

IP Governance Task Force
Intellectual Property & Information Security Governance

To:	Office of the Comptroller of the Currency 250 E Street, SW. Mail Stop 1-5 Washington, DC 20219 OCC: Docket Number OCC-2007-0003 www.regulations.gov	Office of the Comptroller of the Currency 250 E Street, SW. Mail Stop 1-5 Washington, DC 20219 OCC: Docket Number OCC-2007-0004 regs.comments@occ.treas.gov
	Jennifer J. Johnson, Secretary Board of Governors of the Federal Reserve System 20th Street and Constitution Avenue, NW. Washington, DC 20551 Docket No. R-1280 regs.comments@federalreserve.gov	Jennifer J. Johnson, Secretary Board of Governors of the Federal Reserve System 20th Street and Constitution Avenue, NW. Washington, DC 20551 Docket No. OP-1277 regs.comments@federalreserve.gov
	Robert E. Feldman Executive Secretary Federal Deposit Insurance Corporation 550 17 th Street, NW. Washington, DC 20429 Comments@FDIC.gov Model Privacy Form	Robert E. Feldman Executive Secretary Federal Deposit Insurance Corporation 550 17 th Street, NW. Washington, DC 20429 Comments@FDIC.gov Basel II Supervisory Guidance
	Regulation Comments Chief Counsel's Office Office of Thrift Supervision 1700 G Street, NW. Washington, DC 20552 Attention: OTS- 2007-0005 www.regulations.gov	Regulation Comments Chief Counsel's Office Office of Thrift Supervision 1700 G Street, NW. Washington, DC 20552 Attention: No. 2007-06 regs.comments@ots.treas.gov
	Mary Rupp Secretary of the Board National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428 regcomments@ncua.gov Comments on Proposed Rule Part 716 (Model Form for Privacy Notice)	
	Federal Trade Commission Office of the Secretary Room 135 (Annex C) 600 Pennsylvania Avenue, NW. Washington, DC 20580 "Model Privacy Form, FTC File No. P034815" www.regulations.gov	
NPR:	Interagency Proposal for Model Privacy Form Under the Gramm-Leach-Bliley Act; Proposed Rule; Federal Register: March 29, 2007	Proposed Supervisory Guidance for Internal Ratings-Based Systems for Credit Risk, Advanced Measurement Approaches for Operational Risk, and the Supervisory Review Process (Pillar 2) Related to Basel II Implementation; Notice; Federal Register: February 28, 2007
Re:	Comments on Notice of Proposed Rules	Comments on Notice of Proposed Rules
Date:	May 29, 2007	May 29, 2007
Issue:	Model Privacy Form and Information Security Governance, Compliance and Metrics – Basel II	

1	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
---	--	--

IP Governance Task Force
Intellectual Property & Information Security Governance

We appreciate the opportunity to submit comments on the foregoing Notices of Proposed Rules (NPR). These share a common theme on compliance and related disclosures with information security regulations as it relates to identity theft and safeguarding customer identifying information. The direct linkage between the two NPRs is the process for determining, measuring and disclosing if a financial firm is in compliance with the model “confidentiality and privacy” language in the proposed privacy form that states, *per the [NPR dated March 29, 2007](#)*, “*To protect your personal information from unauthorized access and use, we use **security** measures that comply with federal law.*” The NPR of March 29, 2007 does not address a process for determining, measuring or disclosing the accuracy of the “confidentiality and privacy statement” but adopting the model privacy form conveys a Safe Harbor right for the financial firms. False and misleading privacy and security notices under GLBA 503 are an unfair or deceptive practice per the FTC ACT, e.g., [FTC v. Nations Title Agency](#); [FTC v. Nationwide Mortgage](#); [FTC v. Superior Mortgage](#) that in turn represent a “Retail Customer Disclosure Violation” and Operational Risk Loss Event under [Annex 9 of the June 2006, Basel Revised Framework Comprehensive Version](#) and a regulatory legal risk under the Basel II NPR dated [February 28, 2007](#). The security measures defined in GLBA 501(b) broadly fall into 2 categories, i.e., Information Technology and Safeguarding Intellectual Property. Measuring, per effective metrics, and setting, at the Board level, degrees of compliance or risk tolerances with the full range of security measures defined by federal law, specifically GLBA, FTC ACT, and FDICIA Section 112, to protect a consumers personal information is one of the requirements when applying the Basel II Advanced Measurement Approach for Operational Risk on Information Security Governance. Key recommendation: Disclosing Board-approved risk tolerances and matching metrics on the degree of compliance by each firm with federal and state information security regulations on safeguarding customer information should be an integral part of the model privacy form under GLBA 503 as it relates to the “confidentiality and privacy” disclosure. As currently drafted, i.e., “*we use security measures that comply with federal law*”, a firm could gain Safe Harbor status, under the model privacy form, with a partial compliance with federal regulations such as the example provided in the [NPR on page 14997](#), e.g., “These measures include computer safeguards and secured files and buildings.” The proposed language in the [March 29, 2007](#) NPR is not as comprehensive as the language it is replacing in the original confidentiality and privacy statement dated [June 1, 2000 Privacy of Consumer Financial Information; Final Rule](#), i.e., “We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.” Reconciling and unifying the two NPRs so there is a clarity, consistency, and coordination on standards for measuring and disclosing the degrees of compliance with federal information security regulations, including the model privacy statement, is the central objective of our combined comments on the two NPRs.

In our comments that follow, we define an Information Security Governance Framework, for financial firms regulated by the OCC, OTS, FRB, FDIC and NCUA, that is modeled on (1) the Basel II Advanced Measurement Approach for Operational Risk, (2) a literal interpretation of existing federal regulations on information security and consumer

2	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
---	---	---

IP Governance Task Force
Intellectual Property & Information Security Governance

protection laws and (3) a forensic analysis on enforcement cases by the FTC, OCC, OTS, FRB, FDIC and NCUA involving information security, information technology and consumer protection laws. Identity theft, reputation risks and information security vulnerabilities are cited with good reason by Audit Committees as priority issues for 2007 in large part because financial firms have yet to implement an Information Security Governance Framework at the board level as defined by the 32 Supervisory Standards of Appendix B per the Basel II Advanced Measurement Approach for Operational Risk that is based on a literal interpretation of existing federal regulations on information security and consumer protection laws. Currently, the lack of independent verification and validation of compliance with information security and consumer protection regulations at the Board level plus a scenario analysis with effective metrics on operational risks related to non-compliance with federal regulations by independent counsel is contributing, we believe, to the unbridled growth of online identity theft and related cyber attacks on consumers and Information technology networks. In other words, Boards lack effective, independent metrics and advice to measure compliance with information security governance regulations. Additionally, the complexity of the federal regulations with multiple regulators is a daunting task for large and small financial firms and their subject matter experts. This contributes to “regulatory fatigue” or non-compliance with information security regulations. Finally, there is a systemic imbalance in the application of information security regulations that includes, on one side, a concentration on Information Technology and, on the other side, a *de minimis* attention to safeguarding digital assets or intellectual property governance that enable federal crimes in the form of corporate identity theft against consumers and IT Networks, including multi-factor authentication. These issues all bubble to the surface when one maps out and measures compliance with the federal regulations on information security and consumer protection laws per the Basel II Advanced Measurement Approach for Operational Risk. Fundamentally, Boards of Directors need a refresher course on their obligations to comply with current federal regulations on information security and consumer protection especially given the stated objective of the federal financial regulators to investigate and enforce data security violations per the President’s Identity Theft Task Force Report. Our Task Force is preparing a series of seminars and webinars to address this issue based on our findings and recommendations herein. Secondly, Boards are strongly encouraged to engage qualified independent legal counsel to architect an Information Security Governance Framework for Basel II that complies with existing regulations. This is consistent with the recommendations by the federal financial agencies (1) in their enforcement cases when they recommend that counsel architect Information Security Programs and (2) in the Basel II NPR when they require independent verification and validation plus a scenario analysis involving expert opinions from business managers and risk management experts to derive reasoned assessments of the likelihood and loss impact of plausible high-severity operational losses. Qualified independent legal counsel should thus play the lead role in architecting, verifying and validating an Information Security Governance Framework for Basel II. Finally, measuring and managing compliance at the Board level with information security regulations should draw upon external (1) industry statistics on consumer and corporate identity theft from the FTC and FINCEN, (2) IT Audit metrics from the federal regulators and FFIEC for individual banks, (3) open-source IP Audit statistics and metrics

3	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
---	---	---

IP Governance Task Force
Intellectual Property & Information Security Governance

Introduction to Information Security Governance Framework

Enterprise Risk Management	Information Security Governance Framework: A Basel II Advanced Measurement Approach (AMA) for Operational Risk on Identity Theft.
Objective	Defining an open-source, enterprise risk management model for measuring and comparing: <ul style="list-style-type: none"> ▪ exposures to online identity theft. ▪ compliance with federal and state information security regulations.
Methodology	A literal interpretation and application of existing federal and state regulations on information security, i.e., GLBA, FTC ACT, FDICIA Section 112, Sarbanes-Oxley and California’s AB 1950, for banks, savings institutions and credit unions regulated by the FDIC, OCC, OTS, FRB and NCUA.
Paradigm	Intellectual Property owners have a fiduciary and legal obligation, especially in this digital age, to safeguard their intellectual property or digital assets from cyber attacks that are used in downstream federal crimes against their IT networks and online consumers. IP owners increasing their ownership levels of confusingly similar domain names used in fake web sites, email spam and phishing sites decrease (1) their supply for future cyber attacks, (2) the rate of future attacks on IT Networks and Consumers, (3) related operational losses for the bank and its consumers, (4) demands on law enforcement, and (5) reputation and operational risks thus leading to renewed consumer confidence and usage of internet channels for a positive ROI. Complying with information security regulations leads to operating efficiencies and a competitive advantage but it depends fully on Boards of Directors taking leadership and setting Board-approved risk tolerance metrics for compliance and providing relevant resources to achieve these objectives as outlined in Basel II.

A comparative review and mapping of the Basel II AMA objectives to the **Information Security Governance Framework and its Matrixes** is noted below in **bold font type**.

A bank’s AMA System should provide for the consistent application of operational risk policies and procedures throughout the bank, and address the roles of both the independent firm-wide operational risk management function and the lines of business. A sound AMA System will identify operational risk losses (**Matrix A**), calculate operational risk exposures (**Matrix B**) and associated operational risk capital, promote (**Matrix E1 – Scorecard**) risk management process and procedures to mitigate or control operational risks, and help ensure that management is fully aware of emerging operational risk issues. This framework should also provide (**Matrix E1 – Scorecard**) for the consistent and comprehensive capture and assessment of data elements needed to identify, measure, monitor and control the bank’s operational risk exposure. This includes identifying the nature, type(s), and underlying cause(s) of the operational loss event(s) (**Matrix D2 Scenario Analysis**). Moreover, the framework must also include independent verification and validation (**Matrix E1 – Scorecard**) to assess the effectiveness of the controls supporting the bank’s AMA System, including compliance (**Matrixes D, D1**) with policies, processes, and procedures. Given the importance of these functions, the Agencies believe that a bank’s validation and verification functions should begin their work soon after the bank has started to implement its AMA System. [NPR pages 9170-9171]

IP Governance Task Force
Intellectual Property & Information Security Governance

Mapping Basel II's 32 AMA Supervisory Standards to the Information Security Governance Framework

Five Major Groupings [Page 9170] and Supervisory Standards(S) from Appendix B	Narrative from NPR [Page 9170]	Information Security Governance Framework	
Operational Risk Management S1-S10	Standards for the Governance and organizational structures, including reporting, needed to manage operational risk. Basel II Supervisory Standards	Governance	Matrixes E, E1
		Operational Losses	Matrix A
		Operational Risks	Matrix B
Operational Risk Data and Assessment S11-S22	Establishes the standards for a consistent and comprehensive capture of the 4 elements of the AMA Internal Operational Loss Event Data External Operational Loss Event Data Scenario Analysis Business Environment and Internal Control Factors	Operational Losses	Matrix A
		Operational Risks	Matrix B
		Compliance & Internal Controls	Matrixes D, D1
		Scenario Analysis	D2
		Operational Risks	Matrixes B, B1, B2
Operational Risk Quantification S23-S30	Standards governing the systems and processes that quantify a bank's operational risk exposure.	Operational Risks	Matrix E1
Data Management and Maintenance S31	Standards to help insure that a bank's AMA system remains robust and relevant as its operational profile changes over time.	Governance	Matrix E1
Verification and Validation S32	Standards to help insure rigor, integrity and transparency for each bank's AMA System and the resulting operational risk component of the bank's risk-based capital requirement.	Governance	Matrix E1

IP Governance Task Force Intellectual Property & Information Security Governance

Definition: Information Security Governance includes IP or Intellectual Property Governance, IT or Information Technology Governance and Compliance Disclosures. These categories are derived from the supervisory guidances issued under GLBA¹ (Matrixes D, D1) to address the lifecycle of online identity theft risks. In the initial lifecycle stage, cyber criminals attack vulnerabilities in IP Governance by frequently using the digital assets or corporate identity of firms in the form of infringing domain names to launch downstream federal and state crimes such as fake or spoof web sites, sub-domain names, email-spam and phishing attacks to defraud consumers of their identifying information, a trade secret of a bank, and to penetrate a bank's IT network and multi-factor authentication.

