request Letter.” Date 2003. Accessed 3 August 4 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_03c_exam_letter.html

[53.] Federal Reserve Board. Joint Notice of Proposed Rulemaking. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework.” 370 of 501. Date 5 September 2006. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[54.] Federal Reserve Board. Joint Notice of Proposed Rulemaking. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework.” 464 of 501. Date 5 September 2006. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[55.] Jonathan J. Rusch, Esq. “Phishing and Federal Law Enforcement” Date 6 August 2004. Accessed 14 September 2006. Available: http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt

[56.] Tennessee State Legislature. “Anti-Phishing Act of 2006” Date 1 July 2006. Accessed 14 September 2006. Available: http://www.legislature.state.tn.us/bills/currentga/Chapter/PC0566.pdf

[57.] FINCEN. “Suspicious Activity Report”. Date July 2003. Accessed 8 August 2006. Available http://www.fincen.gov/forms/f9022-47_sar-di.pdf

[58.] FDIC. “Risk Management Manual of Examination Policies”. Accessed 3 August 2006. Available http://www.fdic.gov/regulations/safety/manual/section10-1.html#part2

[59.] FDIC. “FDIC Law, Regulations, Related Acts; Suspicious Activity Reports” Accessed 3 August 2006. Available http://www.fdic.gov/regulations/laws/rules/2000-7500.html

[60.] Interagency Advisory. “Federal Court Reaffirms Protections for Financial Institutions Filing Suspicious Activity Reports”. Date 24 May 2004. Accessed 3 August 2006. Available http://www.federalreserve.gov/boarddocs/srletters/2004/SR0408a1.pdf

[61.] E. and J. Gallo Winery v. Spider Webs Ltd., et al.. Date 2001 Accessed 3 September 2006. Available http://www.phillipsnizer.com/library/cases/lib_case5.cfm

[62.] Pinehurst v. Wick. Date 2002. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=290&type=trademark

[63.] Graduate Mgmt. Admission Council v. Raju. Date 2003. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=331&type=trademark

[64.] Elecs. Boutique Holdings Corp. v. Zuccarini. Date 2000. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=79&type=trademark

[65.] Louis Vuitton Malletier v. Veit.Date 2002. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=310&type=trademark

[66.] Entrepreneur Media, Inc. v. Smith. Date 2002. Accessed 3 September 2006. Availablehttp://www.finnegan.com/publications/news-popup.cfm?id=81&type=trademark

[67.] Petmed Express, Inc. v. Medpets.com, Inc. Date 2004. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=386&type=trademark

[68.] Rolex Watch U.S.A., Inc. v. Jone. Date 2000. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=192&type=trademark

[69.] Australian Gold, Inc. v. Hatfield. Date 2006. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=423&type=trademark

[70.] Philip Morris USA, Inc. v. Otamedia Ltd. , Date 2005. Accessed 3 September 2006. Available http://www.finnegan.com/publications/news-popup.cfm?id=378&type=trademark

[71.] FINCEN. “SAR Review Issue #9. Date October 2005. Accessed 3 August 2006. Available: http://www.fincen.gov/sarreviewissue9.pdf

[72.] FINCEN. “SAR Review Issue #9. Date October 2005. 23 of 67. Accessed 3 August 2006. Available: http://www.fincen.gov/sarreviewissue9.pdf

[73.] FINCEN. “SAR Review Issue #9. Date October 2005. 24 of 67. Accessed 3 August 2006. Available: http://www.fincen.gov/sarreviewissue9.pdf

[74.] FINCEN. “SAR Review Issue #9. Date October 2005. 25 of 67. Accessed 3 August 2006. Available: http://www.fincen.gov/sarreviewissue9.pdf

[75.] Serious Organized Crime Agency. “SOCA’s Aims”. Accessed 14 September 2006. Available: http://www.soca.gov.uk/financialIntel/disclosure.html

[76.] FDIC. “Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies”. Date 20 January 2006. Accessed 3 August 2006. Available http://www.fdic.gov/news/news/financial/2006/fil06005.html