INFORMATION SECURITY GOVERNANCE			NPRs
INFORMATION SECURITY GOVERNANCE FRAMEWORK (Basel II)			
FDICIA SECTION 112			
IP Governance	IT Governance	Compliance Disclosures	
GLBA 501(b), 521, 523	GLBA 501(b)	GLBA 503	Basel II Federal Register: February 28, 2007
IP Governance/IP Perimeter	IT Governance/IT Perimeter	The institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.	"Model Privacy Form" Federal Register: March 29, 2007
Trademark Infringements	Firewalls		
Corporate Identity Theft, Pretexting	Secure Socket Layers	FDICIA SECTION 112	
Domain Names (IP Asset Frauds)	Virus Protection		
Fake, Spoof Web Sites	Multi-Factor Authentication	SARBANES-OXLEY	
Sub-Domain Names	Virus Protection		
*Email-spam	Network Vulnerability	FTC ACT (UDAP) Deceptive Practices	
**Phishing	Intrusion Detection		
FTC ACT (UDAP)	Remote Access	Risk Tolerance Metrics	
*Deceptive Practices	Penetration Tests		
**Unfair Practices	Pharming Risks		
IP Audit Metrics	IT Audit Metrics		
Trade Secrets			
Customer Identifying Information			
Attempts to Acquire Consumer Identity Information	Attempts to Misuse Consumer Identity Information	Crime Completed Victim Harmed	
LIFE CYCLE OF IDENTITY THEFT			
President's Identity Theft Task Force Report: idtheft.gov			

An analysis of FTC enforcement cases involving phishing² confirm the following intellectual property and consumer protection risks, i.e.,

Intellectual Property & Consumer Protection Risks	Federal Regulations
False corporate affiliation, fraudulent email and web sites	Deceptive Acts under Section 5(a) FTC Act, Trademark Infringements
False claim of need to provide information	Deceptive Acts under Section 5(a) FTC Act
Email spoofing causing substantial injury to consumers	Unfair Practice under Section 5(a) FTC ACT
Unfair Use of Consumer's Information	Unfair Practice under Section 5(a) FTC ACT
Deceptive Pretexting of Financial Information by sending spam email and operating fraudulent web pages	Deceptive Acts under Section 5(a) FTC Act; GLBA 521, Trademark Infringement
Phishing (FTC Congressional Testimony)	Unfair Practice under Section 5(a) FTC ACT

7	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
---	--	---

IP Governance Task Force Intellectual Property & Information Security Governance

Operational Risk Loss Events – Matrix A:

A sound AMA System will identify operational risk losses (**Matrix A**). Presented below is **Matrix A, Operational Loss Events for Information Security and Identity Theft**. This includes relevant operational loss events from the US version of Basel II (NPR: 2-15-07) and the international version of Basel dated June 6, 2006, International Convergence of Capital Measurement and Capital Standards, for federal information security regulations on identity theft. This includes the addition from the international version of Basel these operational loss events omitted from the US version, i.e., Breach of Privacy, Retail Customer Disclosure Violations. These last two operational loss events are directly relevant for GLBA 503 and our earlier comments and recommendations for determining, measuring and disclosing the accuracy of the confidential and privacy statement per the Model Privacy Form and NPR of [March 29, 2007](#).

OPERATIONAL LOSS EVENTS - INFORMATION SECURITY AND IDENTITY THEFT		
Operational Risks	Operational Losses: 12 Events	Operational Loss Event (For Identity Theft)
Schedule V, February 15, 2007 (Page 9189)	BASEL Annex 9, June, 2006	Appendix E, Feb. 15, 2007
Business Environment and Internal Control Factors: The indicators of a bank's operational risk profile that reflect a current and forward-looking assessment of the bank's underlying business risk factors and internal control environment.	Client, Products, Bus. Practices Suitability, Disclosure & Fiduciary Fiduciary Breaches Guideline Violations	Client, Products, Bus. Practices Fiduciary Breaches Misuse of confidential customer information Money Laundering & Sale of Unauthorized products
Operational Risk 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).	Internal Fraud Unauthorized Activities Transactions Not Reported Theft and Fraud Account take-over, impersonations	Internal Fraud Employee theft, intentional misreporting of positions & insider trading by staff
Scenario Analysis A systematic process of obtaining expert opinions from business managers and risk management experts to derive reasoned assessments of the likelihood and loss impact of plausible high severity operational losses.	External Fraud Theft & Fraud Theft/robbery Systems Security Hacking Damage Theft of information w/ monetary loss Identity Theft (NPR 2-15-07)	External Fraud Robbery, forgery, check kiting Credit Card Losses (Identity Theft) (Page 202 of 254) Identity Theft
Unit of Measure The level (for example, organizational unit or operational loss event type) at which the bank's operational risk quantification system generates a separate distribution of potential operational losses.	Client, Products, Bus. Practices Retail Customer Disclosure Violations Breach of Privacy Losses from process management Unapproved access given to accounts	Client, Products, Bus. Practices Losses from process management Unapproved access given to accounts
Schedule V: February 15, 2007	Operational Losses (Basel)	Operational Losses (US Regulators)
Operational Risks	QIS 04 (FRB Boston)	
(Matrixes B & D: Reg. Compliance)	Est: .04% Total Assets or 12% of 4thQ NI, '05	
CAPITAL IMPACT	PROFIT & LOSS IMPACT (Matrix A)	PROFIT & LOSS IMPACT
MATRIX A: Operational Losses		

© Copyright 2007 by IP Governance Task Force. All Rights Protected

Unit of Measure should be calibrated on a consistent basis in the industry by auditing firms to match external statistics, per Matrix B, or the average identity theft loss reported to the FTC by consumers recognizing 46% of consumer identity theft attacks involve financial frauds (FTC & FINCEN statistics). Additionally, FRB Boston is requested to reveal for the public the retail banking identity theft losses as a percent of total assets as reported by the 23 largest US banks in the [QIS 04](#) study of \$25 billion in operational losses. Our rough analysis, after removing \$9 billion of operational losses for Enron and Worldcom from the \$25 billion, is that retail identity theft losses in 2004 approximate 4 basis points of total assets. This equates to approximately 12% of 4th Quarter Net Income 2005.

8	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
---	---	---



IP Governance Task Force Intellectual Property & Information Security Governance

Operational Risk Events – Matrix B:

A sound AMA System will calculate operational risk exposures and provide effective metrics to the Board for measuring and managing Board-approved risk tolerance levels.

Basel II NPR on Risk Tolerance Metrics	S 2. The bank must have and document a process that clearly describes its AMA System, including how the bank identifies, measures, monitors, and controls operational risk.
Board of Director Responsibility	“Other board of directors’ responsibilities with respect to operational risk may include: Understanding and approving the bank’s tolerance for operational risk; ¹³ ¹³ Banks use several approaches to define operational risk tolerance...These approaches will continue to evolve and <i>banks are encouraged to continue to develop effective metrics to define their operational risk tolerance.</i> ”

Presented below is **Matrix B, Operational Risk Drivers for Information Security and Identity Theft**. This is a sequence or pipeline of operational risk and operational loss phases that multiple in severity as they evolve from the root source of corporate identity theft risks into federal crimes that cause substantial harm to consumers across America in violation of federal information security regulations and consumer protection laws (Matrix D).

OPERATIONAL RISK DRIVERS: INFORMATION SECURITY AND IDENTITY THEFT				
IPGOVERNANCE.COM - Cascading Risks Flowing from a Fiduciary Failure to Safeguard IP				
Domain Name Ownership Levels	IP ASSETS	IP ASSET RISKS	Operational Risks: 11 Classes	Operational Losses: 12 Events
 Brand Safety	TRADEMARKS DOMAIN NAME UDRP = Infringement and Customer Confusion	FCM Metrics IP Ownership vs. Infringement Levels Identity Theft Criminal Act against Bank Asset SARS BOX 35u DOJ: BiNational Report	Regulatory Compliance FDICIA Section 112 Safeguard Assets, Comply with Regulations GLBA 501 (b): Prevent, Detect & Report Identity Theft SOX: IP Internal Controls Suspicious Activity	BASEL Annex 9 June 2006 Client, Products, Bus. Practices Suitability, Disclosure & Fiduciary Fiduciary Breaches Guideline Violations
	TRADE SECRETS SARS REPORTS IDENTITY THEFT CUSTOMER IDENTIFYING INFORMATION SEE FTC CONSUMER IDENTITY THEFT RISKS 46% FINANCIAL RISKS Per FTC Statistics	Computer Intrusion SARS BOX 35f Consumer Loan Fraud SARS BOX 35g Credit Card Fraud SARS BOX 35k Mortgage Loan Fraud SARS BOX 35p Terrorist Funding SARS BOX 35t	Reports Identity Theft Regulatory Fines Failure to Submit SARS & Lack of adequate Internal Controls, Senior Management Involvement, Training Enabling Federal Crimes (DOJ) Identity Theft, Wire Fraud, Bank Fraud, Computer Fraud & Abuse CAN-Span	Internal Fraud Unauthorized Activities Transactions Not Reported Theft and Fraud Account take-over, impersonations External Fraud Theft & Fraud Theft/robbery Systems Security Hacking Damage Theft of Information w/ monetary loss Identity Theft (NPR 2-15-07)
 Brand Risks	CORPORATE IDENTITY THEFT PHISHING EMAIL ADDRESSES FAKE WEB SITES SUB-DOMAIN NAME DOMAIN NAMES ENABLE	Domain Name in Header Deceptive Disclosures TARGETING CUSTOMER IDENTIFYING INFORMATION FINCEN Metrics	GLBA 503: Privacy Disclosure FTC Act, Section 5 UDAP: Unfair, Deceptive Acts or Practices California's AB 1950 GLBA 501(B) Non-compliance COSO - ERM	Unapproved access given to accounts
IP (ASSET) FRAUDS	IP (ASSET) FRAUDS	Operational Losses	Regulatory Compliance	Operational Losses (Basel)
Domain Name Ownership Levels	IP ASSETS	IP ASSET RISKS	Operational Risks	QIS 04 (FRB Boston)
Matrixes B1-2: IP Risk Tolerance & Online Brand Rating Models			(Matrixes B & D: Compliance)	Est: .04% Total Assets or 12% of 4thQ NI, '05
FRONT-END RISKS			CAPITAL IMPACT	PROFIT & LOSS IMPACT (Matrix A)
MATRIX B: OPERATIONAL RISK DRIVERS				

© Copyright 2007 by IP Governance Task Force. All Rights Protected

9	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
---	---	---

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Dynamic, Ongoing Quantification Process:

Quantification of each operational risk phase involves a combination of Intellectual Property Audits and a Scenario Analysis, each by independent counsel. Each of the quantification phases and models, summarized below, is dynamic and dependent on each other and change based on modifications within each model. The phases and models include:

IP Risk Tolerance Trend Analysis: 1999-2007.	
Partial Scenario Analysis for Operational Risks per Matrix B.	
Ownership Levels of Confusingly Similar Domain Names: Online Brand Rating.	Matrix B1
Operational or Legal Risk Exposure relating to potential litigation and/or regulatory fines, under the Scenario Analysis, for failing to enact GLBA and Consumer Protection Laws.	
IP Risk Tolerance Model: Matrix of Ownership Levels & Remediation Budgets to Compliance.	Matrix B2
Quarterly reports showing changes in the domain name ownership level based on degrees of success in (a) reaching and maintaining Board-approved domain-name ownership levels (b) preventing new domain name infringements.	

Summary: Independent Intellectual Property Audits and corresponding IP Ratings complement industry standard IT Audit and IT Audit Ratings from the FFIEC, which are now firmly established within the financial industry and regulatory examinations. Collectively, IP Ratings and IT Ratings independently (1) verify degrees of compliance with the full range of information security and consumer identity theft protection laws and (2) facilitate a peer review. Boards are directed by Basel II to develop effective metrics to define their operational risk tolerances. These metrics should be common, independent and available to the public to help the market conduct peer reviews and assess degrees of compliance with information security and consumer protection regulations for the model privacy statement, per the NPR of [March 29, 2007](#), and for general stakeholder interest in determining the relative quality of each information security program.

**IP Governance Task Force
Intellectual Property & Information Security Governance**

IP Risk Tolerance Trend Analysis 1999-2007:

External, open-source data bases, reveal the following domain name ownership levels, over the past 9 years, of confusingly similar domain names for 91 financial firms headquartered in the midwest and south, with total assets ranging from \$75 million to \$181 billion:

- The firms, on average, own less than 7% of the universe of confusingly similar domain names for their brands.
- Cyber criminals own double that figure – all of which are trademark infringements eligible for remediation through the cost-effective, global domain name arbitration process called UDRP or [Uniform Domain Name Dispute Resolution Policy](#). The IP owners, in this span of 9 years, have only reclaimed ownership of 58 infringing domain names through the UDRP process. The range of actual and/or potential federal crimes for each domain name is noted below:

Intellectual Property & Consumer Protection Risks	Federal Regulations
False corporate affiliation, fraudulent email and web sites	Deceptive Acts under Section 5(a) FTC Act, Trademark Infringements
False claim of need to provide information	Deceptive Acts under Section 5(a) FTC Act
Email spoofing causing substantial injury to consumers	Unfair Practice under Section 5(a) FTC ACT
Unfair Use of Consumer's Information	Unfair Practice under Section 5(a) FTC ACT
Deceptive Pretexting of Financial Information by sending spam email and operating fraudulent web pages	Deceptive Acts under Section 5(a) FTC Act; GLBA 521, Trademark Infringement
Phishing (FTC Congressional Testimony)	Unfair Practice under Section 5(a) FTC ACT

- And the balance or 81% is available for registration and use by any party.

These systemic intellectual property vulnerabilities have been building for 9 consecutive years and gaining in virility and effectiveness due to a *de minimis* effort by IP owners to safeguard their domain names and to clever advances by cyber criminals to penetrate IT security networks, including multi-factor authentication.

Board Choices & Consequences

Using Bank Assets For Fraud

Brand Risk Metrics

Domain Name Ownership Levels

"F" Rating

Current Paradigm:

High Risk =
Low Ownership
Levels of Bank
Assets

91 Midwest, Southern Financial Firms

IP Governance Task Force
Intellectual Property & Information Security Governance

Scenario Analysis for Operational Risks per Matrix B:

Financial firms and their Boards of Directors are exposed to a range of information security violations and operational/legal risks for their failure to:

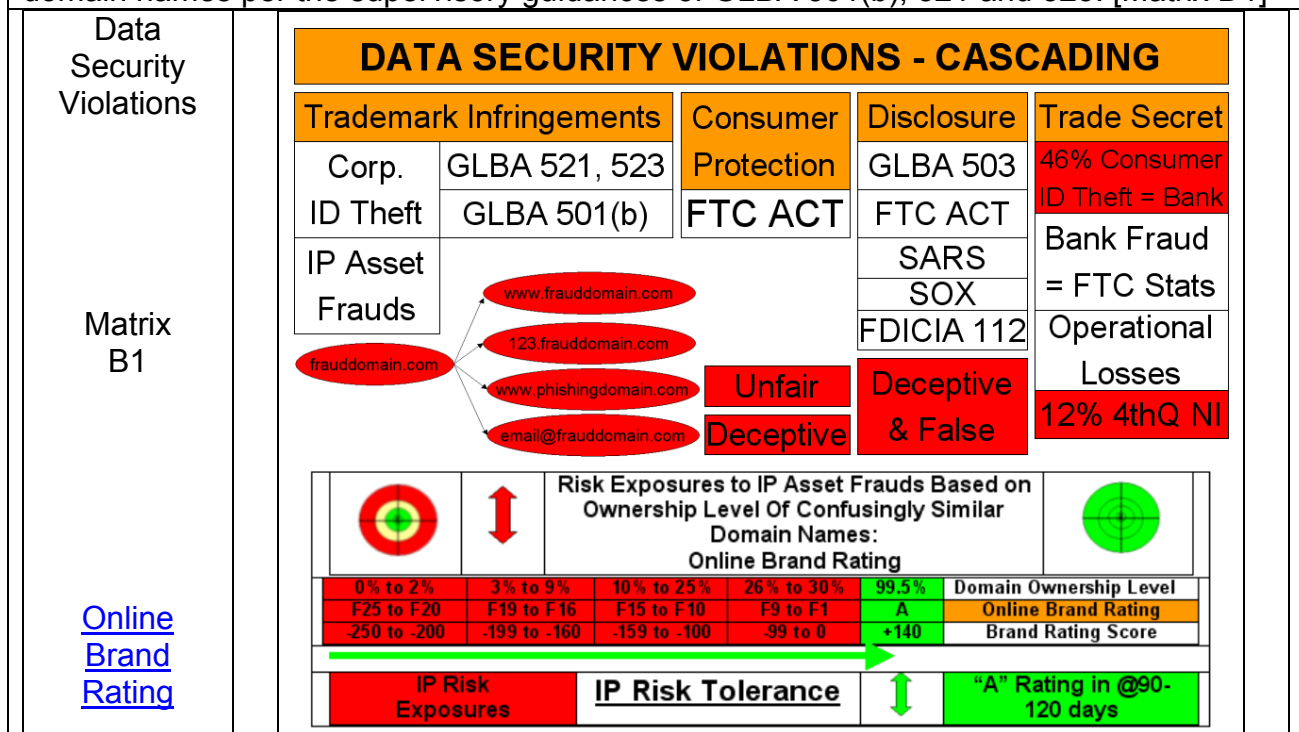
1. safeguard material assets, i.e., trademarks which are defined as brands and domain names and trade secrets which are defined as customer identifying information, per their fiduciary responsibilities under FDICIA Section 112. See TJ Hooper Case and RSA Case in Matrix D as examples of fiduciary failures of non-financial firms to safeguard material assets. Parallel arguments can be made under FDICIA Section 112 on the failure of financial firms to safeguard their digital assets from federal crimes in this digital age, especially by applying the TJ Hooper case. “*T.J. Hooper* held that the “avoidance of negligence” requires adherence to existing standards of care; standards which change as technology evolves. The *T.J. Hooper* concept of evolving standards is still good law. Standards can ratchet up over time, as new innovations become accepted practice.” Source: [Chris Gallagher](#). In 2007, the standards for information security and consumer protection laws are defined by the 11 classes of information security regulations in Matrix B.
2. comply with GLBA and the FTC ACT on safeguarding their brands and consumers from criminal acts and related federal crimes (Matrix B) per the supervisory guidances of GLBA 501(b), GLBA 521, GLBA 523, and the FTC ACT on deceptive and unfair practices per Matrixes D and D1. See the GLBA enforcement cases by the regulators whereby Boards of Directors failed to fully apply GLBA in Matrix D2.
3. post accurate Privacy and Security Statements under GLBA 503 when they fail to safeguard their intellectual property per GLBA and then state, in a deceptive manner, that, “We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.” See Matrix D2 and FTC v. Nations Title; FTC v. Nationwide Mortgage; FTC v. Superior Mortgage.
4. report suspicious activity reports as required by law and as confirmed by the Department of Justice (DOJ) in its October, 2006 BiNational Report on Phishing. The DOJ states (1) financial firms are legally required to submit Suspicious Activity Reports on a crime affecting a financial institution (including phishing)³ and (2) “companies that are victimized by phishing may not report these instances to law enforcement. Unlike some other types of internet-based crime, such as hacking, that may be conducted surreptitiously, phishing, by its nature, involves public misuse of legitimate companies’ and agencies’ names and logos [*trademark infringements – our insertion*]. Nonetheless, some companies may be reluctant to report all such instances of phishing to law enforcement – in part because they are concerned that if the true volume of such phishing attacks were made known to the public, their customers or accountholders would mistrust the companies or they would be placed at a competitive disadvantage.”⁴

12	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

**IP Governance Task Force
Intellectual Property & Information Security Governance**

5. report suspicious activity reports for one or more of the 6 relevant Identity Theft Operational Loss federal crimes (Matrix B) that include computer intrusions, consumer loan fraud, credit card fraud, mortgage loan fraud, terrorist funding (BSA/AML Examination Handbook defines identity theft⁵ as a form of terrorist funding) plus corporate identity theft (SARS Box 35u), i.e., infringing domain names in deceptive and unfair practices.
6. establish adequate internal controls per FDICIA Section 112 and COSO to prevent, detect and report criminal acts against bank assets to FINCEN and the Board of Directors. The risk profiles of the financial firms fined in BSA/AML civil money cases by FINCEN (Matrix D2) are similar in nature to the risk profiles of the financial firms that are failing to safeguard their intellectual property per GLBA and FTC ACT, i.e., lack of senior management involvement, lack of internal controls, lack of training, failure to report suspicious activity reports, and lack of a compliance officer for this class of risk.

The top half of the diagram below is a summary of the range of Data Security Violations due to the failure of financial firms to fully enact the information security regulations of GLBA¹, especially as it relates to preventing the deceptive and defrauding use of bank domain names per the supervisory guidances of GLBA 501(b), 521 and 523. [Matrix D1]



The lower half of the diagram measures the ownership levels of confusingly similar domain names for a portfolio of bank trademarks on a scale ranging from less than 1% to 99.5% as a way to measure degrees of (1) compliance with safeguarding brands from infringing domain names and (2) exposure to operational risks (data security violations) for failing to safeguard domain names from use in federal crimes. *Low ownership levels equate to high risk exposures. This is the Online Brand Rating model. – Matrix B1.*

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Ownership Levels of Confusingly Similar Domain Names: Online Brand Rating	Matrix B1
--	--------------

<p>IP Risk Tolerances:</p> <p>Online Brand Rating</p> <p>Peer Review</p>	<p>The lower half of the diagram in Matrix B1 (see above) measures the ownership levels of confusingly similar domain names for a portfolio of bank trademarks on a scale ranging from less than 1% (F25 Rating) to 99.5% (A Rating) as a way to measure degrees of (1) compliance with safeguarding brands from infringing domain names and (2) exposure to operational risks (data security violations) for failing to safeguard domain names from use in federal crimes. <i>Weak online brands (F Ratings) are defined by low domain name ownership levels that equate to low remediation budgets and high operational risk exposures while strong online brands (A Ratings) are defined by high domain name ownership levels that equate to corresponding intellectual property investment budgets and low operational risk exposures. This is the Online Brand Rating model. – Matrix B1.</i></p>
---	--

Board of Director Metrics: Boards select and approve a desired ownership level or risk tolerance for confusingly similar domain names on a scale of less than 1% (F25 Rating) to 99.5% (A Rating) for the brands of their firm. The ownership level and corresponding Online Brand Rating has a matching:

1. Operational or Legal Risk Exposure relating to potential litigation and/or regulatory fines, under the Scenario Analysis, for failing to enact GLBA and Consumer Protection Laws.
2. Remediation budget for reaching the desired domain-name ownership level and Online Brand Rating. A scale of domain name ownership levels and remediation budgets is provided in Matrix B2 in the “IP Risk Tolerance Model - Matrix of Ownership Levels & Remediation Budgets to Compliance”
3. Quarterly report showing changes in the domain name ownership level and Online Brand Rating based on degrees of success in (a) reaching and maintaining Board-approved domain-name ownership levels and (b) preventing new domain name infringements.