[77.] FINCEN. Regulatory/Enforcement Actions. Accessed 3 August 2006. Available http://www.fincen.gov/reg_enforcement.html

[78.] FINCEN. “Assessment of Civil Money Penalty: Liberty Bank of New York”. Date 18 May 2006. Accessed 8 August 2006. Available http://fincen.gov/liberty_assessment.pdf

[79.] FINCEN. “Assessment of Civil Money Penalty: SampleBank”. Date 26 April 2006. Accessed 8 August 2006. Available http://fincen.gov/SampleBank_assessment.pdf

[80.] FINCEN. “Assessment of Civil Money Penalty: Metrobank”. Date 18 April 2006. Accessed 8 August 2006. Available http://fincen.gov/metro_assessment.pdf

[81.] FINCEN. “Assessment of Civil Money Penalty: ABN AMRO”. Date 19 December 2005. Accessed 8 August 2006. Available http://fincen.gov/abn_assessment.pdf

[82.] FINCEN. “Assessment of Civil Money Penalty: Amsouth”. Date 12 October 2004. Accessed 8 August 2006. Available http://fincen.gov/amsouthassessmentcivilmoney.pdf

[83.] FINCEN. “Assessment of Civil Money Penalty: Riggs”. Date 13 May 2004. Accessed 8 August 2006. Available http://fincen.gov/amsouthassessmentcivilmoney.pdf

[84.] FINCEN. “Assessment of Civil Money Penalty: Banco de Chile”. Date 12 October 2005. Accessed 3 September 2006. Available http://www.fincen.gov/bancodechile.pdf

[85.] FINCEN. “Assessment of Civil Money Penalty: Korea Exchange Bank. Date 24 June 2003. Accessed 3 September 2006. Available http://www.fincen.gov/koreaexchangeassessment.pdf

[86.] FINCEN. “Fine NY State Department of Banking. Western Union. Date 3 June 2003. Accessed 3 September 2006. Available http://www.fincen.gov/western_union_assessment.pdf

[87.] FTC. “Gramm-Leach-Bliley Act, 15 USC 6801”. Accessed 6 August 2006. Available http://www.ftc.gov/privacy/glbact/glbsub2.htm

[88.] FTC. “FTC v. C.J., Civ. No. 03-5275”[61]. Date 21 July 2003. Accessed 8 August 2006. Available http://www.ftc.gov/opa/2003/07/phishing.htm

[89.] FTC. “FTC v. Zachary Keith Hill, Civ. Action No. H 03-5537”. Date 22 March 2004. Accessed 8 August 2006.
Available http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm

[90.] FFIEC. “Gramm-Leach-Bliley Act, 15 USC 6801”. Accessed 6 August 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/elect_bank/con-15usc_6801_6805-gramm_leach_bliley_act.pdf

[91.] FTC. “Gramm-Leach-Bliley Act, 15 USC 6801”. Accessed 6 August 2006. Available http://www.ftc.gov/privacy/glbact/glbsub2.htm

[92.] Serious Organized Crime Agency. “SOCA’s Aims”. Accessed 14 September 2006. Available: http://www.soca.gov.uk/aboutUs/aims.html

[93.] Federal Reserve Board. Joint Notice of Proposed Rulemaking. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework.” 344 of 501. Date 5 September 2006. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[94.] Federal Reserve Bank of New York “Industry Sound Practices for Financial and Accounting Controls at Financial Institutions”
http://www.ny.frb.org/banking/soundpracticepaper.pdf

[95.] FDIC. Financial Institution Letter. CORPORATE GOVERNANCE, AUDITS, AND REPORTING REQUIREMENTS; Effect of the Sarbanes-Oxley Act of 2002 on Insured Depository Institutions. FIL-17-03. March 5, 2003
http://www.fdic.gov/news/news/financial/2003/fil0317.html