IP Governance Task Force
Intellectual Property & Information Security Governance

The next phase in the Operational Risk Quantification process is the:

Operational or Legal Risk Exposure relating to potential litigation and/or regulatory fines, under the Scenario Analysis, for failing to enact GLBA and Consumer Protection Laws.

This analysis centers on domain name valuations and compliance with the reporting of infringing domain names and their variations through Suspicious Activity Reports (BOX 35u-Identity Theft) to FINCEN and Boards of Directors as required by FDICIA Section 112 and GLBA 501(b). This last part requires analysis and verification by independent counsel due to the confidential nature of Suspicious Activity Reports.

Our analysis begins with a quote from the FDIC FIL 64-2005 on the importance of domain names, then provides a valuation range on infringing domain names and concludes with an economic summary of estimated operational risks.

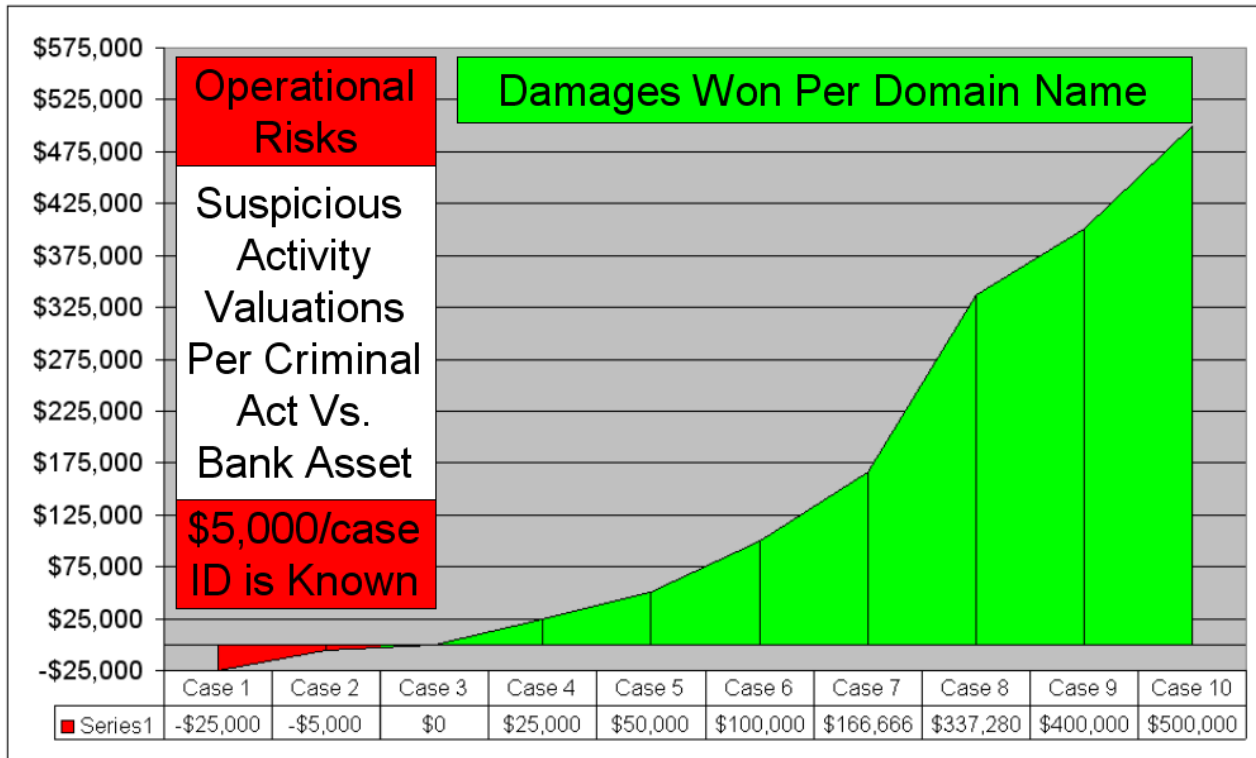
Domain Name Valuations:

The [FDIC's 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*."

Banks are required to report infringing domain names through Suspicious Activity Reports, [BOX 35U-Identity Theft](#), per FDICIA Section 112 and the GLBA 501(b) supervisory guidances (Matrix D1) and their failure to do so exposes the banks to operational or legal risks and fines through civil money penalties from the regulators and/or FINCEN.

Valuations of infringing domain names are addressed in the following chart.

**IP Governance Task Force
Intellectual Property & Information Security Governance**



-\$25,000	SARs Box 35U : Section 1c for infringing domain names where the identity of the perpetrator is not known per the whois domain name records.
	SARs Box 35U : Section 1b for infringing domain names where the identity of the perpetrator is known per the whois domain name records.
-\$0	SARs Box 35U : Section 2 of SARs for Phishing Sites where consumers reveal sensitive customer information in fraudulent web sites.
\$25,000	'01 Damages for ernestandjuliogallo.com (holding it as real estate).
\$50,000	'02 Damages for pinehurstresort.com (dilution and cybersquatting): Pinehurst v. Wick
\$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. Elec. Boutique Holdings Corp. v. Zuccarini
\$166,666	'02 Damages for watchreplica.com (counterfeiting, infringement, dilution, and cybersquatting). Louis Vuitton Malletier v. Veit
\$337,280	'02 Damages for entrepreneurpr.com . Plaintiff, owner of the registered mark

IP Governance Task Force
Intellectual Property & Information Security Governance

	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
\$400,000	'04 Damages for medpets.com (dilution, infringement, unfair competition, cybersquatting). Petmed Express, Inc. v. Medpets.com, Inc.
\$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 . Damages may be trebled to \$1,500,000 in egregious phishing cases.
\$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
\$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)
\$28,945,515	'05 Damages for yesmoke.com (Sale of gray-market cigarettes): Philip Morris USA, Inc. v. Otamedia Ltd

Given the historical damages won by trademark owners on domain name infringement cases ranging from \$25,000 and higher, the ability of trademark owners to litigate for damages of up to \$500,000 per infringing domain name under recent state-based anti-phishing laws and given the harm caused to consumers by fake web sites, email spam and phishing, Boards of Directors should adopt a zero tolerance level and require the reporting and remediation of all infringing domain names in an effort to take leadership and safeguard their bank brands, customers and reputations from direct cyber attacks. This strategy represents a paradigm shift in the industry whereby IP owners and Boards of Directors step forward and take responsibility for safeguarding their intellectual property thus minimizing downstream cyber attacks on their consumers and IT networks. This model is embedded in the existing information security regulations based on a literal interpretation and application of GLBA 501(b), GLBA 521, GLBA 523, the FTC ACT and FDICIA Section 112.

IP Governance Task Force
Intellectual Property & Information Security Governance

One way to quantify operational or legal risks within the information security and consumer protection program is to apply the \$5,000 reporting valuation for a Corporate Identity Theft crime against a bank asset, per BOX 35U of the Suspicious Activity Report, for every infringing domain name that has not been reported in a SARS report and for matching but available domain names. Considering firms own on average less than 7% of confusingly similar domain names, that cyber criminals own double that amount and the balance or 81% is available for registration by any party, it is fair to characterize the industry's exposure to infringing domain names and related federal crimes as severe and serious. Applying this operational risk quantification model to the 91 financial firms headquartered in the midwest and south yields an average Operational Risk figure of approximately 5% of 4th Quarter Net Income for all 91 firms, including those with assets in excess of \$1 billion. The Operational Risk exposure represents a larger percentage of 4thQ Net Income, 2005 for firms with assets less than \$1 billion as they lack the economies of scale with a smaller asset base for their brand. *This is a systemic risk in the banking industry that cuts across firms regulated by the FDIC, OCC, OTS, FRB and NCUA.*

1			91 Firms
106	Operational Risks/ Net Income 4thQ 2005		
107	\$181b to \$32b	9	4%
108	\$31.9b to \$15.1B	4	4%
109	\$15b to \$5.1b	9	10%
110	\$5b to \$1b	26	16%
111	Greater Than \$1b	48	5%
112			
113	Less Than \$1b		
114	\$0.99b to \$0.45b	21	22%
115	\$0.44b to \$0.075B	22	88%
116	Less Than \$1b	43	34%
117	Average	91	5%

1	Total Assets By Primary Regulator	# of Firms	2005
2	FDIC	29	\$42,420,327,000
3	OCC	25	\$391,795,131,730
4	OTS	5	\$28,235,357,000
5	FRB	16	\$544,454,776,000
6	Credit Unions	16	\$7,450,561,897
7	Total Assets	91	\$1,014,356,153,627

Another way to quantify operational risk exposures is to compare civil money penalties and litigation settlements in comparable cases for each firm under the leadership of independent counsel.

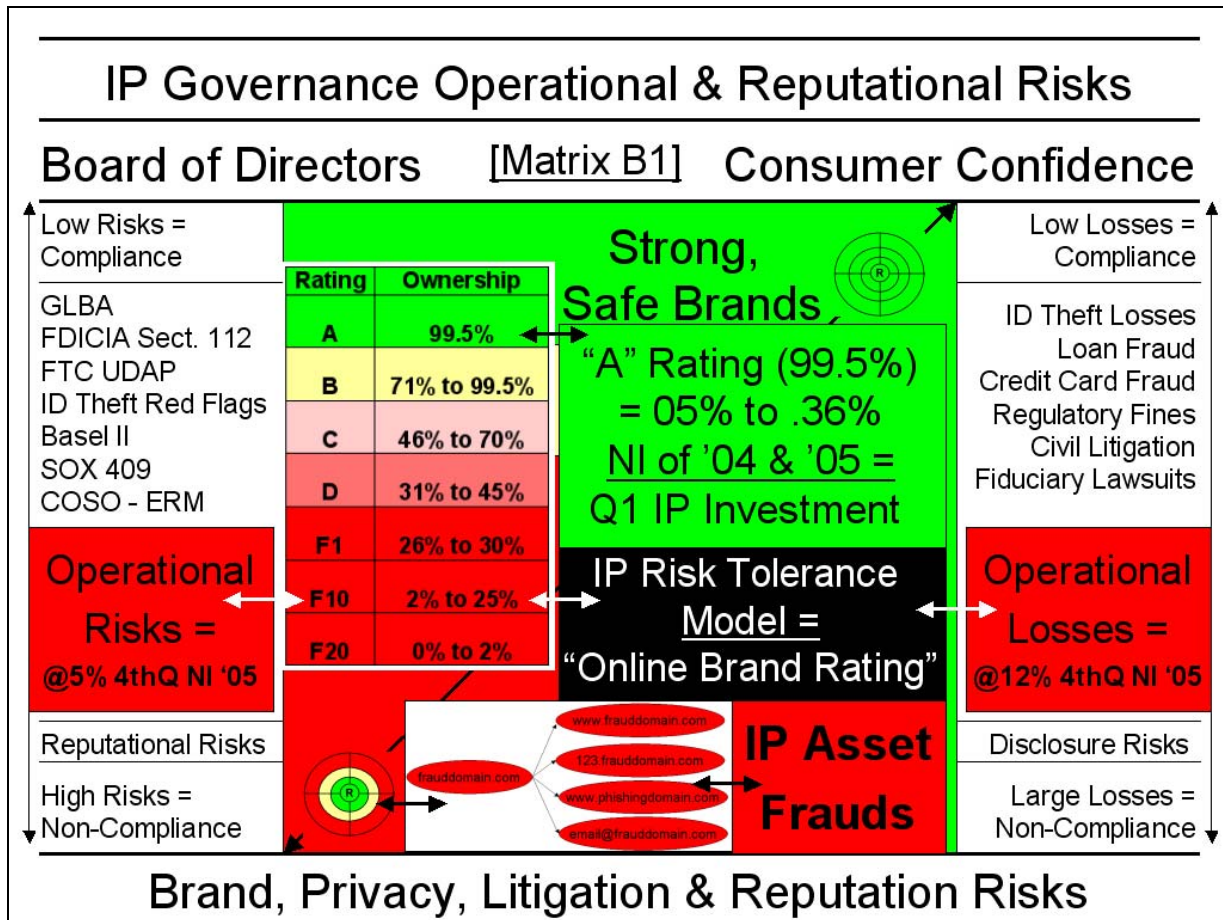
Of course, the need for such analysis diminishes in direct relationship with a firm's compliance with existing information security and consumer protection regulations.

**IP Governance Task Force
Intellectual Property & Information Security Governance**

IP Risk Tolerance Model - Board Approved IP Risk Tolerances – Matrix B2

Merging and plotting the key drivers from the foregoing models into the IP Risk Tolerance Model shows how a range of low, medium and high ownership levels of confusingly similar domain names for a set of brands and trademarks corresponds with:

- **operational losses** as defined in Matrix A and Matrix B. Low domain name ownership levels explain the rapid growth of fake web sites, email spam and phishing and related consumer and corporate identity theft operational losses. It also foretells a continuation of existing identity theft trends in the financial sector due to a failure of individual firms to attack this problem at its root source.
- **operational risk exposures** or legal risks for failing to safeguard its intellectual property, i.e., trademarks and trade secrets from IP Asset Frauds or federal crimes as defined in Matrixes A & B and the Scenario Analysis.
- **an investment/remediation budget** tied to desired domain name ownership level by a Board of Directors. Reversing the current trend requires leadership by a Board of Directors to safeguard its intellectual property by increasing their ownership levels of confusingly similar domain names through remediation to a level close to a 99.5% ownership level or “A” Online Brand Rating. This is estimated to equal between 5 basis points and 36 basis points of consolidated net income for 2005 and 2004 per our



IP Governance Task Force
Intellectual Property & Information Security Governance

recent study on 91 financial firms headquartered in the midwest and south. This same level of investment to solve 9 years of ballooning risks equates to less than 4% of the marketing budget for 2005 and 2004 for the smallest firms or less than .46% of the marketing budget for 2005 and 2004 for the largest firms in the study. This is a relatively small investment for a Board in a firm's brand to (1) reach compliance and (2) safeguard their brands, consumers and IT Networks from online identity theft attacks.

1			91 Firms
2	Total Assets	# of Firms	2005
143			
144	IP Investment ("A" Rating)/Net Income (04 & 05)		
145	\$181b to \$32b	9	0.03%
146	\$31.9b to \$15.1B	4	0.06%
147	\$15b to \$5.1b	9	0.11%
148	\$5b to \$1b	26	0.19%
149	Greater Than \$1b	48	0.05%
150			
151	Less Than \$1b		
152	\$0.99b to \$0.45b	21	0.29%
153	\$0.44b to \$0.075B	22	0.64%
154	Less Than \$1b	43	0.36%
155	Average	91	0.05%
413			
414	IP Investment / Marketing Budget (04 & 05)		
415	\$181b to \$32b	9	0.46%
416	\$31.9b to \$15.1B	4	0.79%
417	\$15b to \$5.1b	9	0.93%
418	\$5b to \$1b	26	2.37%
419	Greater Than \$1b	48	0.62%
420		0	
421	Less Than \$1b	0	
422	\$0.99b to \$0.45b	21	2.52%
423	\$0.44b to \$0.075B	22	3.71%
424	Less Than \$1b	43	2.86%
425	Average	91	0.66%

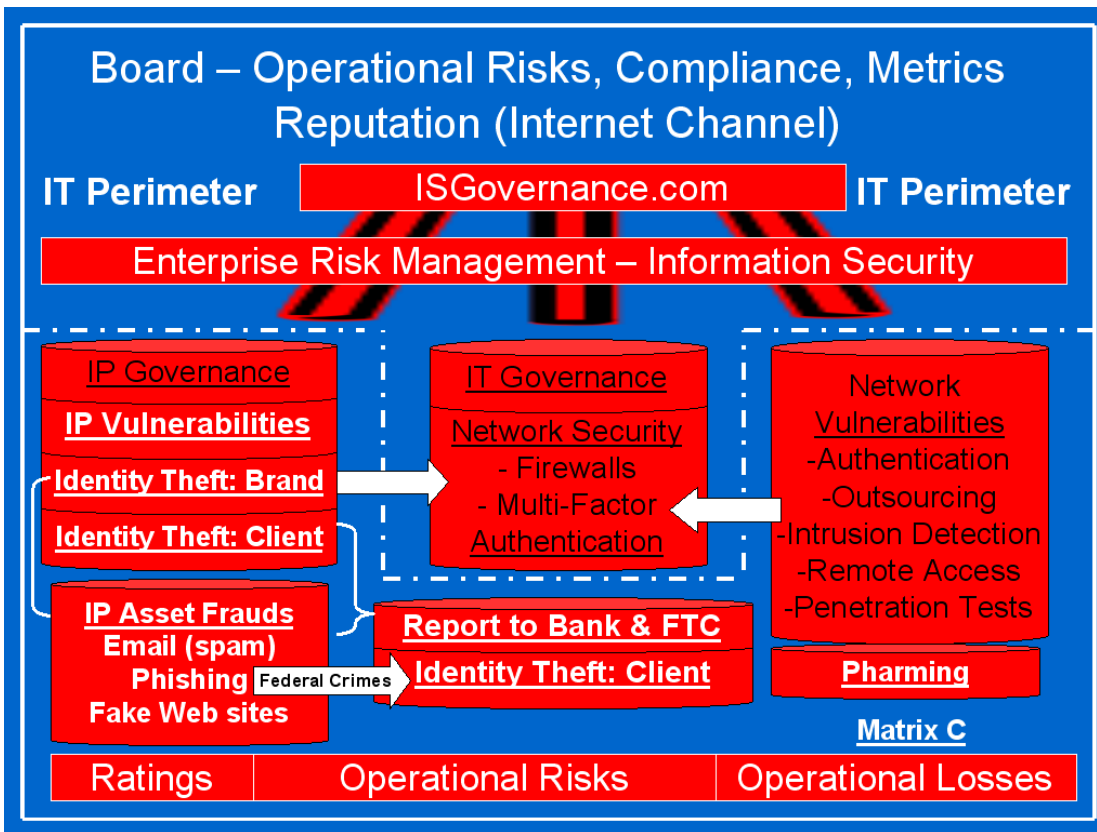
In summary, the operational risk quantification program include these interrelated models:

IP Risk Tolerance Trend Analysis: 1999-2007	
Partial Scenario Analysis for Operational Risks per Matrix B	
Ownership Levels of Confusingly Similar Domain Names: Online Brand Rating	Matrix B1
Operational or Legal Risk Exposure relating to potential litigation and/or regulatory fines, under the Scenario Analysis, for failing to enact GLBA and Consumer Protection Laws.	
IP Risk Tolerance Model: Matrix of Ownership Levels & Remediation Budgets to Compliance	Matrix B2
Quarterly reports showing changes in the domain name ownership level based on degrees of success in (a) reaching and maintaining Board-approved domain-name ownership levels (b) preventing new domain name infringements.	

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Information Security – Matrix C:

This is a diagram of 3 parallel and complementary functions defined in the Information Security guidances issued under GLBA 501(b) by the federal banking regulators. The terms IT or Information Technology Governance and Network Vulnerability are common terms and functions within the Information Technology industry. We coined the term IP or Intellectual Property Governance to address the body of federal regulations on safeguarding trademarks and trade secrets from online identity theft. The foregoing operational risk analysis confirms there is a systemic imbalance in the application of information security regulations that includes, on one side, a concentration on Information Technology and, on the other side, a *de minimis* attention to safeguarding digital assets or intellectual property governance that enable federal crimes in the form of corporate identity theft against consumers and IT Networks, including multi-factor authentication. The purpose of our comments is to outline the foregoing systemic risks and recommend a holistic Enterprise Risk Management model for Information Security Governance that unifies all 3 parallel, complementary and required functions for an effective model in safeguarding online customer information. Thinking outside of the IT Perimeter and addressing the external risks involving the fraudulent use of bank assets against online consumers and IT Networks is consistent with a literal interpretation and application of existing federal regulations on information security and consumer protection laws.

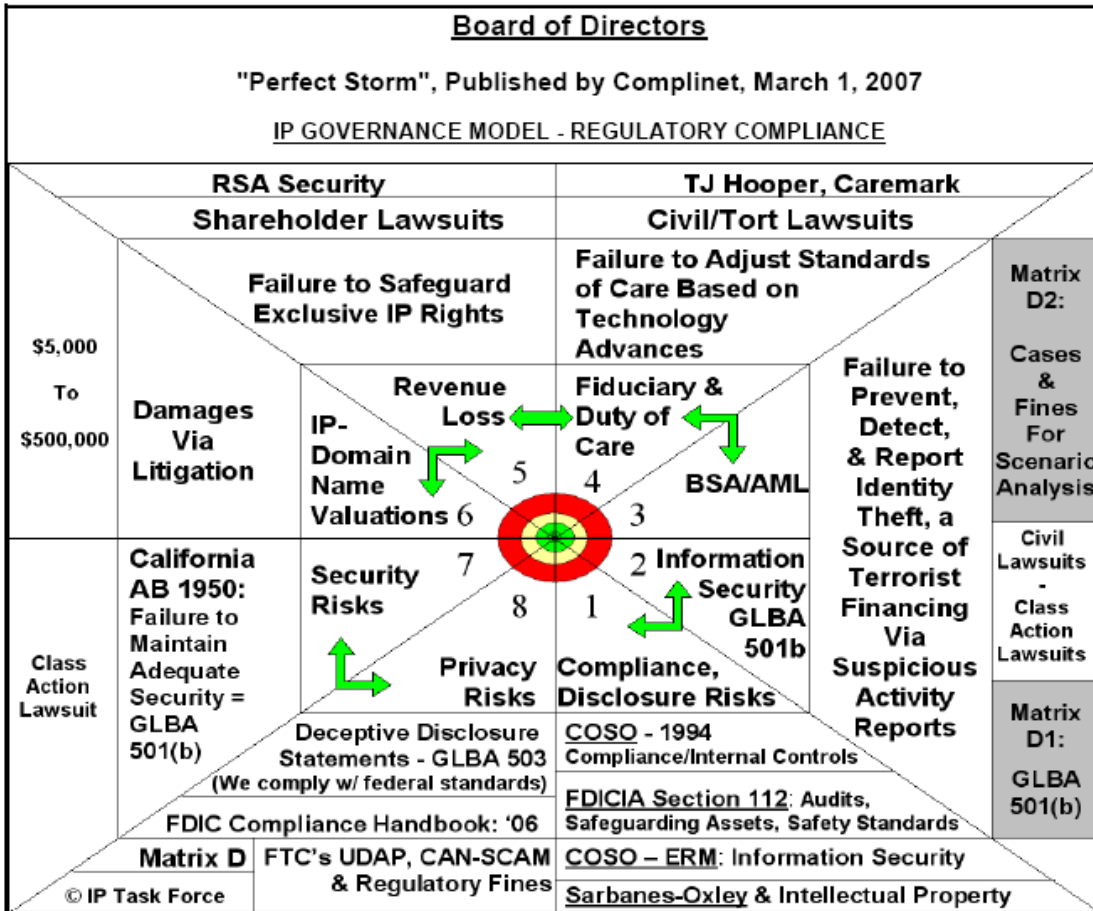


"F" Ratings	5% - 4thQ, NI, '05 & '04	12% - 4thQ NI, '05 & '04
--------------------	-------------------------------------	--

21	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Compliance & Internal Controls: IP Governance: Matrix D



Matrix D analyzes the maze of federal and state regulations that are relevant for intellectual property operational risks and operational losses per information security and consumer protection laws. This analysis is available [online](#) and has already been shared with the FDIC and FRB in January, 2007. A letter from the FDIC thanked the IP Governance Task Force for its analysis and indicated the analysis was being shared with staff members. In summary, the regulations direct financial firms to safeguard their intellectual property especially as it relates to federal crimes involving information security and consumer protection laws. As it relates to our comments herein on the 2 NPRs, we shall focus on the specific GLBA and FTC regulations (Matrix D1) and enforcement cases (Matrix D2) that have a direct bearing on firm's degree of compliance with safeguarding its intellectual property, i.e., trademarks and trade secrets from federal crimes against consumers and IT networks. These regulations, supervisory guidances and enforcement cases are listed in the following Matrixes and may be accessed by clicking on each one within the live version of the Information Security Governance Framework cited in the Table of Contents. This is a comprehensive virtual library that includes supervisory guidances and enforcement cases that are cited and omitted from the President's Identity Theft Task Force Report (www.idtheft.org).