[96.] FRB, OCC, OTS. Statement on Application of Recent Corporate Governance Initiatives to Non-Public Banking Organizations. SR 03-8. May 5, 2003.[122]
http://www.occ.treas.gov/efiles/disk2/resources/audit/frb-srl_03_8-stat_corp_gov_initiat_nonpub_bank_org.pdf#search=%22fdic%20FIL-17-2003%22

[97.] Ernst & Young. “The Impact of SOX on Intellectual Property Management”. Date 15 February 2006. Accessed 5 September 2006. Available
http://www.les-svc.org/Docs/Events2006/The%20Impact%20of%20SOX%20on%20IP%20management.pdf

[98.] “Sarbanes-Oxley and Trademark Portfolio Management: Establishing Internal Controls for Compliance & Preventing Infringement”, by Paul W. Kruse, Esq.
http://www.aspatore.com/store/details.asp?id=50

[99.] "Trade Secret Asset Management; An Executive's Guide to Information Asset Management, Including Sarbaes-Oxley Accounting Requirements for Trade Secrets" , by R. Mark Halligan and Richard F. Weyand.
http://www.aspatore.com/store/details.asp?id=340

[100.] "Trade Secret Asset Management; An Executive's Guide to Information Asset Management, Including Sarbaes-Oxley Accounting Requirements for Trade Secrets" , by R. Mark Halligan and Richard F. Weyand. 240 of 246
http://www.aspatore.com/store/details.asp?id=340

[101.] Federal Reserve Board. Governor Susan Schmidt Bies. "A supervisor's perspective on enterprise risk management". Date 12 June 2006. Accessed 3 September 2006. Available
http://www.federalreserve.gov/boardDocs/speeches/2006/200606122/default.htm

[102.] Federal Reserve Bank of New York "Industry Sound Practices for Financial and Accounting Controls at Financial Institutions"
http://www.ny.frb.org/banking/soundpracticepaper.pdf

[103.] "Trade Secret Asset Management; An Executive's Guide to Information Asset Management, Including Sarbaes-Oxley Accounting Requirements for Trade Secrets" , by R. Mark Halligan and Richard F. Weyand. 140 of 246
http://www.aspatore.com/store/details.asp?id=340

[104.] Federal Reserve. SR 02-20 October 29, 2002 The Sarbanes-Oxley Act of 2002
http://www.federalreserve.gov/boarddocs/SRLETTERS/2002/sr0220.htm

[105.] SEC. "SEC Adopts Rules on Provisions of Sarbanes-Oxley Act" Date 15 January 2003. Accessed 3 August 2006. Available http://www.sec.gov/news/press/2003-6.htm

[106.] CSI/FBI Computer Crime and Security Survey. Date 2005. Accessed 3 August 2006. Available http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

[107.] CSI/FBI Computer Crime and Security Survey. Date 2006. Accessed 3 August 2006. Available http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

[108.] CSI/FBI Computer Crime and Security Survey. Date 2006. 3 of 29. Accessed 3 August 2006. Available http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

[109.] CSI/FBI Computer Crime and Security Survey. Date 2006. 21 of 29. Accessed 3 August 2006. Available http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

[110.] Nathan Drew Larsen. N O R T H W E S T E R N JOURNAL O F TECHNOLOGY A N D INTELLECTUAL PROP ERTY. Evaluating the Proposed Changes to Federal Rule of Civil Procedure 37. Date Spring 2006. 15 of 17. Available
http://www.law.northwestern.edu/journals/njtip/v4/n2/4/Larsen.pdf

[111.] Alan Charles Raul, Frank R. Volpe. BNA Electronic Commerce Law Report, Volume 6 Number 31, Wednesday, August 8, 2001, Page 849.
http://www.sidley.com/cyberlaw/features/liability.asp?print=yes

[112.] Thomas Franklin. Townsend and Townsend and Crew LLP. "Protection Of Intangibles Under Sarbanes-Oxley" Date 4 April 2006. Available http://www.townsend.com/files/SOX.pdf

[113.] "Trade Secret Asset Management; An Executive's Guide to Information Asset Management, Including Sarbaes-Oxley Accounting Requirements for Trade Secrets" [123], by R. Mark Halligan and Richard F. Weyand. 140 of 246 http://www.aspatore.com/store/details.asp?id=340