IP Governance Task Force Intellectual Property & Information Security Governance

Matrix D1 - GLBA and FTC Regulations and Supervisory Guidances

INFORMATION SECURITY GOVERNANCE FRAMEWORK (Basel II)						IP Governance	IP Governance	IT Governance
Matrix D1						Identity Theft Domain Names Suspicious Activity Reports (SARS) Spoofed Web Sites	Phishing	Pharming
C O D E	President's Identity Theft Task Force	Agency	Date	File	Information Security Governance; Regulatory Guidances; GLBA 501(b) FTC ACT Section 5			
R	PITTF	OTS	6/4/2001	CEO Ltr 139	Identity Theft and Pretext Calling	Identity Theft, SARS		
R	PITTF	OTS	3/3/2004	Letter #193	Phishing and E-mail Scams	Domain Name, SARS	Yes	
R	PITTF	OTS	9/8/2004	Letter #205	Phishing Customer Brochure		Yes	
		OTS	3/30/2005	Letter #214	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	Identity Theft		
O	PITTF	OTS	10/12/2005	Letter #228	Interagency Guidance on Authentication in an Internet Banking Environment	Spoof web sites, domain names	Yes	Yes
		OTS	12/14/2005	Letter #231	Interagency Guidelines Establishing Information Security Standards	Identity Theft		
O	PITTF	OCC	07/19/00	Alert 2000-9	Protecting Internet Addresses of National Banks	Domain Name, SARS		
R	PITTF	OCC	4/30/2001	AL 2001-4	Identity Theft and Pretext Calling	Identity Theft, SARS		
R	PITTF	OCC	9/9/2003	Alert 2003-11	Customer Identity Theft: E-Mail-Related Fraud Threats	Domain Name, SARS	Yes	
		OCC	4/14/2005	Bulletin 2005-13	Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance	Identity Theft	Yes	
R	PITTF	OCC	7/1/2005	Bulletin 2005-24	Risk Mitigation and Response Guidance for Web Site Spoofing Incidents	Domain Name, Privacy, SARS	Yes	Yes
O	PITTF	OCC	10/12/2005	Bulletin 2005-35	Authentication in an Internet Banking Environment	Spoof web sites	Yes	Yes
		NCUA	05/30/00	LTR 00-CU-02	Identity Theft Prevention	Identity Theft		
		NCUA	9/30/2001	LTR 01-CU-09	Identity Theft and Pretext Calling	Identity Theft, SARS		
O	PITTF	NCUA	12/02/02	02-CU-16	Protection of Credit Union Internet Addresses	Domain Name		
O	PITTF	NCUA	8/1/2003	03-CU-12	Procedent newspaper, advertisements, and Websites by Entities Claiming to be Credit Unions	Domain Name, SARS		
O	PITTF	NCUA	4/1/2004	LTR 04-CU-06	E-Mail and Internet Related Fraudulent Schemes Guidance	Domain Name, SARS	Yes	
		NCUA	9/30/2004	LTR 04-CU-12	Phishing Guidance for Credit Union Members	Brochure	Yes	
O	PITTF	NCUA	12/1/2005	LTR 05-CU-20	Phishing Guidance for Credit Unions And Their Members	Domain Name, SARS	Yes	Yes
		FTC	11/01/02	FTC vs. GM Funding	FTC Act, Section 5, UDAP	Identity Theft, Unfair Practice - FTC ACT	Phishing Case, Unfair Practice	
		FTC	07/01/03	FTC vs. CJ	FTC Act, Section 5, UDAP	Identity Theft, Unfair Practice - FTC ACT	Phishing Case, Unfair Practice	

INFORMATION SECURITY GOVERNANCE FRAMEWORK (Basel II)						IP Governance	IP Governance	IT Governance
Matrix D1						Identity Theft Domain Names Suspicious Activity Reports (SARS) Spoofed Web Sites	Phishing	Pharming
C O D E	President's Identity Theft Task Force	Agency	Date	File	Information Security Governance; Regulatory Guidances; GLBA 501(b) FTC ACT Section 5			
		FTC	12/4/2003		Fair and Accurate Credit Transactions Act of 2003 (FACT Act)	Identity Theft Definition: 121 Section 111 of the FACT Act defines "identity theft" as "a fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade] Commission may prescribe, by regulation." 15 U.S.C. 1681a(g)(3).		
		FTC	3/1/2004	FTC vs. Zachary Hill	FTC Act, Section 5, UDAP	Identity Theft, Unfair Practice - FTC ACT	Phishing Case, Unfair Practice	
		FTC	6/16/2005	CONGRESSIONAL TESTIMONY	DATA BREACHES AND IDENTITY THEFT	The FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition. 12. The Commission has used this authority to challenge a variety of injurious practices that threaten data security. 13.13 These include, for example, unauthorized charges in connection with "phishing" e.g. See FTC v. Hill, FTC v. C.J.	Yes	
		FTC	7/18/2006		Identity Theft Red Flag Rules - Notice of Proposed Rulemaking	Identity Theft Red Flag Rules		
R	PITTF	FRB	4/8/2001	SR 01-11	Identity Theft and Pretext Calling	Identity Theft, SARS		
		FRB	3/11/2004	CA 04-2	Unfair or Deceptive Acts or Practices by State Chartered Banks	Identity Theft, Unfair Practice - FTC ACT		
O	PITTF	FRB	10/13/2005	SR 05-19	Interagency Guidance on Authentication in an Internet Banking Environment	Spoof web sites	Yes	Yes
		FRB	12/1/2005	SR 05-23	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	Identity Theft	Yes	
		FINCEN	7/1/2003	SARS Box 35u	Identity Theft	Identity Theft (Box 35u)		
		FFIEC	02/01/01		Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness	Yes		
O	PITTF	FFIEC	8/1/2003	E-Banking Booklet	E-Banking Request Letter	Domain Name, SARS		
O	PITTF	FFIEC	10/7/2005		Authentication in an Internet Banking Environment	Spoof web sites	Yes	Yes
R	PITTF	FFIEC	7/30/2006		Information Security Handbook	Domain Name, Spoof web sites, phishing	Yes	Yes

IP Governance Task Force Intellectual Property & Information Security Governance

INFORMATION SECURITY GOVERNANCE FRAMEWORK (Basel II)						IP Governance	IP Governance	IT Governance
Matrix D1						Identity Theft Domain Names Suspicious Activity Reports (SARS) Spoofed Web Sites	Phishing	Pharming
C O D E	President's Identity Theft Task Force	Agency	Date	File	Information Security Governance; Regulatory Guidances; GLBA 501(b) FTC ACT Section 5			
R	PITTF	FFIEC	8/15/2006		FFIEC Guidance on Authentication in an Internet Banking Environment	Spoof web sites, phishing	Yes	Yes
O	PITTF	FDIC	11/08/00	FIL 77-2000 (omitted in FIL-32-2007)	Protecting Internet Domains	Domain Name, SARS		
		FDIC	03/14/01	FIL-22-2001	Guidelines Establishing Standards for Safeguarding Customer Information			
R	PITTF	FDIC	5/9/2001	FIL-39-2001	Guidance on Identity Theft and Pretext Calling	Identity Theft, SARS		
O	PITTF	FDIC	8/24/2001	FIL-58-2001	Examination Procedures to Evaluate Customer Information Safeguards	#7: Incident Responses, reports to law enforcement, regulators		
		FDIC	5/30/2002	FIL-57-2002	Guidance on Unfair or Deceptive Practices	Identity Theft, Unfair Practice - FTC ACT		
		FDIC	8/13/2003	FIL-63-2003	Guidance on Identity Theft Response Programs	Seeking Commentary		
		FDIC	09/26/03	Audit Report No. 03-044	The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V -- Privacy Provisions			
		FDIC	3/11/2004	FIL-26-2004	Unfair or Deceptive Acts or Practices by State Chartered Banks	Identity Theft, Unfair Practice - FTC ACT		
R	PITTF	FDIC	3/12/2004	FIL 27-2004 (Omitted in FIL-32-2007)	Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes	Domain Name, SARS	Yes	
R	PITTF	FDIC	9/13/2004	FIL-103-2004	Interagency Informational Brochure on Internet Phishing Scams	Brochure	Yes	
R	PITTF	FDIC	12/14/2004	FIL 132-2004	Identity Theft Study on "Account Hijacking" Identity Theft and Suggestions for Reducing Online Fraud	Domain Name, SARS	Yes	
		FDIC	4/1/2005	FIL-27-2005	Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	Identity Theft	Yes	
R	PITTF	FDIC	7/5/2005	FIL-59-2005	Identity Theft Study Supplement on "Account Hijacking Identity Theft"	Spoof web sites, phishing	Yes	
O	PITTF	FDIC	7/18/2005	FIL 64-2005	Pharming Guidance on How Financial Institutions Can Protect Against Pharming Attacks	Domain Name, SARS	Yes	Yes
R	PITTF	FDIC	7/22/2005	FIL-66-2005	Guidance on Mitigating Risks From Spyware	Spoof web sites, phishing	Yes	Yes
O	PITTF	FDIC	10/10/2005	FIL 103-2005	FFIEC Guidance Authentication in an Internet Banking Environment	Spoof web sites	Yes	Yes
		FDIC	2/22/2006	FIL-18-2006	Fair Credit Reporting Act Revised Examination Procedures	Identity Theft		
		FDIC	1/10/2007	FIL-10-2007	Compliance Examination Handbook	Unfair Practice, FTC Act		

INFORMATION SECURITY GOVERNANCE FRAMEWORK (Basel II)						IP Governance	IP Governance	IT Governance
Matrix D1						Identity Theft Domain Names Suspicious Activity Reports (SARS) Spoofed Web Sites	Phishing	Pharming
C O D E	President's Identity Theft Task Force	Agency	Date	File	Information Security Governance; Regulatory Guidances; GLBA 501(b) FTC ACT Section 5			
O	PITTF	FDIC	4/11/2007	FIL-32-2007 (omits FDIC FIL-77-2000 and FIL 27-2004)	FDIC's Supervisory Policy on Identity Theft	Identity Theft	Yes	Yes
Omissions						Earlier FDIC Identity Theft Guidances involving bank domain names not cited in FIL-32-2007 include:		
		FDIC	11/08/00	FIL 77-2000	Protecting Internet Domains	Domain Name, SARS		
		FDIC	3/12/2004	FIL 27-2004	Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes	Domain Name, SARS	Yes	
Code:						Footnote #3, Page 84/90 of President's Identity Theft Task Force Committee, Volume II		
NR	Not Relevant for Corporate Identity Theft: GLBA 501(b)							
R	Relevant for Corporate Identity Theft: GLBA 501(b)							
O	Omitted but relevant for Corporate Identity Theft: GLBA 501(b)							
PITTF	President's Identity Theft Task Force							

Matrix D1 defines all relevant GLBA 501(b) supervisory guidances on safeguarding intellectual property for information security and consumer protection as of May 29, 2007. It includes:

- 15 **R**levant supervisory guidances from Footnote #3, Page 84/90 of President's Identity Theft Task Force Committee, Volume II.
- 15 **O**mitted but relevant supervisory guidances from Footnote #3, Page 84/90 of President's Identity Theft Task Force Committee, Volume II.
- Two relevant FDIC Financial Institution Letters on Corporate Identity Theft and Domain Names, i.e., FIL 77-2000 and 27-2004 that were not cited in the FDIC's FIL 32-2007, FDIC's Supervisory Policy on Identity Theft.

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Scenario Analysis for Operational Risks (Full Version)

Defining and understanding all the relevant regulations on information security governance and consumer protection regulations is an essential 1st step in the process to determine, validate and verify compliance with the same regulations – hence the need for Matrixes D and D1 and independent counsel.

Analyzing historical enforcement cases by the regulators and private sector lawsuits is the 2nd step in determining exposures to future litigation and/or regulatory fines due to non-compliance. Presented on the following page is Matrix D2. This is a summary of the historical enforcement cases by the FRB, FDIC, and OCC that were cited in the President's Identity Theft Task Force Report. It also includes relevant enforcement cases on BSA/AML civil money penalties, FDICIA Section 112 and phishing cases. The enforcement cases have been reviewed and allocated by type of enforcement action through these risk categories, i.e., Phishing Cases, Consumer Protection, Data Security Violations, Enterprise Risk Management and Information Security and IT Technology/Governance. The trend that emerges from this analysis is a clear set of major information security violations and operational/legal risks for financial firms that are defined in this Scenario Analysis on page 27.

A 3rd major driver for the Scenario Analysis is that the federal regulators have clearly stated in the President's Identity Theft Task Force Report on page 48 of 120 that beginning immediately, the regulators will initiate investigations of data security violations.



RECOMMENDATION: INITIATE INVESTIGATIONS OF DATA SECURITY VIOLATIONS

Beginning immediately, appropriate government agencies should initiate investigations of and, if appropriate, take enforcement actions against entities that violate the laws governing data security. The FTC, SEC, and federal bank regulatory agencies have used regulatory and enforcement efforts to require companies to maintain appropriate information safeguards under the law. Federal agencies should continue and expand these efforts to ensure that such entities use reasonable data security measures. Where appropriate, the agencies should share information about those enforcement actions on www.idtheft.gov.

The probability of current operational risks converting to operational losses is thus reasonably high in the coming year.

25	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

IP Governance Task Force Intellectual Property & Information Security Governance

Enforcement Cases Matrix D2		Penalties	Phishing Cases: Causing Substantial Injury to Consumers	Consumer Protection	Data Security Violations	ERM & IS Governance	IT Governance
<p>The President's Identity Theft Task Force Report, dated April 23, 2007, states in Volume II, Part B - Enforcement Actions Relating to Data Security that the FDIC took 17 formal enforcement actions between the beginning of 2002 and the end of 2006 that the FRB has taken 14 formal enforcement actions in the past five years that the OCC has taken 18 formal actions since 2002 that the OTS has taken 8 formal enforcement actions in the past five years.</p> <p>Many of these enforcement actions are cited below and are allocated by type of enforcement action. Additional enforcement cases involving BSA/AML and FDICIA Section 112 on Enterprise Risk Management Issues are also included included are the Phishing Cases by the FTC that are very relevant but were omitted from the President's Identity Theft Task Force Report.</p>							
FRB & FDIC	11/14/2001						BSA & Enterprise Risk Management
FRB & FDIC	7/13/2001	\$7,500,000					BSA & Enterprise Risk Management
FRB	12/19/2006	\$80,000,000					Enterprise Risk Management - Full compliance with all US Regulations
FRB	3/10/2004	\$13,000,000					Enterprise Risk Management - Full compliance with all US Regulations
FRB	8/11/2002						ERM & Information Security
FRB	2/24/2002						ERM & Information Security
FRB	5/14/2002						ERM & Information Security
FRB	3/4/2002						ERM & Information Security
FRB	3/27/2002						ERM & Information Security
FRB	11/18/2002						Information Security
FRB	10/21/2002						Information Security
FRB	8/29/2002						Information Security
FRB	4/24/2002						BSA & Information Technology
FRB	10/12/2004	\$70,000,000					BSA & Suspicious Activity Reports
FRB	8/22/2002						ERM & Information Technology
FRB	3/17/2002						ERM & Information Technology
FRB	5/29/2002						Information Technology
FRB	6/1/2002						Information Technology
FDIC	8/20/2002			Consumer Protection			
FDIC	1/17/2002			Consumer Protection			
FDIC	8/15/2002					501(b)	Information Security
FDIC	7/12/2002						Information Technology
FDIC	8/21/2002					501(b)	Information Security
FDIC	1/13/2002						Information Security
FDIC	1/13/2002					501(b)	Information Security
FDIC	1/13/2002					501(b)	Information Security
FDIC	11/19/2002						Information Security
FDIC	7/19/2002						Information Security
FDIC	11/14/2002					501(b)	Information Security
FDIC	1/23/2002						Information Security
FDIC	3/31/2002						Information Technology
FDIC	3/11/2002						Information Technology
FDIC	2/29/2002						Information Technology
FDIC	3/31/2002						Information Technology
FDIC	7/31/2002						Information Technology
FDIC	7/31/2002					501(b)	Information Technology
FDIC	9/23/2002						Information Technology
FDIC	1/11/2002						Information Technology
FDIC	2/22/2002						Information Technology
FDIC	5/11/2002					501(b)	Information Technology
FDIC	5/17/2002						Information Technology
FDIC	6/10/2002						Information Technology
FDIC	8/4/2002						Information Technology
FDIC	8/9/2002						Information Technology

Enforcement Cases Matrix D2		Penalties	Phishing Cases: Causing Substantial Injury to Consumers	Consumer Protection	Data Security Violations	ERM & IS Governance	IT Governance
FDIC	10/12/2002						Information Technology
FDIC	7/31/2002						Information Technology
FDIC	11/19/2002						Information Technology
FDIC	1/24/2002						Information Technology
FDIC	1/17/2002						Information Technology
FDIC	3/11/2002			Consumer Protection Laws			
FDIC	10/19/2002			Consumer Protection Laws			
FDIC	9/9/2002			Consumer Protection Laws			
FDIC	10/24/2002			Consumer Protection Laws			
FDIC	2/6/2002						Information Security
FDIC	2/22/2002						Information Security
FDIC	2/6/2002						Information Security
FDIC	11/19/2002						Information Security
FDIC	8/17/2002	\$50,000,000					BSA
FDIC	10/11/2002	\$4,000,000					BSA
FDIC	1/13/2002	\$5,100,000					BSA
FDIC	1/17/2002	\$10,000,000					Enterprise Risk Management
FDIC	7/27/2002						Information Technology
FDIC	2/22/2002						Information Technology
FDIC	7/27/2002						Information Technology
FDIC	8/29/2002						Information Technology
FTC	1/17/2002		Phishing		GLBA 501		Deceptive Prcticing of Financial Information by sending spam email and operating fraudulent web pages
FTC	7/17/2002		Phishing		Unfair Practice: Section 5(a) FTC ACT		Unfair Use of Consumer's Information Causing Substantial Injury to Consumers
FTC	1/25/2002		Phishing		Unfair Practice: Section 5(a) FTC ACT		Email Spoofing Causing Substantial Injury to Consumers
FTC	6/16/2002		Phishing		Deceptive Acts: Section 5(a) FTC ACT		False Claim of Need to Provide Information Deceptive Solicitation
FTC	8/19/2006		Privacy & Security Statement		GLBA 503; Unfair, deceptive act-Section 5(a) FTC ACT		False, Misleading Privacy & Security Statement
FTC	11/9/2004		Failed to Safeguard Web Site From Attack, etc		GLBA 501(b);		Failed to Safeguard Web Site From Attack, etc
FTC	12/14/2006		Failed to Provide Adequate Security		GLBA 501(b); Unfair, deceptive act-Section 5(a) FTC ACT		Failed to Provide Adequate Security

IP Governance Task Force Intellectual Property & Information Security Governance

Based on the foregoing trends from open-source databases, we repeat the earlier Scenario Analysis, i.e.,

Financial firms and their Boards of Directors are exposed to a range of 6 information security violations and operational/legal risks for their failure to:

1. safeguard material assets, i.e., trademarks which are defined as brands and domain names and trade secrets which is defined as customer identifying information, per their fiduciary responsibilities under FDICIA Section 112. See TJ Hooper Case and RSA Case in Matrix D as examples of fiduciary failures of non-financial firms to safeguard material assets. Parallel arguments can be made under FDICIA Section 112 on the failure of financial firms to safeguard their digital assets from federal crimes in this digital age, especially by applying the TJ Hooper case. "*T.J. Hooper* held that the "avoidance of negligence" requires adherence to existing standards of care; standards which change as technology evolves. The *T.J. Hooper* concept of evolving standards is still good law. Standards can ratchet up over time, as new innovations become accepted practice." Source: [Chris Gallagher](#). In 2007, the standards for information security and consumer protection laws are defined by the 11 classes of information security regulations in Matrix B.
2. comply with GLBA and the FTC ACT on safeguarding their brands and consumers from criminal acts and related federal crimes (Matrix B) per the supervisory guidances issued by the federal regulators under GLBA 501(b), GLBA 521, GLBA 523, and the FTC ACT on deceptive and unfair practices per Matrixes D and D1. See the GLBA enforcement cases by the regulators whereby Boards of Directors failed to fully apply GLBA in Matrix D2.
3. post accurate Privacy and Security Statements under GLBA 503 when they fail to safeguard their intellectual property per GLBA and then state, in a deceptive manner, that, "We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information." See Matrix D2 and *FTC v. Nations Title*; *FTC v. Nationwide Mortgage*; *FTC v. Superior Mortgage*.
4. report suspicious activity reports as required by law and as confirmed by the Department of Justice in its October, 2006 BiNational Report on Phishing. The DOJ states (1) financial firms are legally required to submit Suspicious Activity Reports on a crime affecting a financial institution (including phishing)³ and (2) "companies that are victimized by phishing may not report these instances to law enforcement. Unlike some other types of internet-based crime, such as hacking, that may be conducted surreptitiously, phishing, by its nature, involves public misuse of legitimate companies' and agencies' names and logos [*trademark infringements – our insertion*]. Nonetheless, some companies may be reluctant to report all such instances of phishing to law enforcement – in part because they are concerned that if the true volume of such

27	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

IP Governance Task Force
Intellectual Property & Information Security Governance

phishing attacks were made known to the public, their customers or accountholders would mistrust the companies or they would be placed at a competitive disadvantage.”⁴

5. report suspicious activity reports for one or more of the 6 relevant Identity Theft Operational Loss federal crimes (Matrix B) that include computer intrusions, consumer loan fraud, credit card fraud, mortgage loan fraud, terrorist funding (BSA/AML Examination Handbook defines identity theft⁵ as a form of terrorist funding) plus corporate identity theft (SARS Box 35u), i.e., infringing domain names in deceptive and unfair practices.
6. establish adequate internal controls per FDICIA Section 112 and COSO to prevent, detect and report criminal acts against bank assets to FINCEN and the Board of Directors. The risk profiles of the financial firms fined in BSA/AML civil money cases by FINCEN (Matrix D2) are similar in nature to the risk profiles of the financial firms that are failing to safeguard their intellectual property per GLBA and FTC ACT, i.e., lack of senior management involvement, lack of internal controls, lack of training, failure to report suspicious activity reports, and lack of a compliance officer for this class of risk.

Financial firms are also exposed to litigation risks from the private sector such as the recently filed class-action lawsuit, [Lamb V. TJX Companies and Fifth Third Bancorp.](#)

Having independent counsel provide current commentary and analysis on emerging litigation and regulatory fine trends is an essential part of verifying and validating current and future exposures to operational and/or legal risks on information security and consumer protection laws.