[114.] VISA. Payment Card Industry Data Security Standard, Version 1.0" Date 15 December 2004. Accessed 3 August 2006. Available http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf?it=il|/business/accepting_visa/ops_risk_management/cisp.html|PCI%20Data%20Security%20Standard

[115.] PCI Security Standards Council. PCI Data Security Standard Version 1.1. Date September 2006. Availablehttps://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

[116.] FDIC. "18 U.S.C. Section 709: False advertising or misuse of names to indicate Federal agency" Accessed 3 August 2006. Available: http://www.fdic.gov/regulations/laws/rules/8000-1200.html

[117.] GAO. "INFORMATION SECURITY Emerging Cybersecurity Issues Threaten Federal Information Systems." Date May 2005. 12 of 17. Accessed 8 August 2006. Available http://www.gao.gov/new.items/d05231.pdf

[118.] GAO. "INFORMATION SECURITY Emerging Cybersecurity Issues Threaten Federal Information Systems." Date May 2005. 13 of 17. Accessed 8 August 2006. Available http://www.gao.gov/new.items/d05231.pdf

[119.] WIPO. "Federal Reserve Banks v. Chris Hoffman" Date 18 January 2005. Accessed 14 September 2006. Available: http://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0918.html

[120.] National Arbitration Forum. "Federal National Mortgage Association d/b/a Fannie Mae v. Domain Stuff.com" Date 29 July 2002. Accessed 14 September 2006 Available http://domains.adrforum.com/domains/decisions/114620.htm

[121.] National Arbitration Forum. "Federal Home Loan Mortgage Corporation v. Muhammad Arshad a/k/a SRS" Date 19 September 2002. Accessed 14 September 2006 Available http://domains.adrforum.com/domains/decisions/116767.htm

[122.] National Arbitration Forum. "Federal Home Loan Mortgage Corporation v. Perfect Leads LLC" Date 23 December 2002. Accessed 14 September 2006 Available http://domains.adrforum.com/domains/decisions/128653.htm

[123.] National Arbitration Forum. "Federal Home Loan Mortgage Corporation v. Suren Deep" Date 12 May 2003. Accessed 14 September 2006 Available http://domains.adrforum.com/domains/decisions/154102.htm

[124.] National Arbitration Forum. “Federal Home Loan Mortgage Corporation v. Willie Stroud” Date 9 June 2003. Accessed 14 September 2006 Available http://domains.adrforum.com/domains/decisions/155173.htm

[125.] National Arbitration Forum. “Federal Home Loan Mortgage Corporation v. Karen Blodgett d/b/a KOG Enterprises, Inc.” Date 4 November 2005. Accessed 14 September 2006 Available http://domains.adrforum.com/domains/decisions/566605.htm

[126.] OCC. Privacy Regulations.12 CFR 40.3(i)(1). Date 1 January 2005. Accessed 3 September 2006. Available http://a257.g.akamaitech.net/7/257/2422/11feb20051500/edocket.access.gpo.gov/cfr_2005/janqtr/pdf/12cfr40.3.pdf#search=%2212%20CFR%2040.3(i)(1)%22

[127.] Federal Reserve Board. Privacy Regulations. 12 CFR 216.3(i)(1). Date 1 January 2002. Accessed 3 September 2006. Available http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/cfr_2002/janqtr/pdf/12cfr216.3.pdf

[128.] FDIC. Privacy Regulations. 12 CFR 332.3(i)(1) (FDIC). Date 1 Janaury 2001. Accessed 3 September 2006. Available http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/cfr_2001/janqtr/pdf/12cfr332.3.pdf#search=%2212%20CFR%20332.3(i)(1)%22

[129.] OTS. Privacy Regulations. 12 CFR 573.3(i)(1) Date 1 January 2006. Accessed 3 September 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061500/edocket.access.gpo.gov/cfr_2006/janqtr/pdf/12cfr573.3.pdf#search=%2212%20CFR%20573.3(i)(1)%20%22

[130.] NCUA. Privacy Regulations. 12 CFR 716.3(j). Date 1 January 2006. Accessed 3 September 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061500/edocket.access.gpo.gov/cfr_2006/janqtr/pdf/12cfr716.3.pdf#search=%2212%20CFR%20716.3(j)%22

[131.] FTC. Privacy Regulations. 16 CFR 313.3(i)(1). Date 23 May 2002. Accessed 3 September 2006. Available http://www.ftc.gov/os/2002/05/67fr36585.pdf#search=%2216%20CFR%20313.3(i)(1)%20(FTC)%22

[132.] Federal Register. “Privacy of Consumer Financial Information. Final Rule. Date 1 June 2000. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/info_sec/joi-privacy_final_rule_000601.pdf

[133.] Federal Register. “Privacy of Consumer Financial Information. Final Rule.13 of 76. Date 1 June 2000. 13 of 76. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/info_sec/joi-privacy_final_rule_000601.pdf

[134.] Federal Register. “Privacy of Consumer Financial Information. Final Rule.13 of 76. Date 1 June 2000. 56 of 76. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/info_sec/joi-privacy_final_rule_000601.pdf

[135.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 464-465 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[136.] Federal Register. “Privacy of Consumer Financial Information. Final Rule.13 of 76. Date 1 June 2000. 24vof 76. Accessed 3 September 2006. Available http://www.ffiec.gov/ffiecinfobase/resources/info_sec/joi-privacy_final_rule_000601.pdf

[137.] Friedman, Billings, Ramsey Group, Inc., SEC 10-K. Date 31 December 2005. 22 of 155. Accessed 3 September 2006. Available http://library.corporate-ir.net/library/71/713/71352/items/190515/FBR%2010K2005.pdf#search=%22california%20ab1950%20law%20su

[138.] Hunton & Williams. Testimony. U.S. HOUSE OF REPRESENTATIVES Committee on Small Business Subcommittee on Regulatory Reform and Oversight. “Data Protection and the Consumer: Who Loses When Your Data Takes a Hike?”. Date 23 May 2006. Accessed 3 September 2006. Available http://www.hunton.com/files/tbl_s47Details/FileUpload265/1497/Sotto_testimony_data-protection.pdf#search=%22California%20Information%20Saf

[139.] Anthony D. Milewski, Jr. “Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide” Shidler J. L. Com. & Tech. 19. Date 14 April 2006. Accessed 3 September 2006. Available http://www.lctjournal.washington.edu/Vol2/a019Milewski.html

[140.] California Civil Code. Civil Code Section 1798.80-1798.84. California’s AB 1950. Accessed 3 September 2006. Available http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

[141.] Federal Register. “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”. Date 29 March 2005. Vol. 70, No. 59. 3 of 19. Accessed 8 August 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/pdf/05-5980.pdf

[142.] National Science and Technology Council. “Federal Plan for Cyber Security and Information Assurance Research and Development”. Date April 2006. Accessed 3 August 2006. Available http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf

[143.] National Science and Technology Council. “Federal Plan for Cyber Security and Information Assurance Research and Development”. Date April 2006. Accessed 3 August 2006. Page xi. Available http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf

[145.] National Science and Technology Council. “Federal Plan for Cyber Security and Information Assurance Research and Development”. 79 of 140. Date April 2006. Accessed 3 August 2006. Available http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf

[146.] COSO. “Internal Control - Integrated Framework”. Date 1994. 9 of 163. Accessed 3 August 2006. Available https://www.cpa2biz.com/CS2000/Products/CPA2BIZ/Publications/Sub+1/Internal+Control+-+Integrated+Framework.htm

[147.] FDIC. “Risk Management Manual of Examination Policies – Bank Management’s Role” Accessed 14 September 2006. Available: http://www.fdic.gov/regulations/safety/manual/section10-1.html#part2

[148.] FDIC. Financial Institution Letter (FIL-64-2005). “Guidance on How Financial Institutions Can Protect Against Pharming Attacks”. Date 18 July 2005. Accessed 3 August 2006. Available http://www.fdic.gov/news/news/financial/2005/fil6405.html

[149.] Federal Register. “Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy”. Date 18 July 2006. 6 of 42. Accessed 3 August 2006. Available http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-6187.pdf

[150.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 11 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[151.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 23, 24 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[152.] FFIEC. “Information Security Booklet. Information Security Risk Assessment”. Date 27 July 2006. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/information_security/02_info_sec_%20risk_asst.htm

[152.] FFIEC. “Information Security Booklet. IT Handbook Presentation”. Date 27 July 2006. 4 of 10. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/presentations/infosec_presntation.pdf

[154.] FFIEC. E-Banking Handbook. Examination Procedures. 2003. Objective 6. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_03b_exam_procedures.html

[155.] FFIEC. “E-Banking Handbook. Risk Management of E-Banking Risks”. 2003. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_02_risk_mang.html

[156.] FFIEC. “E-Banking Handbook. Risk Management of E-Banking Risks”. 2003. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_02_risk_mang.html

[157.] FFIEC. “E-Banking Handbook. Risk Management of E-Banking Risks”. 2003. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_02_risk_mang.html

[158.] FFIEC. “Information Security Booklet. IT Handbook Presentation”. Date 27 July 2006. 2 of 10. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/presentations/infosec_presntation.pdf

[159.] FFIEC. “Information Security Booklet. Glossary”. Date 27 July 2006. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/information_security/08_app_glossary.html

[160.] FFIEC. “E-Banking Handbook. Presentation”. 2003. 2 of 10. Accessed 3 August 2006. Available http://www.ffiec.gov/ffiecinfobase/presentations/ebank_pres.pdf

[161.] FFIEC. “E-Banking Handbook. Glossary”. 2003. Accessed 2 August 2006. Available http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html

[162.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 266 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[163.] Federal Reserve Bank of Boston. “A Tale of Tails: An Empirical Analysis of Loss Distribution Models for Estimating Operational Risk Capital”. Date June 2006. 8 of 92. Accessed 14 September 2006. Available: http://www.bos.frb.org/economic/wp/wp2006/wp0613.pdf

[164.] Federal Reserve. Notice of Proposed Rule Making. “Risk-Based Capital Standards: Advanced Capital Adequacy Framework”. Date 5 September 2006. 1 of 501. Accessed 7 September 2006. Available http://www.federalreserve.gov/GeneralInfo/Basel2/NPR_20060905/NPR/Basel_II_NPR.pdf

[165.] MaCafee. “Top 10 Phishing Brands”. Date 14 September 2006.. Accessed 14 September 2006. Available http://www.mcafee.com/us/threat_center/anti_phishing/phishing_top10.html

[166.] Wall Street Journal. “Checks on Internal Controls Pays Off.” Date 8 May 2006

[167.] NOLO. “Domain Name”. Accessed 3 August 2006. Available http://www.nolo.com/definition.cfm/Term/3E9F8AE7-B46F-40A6-9E737BBFA8FDAE75/alpha/D/

[168.] Internet Society. “Domain Name System”. Date 27 January 2005. Accessed 3 August 2006. Available http://www.isoc.org/briefings/020/

[169.] Internet Society. “Culturally-appropriate Local Environments and a Global Internet Supplemental Information and Readings”. Date 9 May 2006. Accessed 3 August 2006. Available http://www.isoc.org/internet/issues/naming/multilingual-reading-prelim.pdf

[170.] FDIC. Financial Institution Letter (FIL-64-2005). “Guidance on How Financial Institutions Can Protect Against Pharming Attacks”. Date 18 July 2005. Accessed 6 August 2006. Available http://www.fdic.gov/news/news/financial/2005/fil6405a.html

[171.] The National Academies Press. “Signposts in Cyberspace: The Domain Name System and Internet Navigation (2005)”. Date 2005. 263 of 392. Accessed 6 August 2006. Available http://www.fdic.gov/news/news/financial/2005/fil6405a.html