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Disclosure Risks on Information Security and Consumer Protection Regulations

GLBA 503: Qualitative Review of the Accuracy of Privacy and Security Statements

An independent, comparative analysis on:

- Operational Risk Exposures and Related Metrics for Information Security Governance and Consumer Protection Regulations per Matrixes B and B1 and IT Audit Ratings per FFIEC,
- Historical enforcement cases on Unfair and Deceptive Privacy and Security Statements issued under GLBA 503 as cited in Scenario Analysis Issue #3, and
- Privacy and Security Statements such as the:
 - current one, i.e., “We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.”
 - or the proposed one, i.e., “These measures include computer safeguards and secured files and buildings”,

enables an independent counsel to evaluate the holistic, enterprise risk management profile of a firm and either conclude a firm is in compliance or is not in compliance with the information security and consumer protection laws and thus determine whether the model privacy and security statement is accurate or false and misleading and thus subject to data security violations.

FDICIA Section 112: Qualitative review of compliance with fiduciary obligations to safeguard material assets and comply with federal regulations.

An independent, comparative analysis on:

- Operational Risk Exposures and Related Metrics for Information Security Governance and Consumer Protection Regulations per Matrixes B and B1 and IT Audit Ratings per FFIEC, and
- Historical enforcement cases on enterprise risk management cases per Matrix D2,

enables an independent counsel to evaluate the holistic, enterprise risk management profile of a firm and either conclude a firm is in compliance or is not in compliance with the enterprise risk management regulations information security and consumer protection laws.

Sarbanes-Oxley: Evaluating degrees of compliance and related operational risks and remediation budgets on information security and consumer protection laws merit disclosure, if these are materially negative and adverse, through Sarbanes-Oxley 409.

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Board of Directors – Enterprise Risk Management: Information Security Governance

INFORMATION SECURITY GOVERNANCE			NPRs Basel II Federal Register: February 28, 2007 “Model Privacy Form” Federal Register: March 29, 2007
INFORMATION SECURITY GOVERNANCE FRAMEWORK (Basel II)			
FDICIA SECTION 112			
IP Governance	IT Governance	Compliance Disclosures	
GLBA 501(b), 521, 523	GLBA 501(b)	GLBA 503	
IP Governance/IP Perimeter	IT Governance/IT Perimeter	The institution’s policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. FDICIA SECTION 112 SARBANES-OXLEY	
Trademark Infringements	Firewalls		
Corporate Identity Theft, Pretexting	Secure Socket Layers		
Domain Names (IP Asset Frauds)	Virus Protection		
Fake, Spoof Web Sites	Multi-Factor Authentication		
Sub-Domain Names	Virus Protection	FDICIA SECTION 112	
*Email-spam	Network Vulnerability	SARBANES-OXLEY FTC ACT (UDAP) Deceptive Practices	
**Phishing	Intrusion Detection		
FTC ACT (UDAP)	Remote Access		
*Deceptive Practices	Penetration Tests	FTC ACT (UDAP) Deceptive Practices	
**Unfair Practices	Pharming Risks		
IP Audit Metrics	IT Audit Metrics	Risk Tolerance Metrics	
Trade Secrets			
Customer Identifying Information			
Attempts to Acquire Consumer Identity Information	Attempts to Misuse Consumer Identity Information	Crime Completed Victim Harmed	
LIFE CYCLE OF IDENTITY THEFT			
President’s Identity Theft Task Force Report: idtheft.gov			

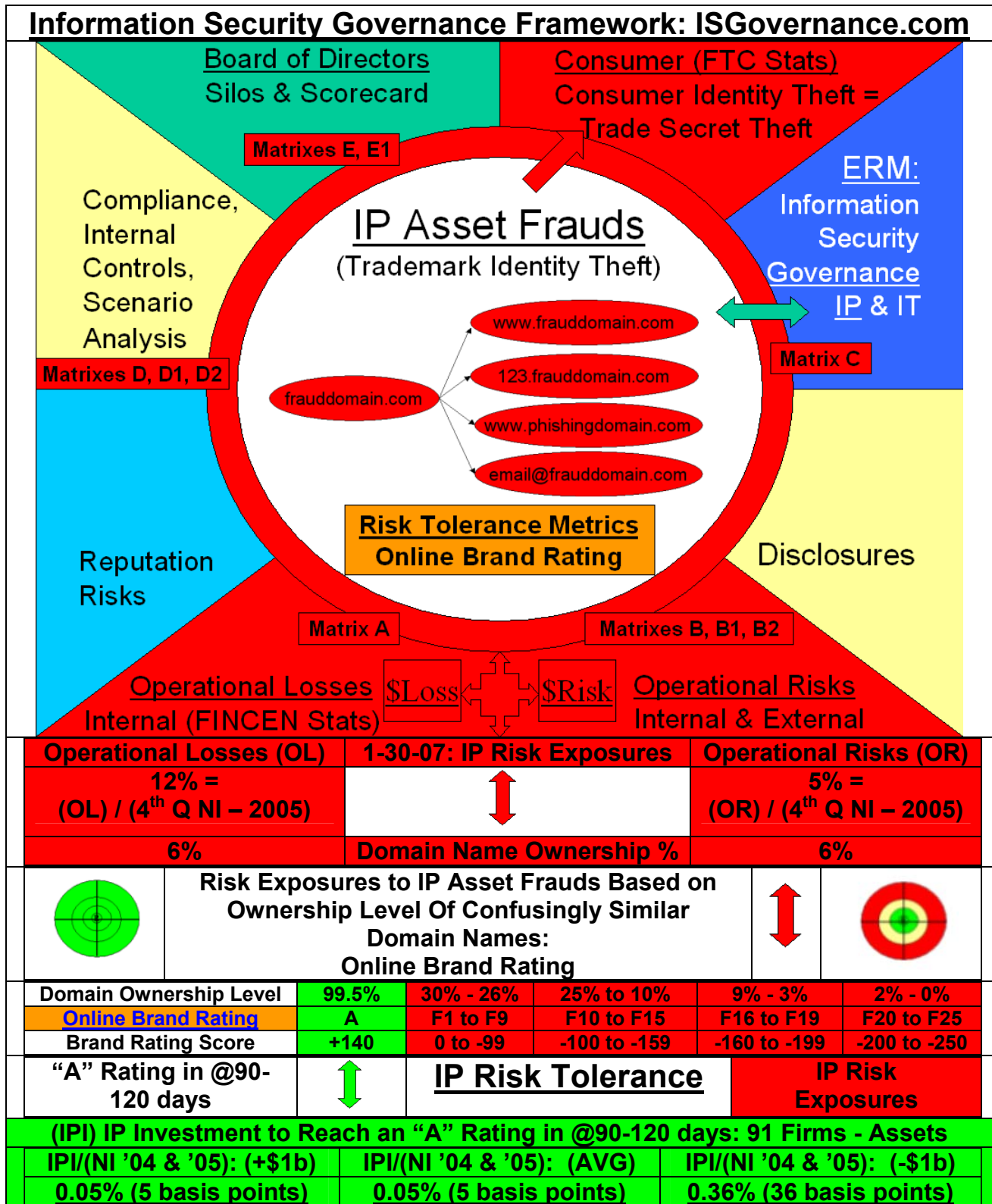
Unifying and integrating the foregoing components requires coordination between lead, independent counsel for architecting, validating and verifying current and ongoing operational risks on information security governance and internal auditors in capturing historical and ongoing operational loss events using, ideally a common Unit of Measure within the industry that equates to the average identity theft loss as reported by consumers to the FTC and as incurred by the bank. Consolidating this information into a quarterly Information Security Governance Scorecard (Matrix E1) for review by Boards of Directors overcomes inefficiencies now embedded in corporate silos and the current “IT Governance” paradigm (Matrix E) and enables a Board to:

1. analyze the allocation of relevant resources that include marketing and IT budgets.
2. analyze operational losses and operational risks.
3. establish Board-approved risk tolerance metrics and corresponding remediation budgets for IP Audit Metrics and IT Audit Metrics.
4. manage these metrics as required by Basel II based on quarterly progress reports.
5. disclose these metrics within the model Privacy Statement.

Page 31	Board of Directors: Information Security Governance Framework www.isgovernance.com	
32	Board of Directors: Information Security Silos	Matrix E
33	Board of Directors: Information Security Governance Scorecard	Matrix E1

30	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

**IP Governance Task Force
Intellectual Property & Information Security Governance**



IP Governance Task Force Intellectual Property & Information Security Governance

32	Board of Directors: Information Security Silos	Matrix E
----	--	----------

This maps current corporate silos on IP Governance, IT Governance, and consumer protection laws under the current industry paradigm for information security governance. It is a state of chaos that contributes to regulatory fatigue and non-compliance, which in turn enables federal crimes against bank assets.

Matrix E

Operational Risk Committee (See Matrix E1)		BOARD OF DIRECTORS - Matrix E		FIDUCIARY RISK: TJ HOOPER	
FFIEC-Management Resources					
COSO ERM: 2004		COSO - ENTERPRISE RISK MANAGEMENT		FRB SPEECH - ERM	
FRB NY: 2006		"Industry Sound Practices for Financial and Accounting Controls at Financial Institutions"		FRB Boston: 2004 FDICIA & COSO: ERM	
FDIC COMPLIANCE HANDBOOK		Extent of Board oversight/involvement in assuring compliance with consumer protection & fair lending laws & regulations.		Is the Board aware that it is ultimately responsible for the institution's compliance management system?	
FTC: IDENTITY THEFT		FTC CONGRESSIONAL TESTIMONY: DATA BREACHES AND IDENTITY THEFT (JUNE 16, 2006) <i>The FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.12</i> <i>The Commission has used this authority to challenge a variety of injurious practices that threaten data security.13</i> <i>13 These include, for example, unauthorized charges in connection with "phishing" e.g., See FTC v. Hill, FTC v. C.J.,</i>			
UDAP: "Unfair and Deceptive Practices"					
REGULATORY COMPLIANCE		INTELLECTUAL PROPERTY GOVERNANCE: OPERATIONAL RISK MANAGEMENT			
Annual Board Approval		PART 364—STANDARDS FOR SAFETY AND SOUNDNESS			
Information Security Governance (IS Governance) - Matrix C					
Basel		Identity Theft		Operational Losses	
Annual Board Approval		GLBA		Matrix A	
FEDERAL TRADE COMMISSION		GLBA 501(B) Security Guidelines (2001)		Operational Losses (BASEL)	
Fair and Accurate Credit Transactions Act ("FACT Act")		FFIEC's Information Security, Appendix C		REPUTATION RISK	
Section 111 "Identity theft" means a fraud committed using identifying information of another person		INFORMATION SECURITY [GLBA 501(B)]		INVESTOR RELATIONS	
FTC ACT UDAP		ENTERPRISE RISK MANAGEMENT		CONSUMER CONFIDENCE	
PRIVACY & CONSUMER PROTECTION		IP GOVERNANCE		Gartner: 2005	
ABUSIVE PRACTICES		IT GOVERNANCE		Gartner: 2006	
METRICS: INDUSTRY		Matrix D1		RATING AGENCIES	
IDENTITY THEFT BY STATE		SOX: Trademarks		FTC FINES: UDAP	
IP ASSET FRAUD RISK EXPOSURE		SOX: Trade Secrets		GLBA PHISHING	
Down-Stream Risks		IP AUDIT REPORT		EGMONT IDENTITY THEFT CASES	
GLOBAL RESOURCES		ONLINE BRAND RATING		QIS 04	
LAW ENFORCEMENT		IT AUDIT (FDIC)		FRB BOSTON	
OPERATIONAL RISKS		IT Audit Risk Scoring (1 to 5)		IDENTITY THEFT FINANCIAL FRAUD	
OPERATIONAL LOSSES		GLBA 501(B) Response Programs (2005)		FTC INTERNET FRAUD BY STATE	
		FDIC IT Ex. Handbook		IDENTITY THEFT BY STATE	
		Operational Losses (Matrix A)		FTC IDENTITY THEFT BY STATE	
		IDENTITY THEFT		CONSUMER IDENTITY THEFT ATTACKS	
		Computer Intrusion		PROTECTING CONSUMERS ONLINE	
		IP ASSET FRAUD		IDENTITY THEFT TERRORISM FUNDING SOURCE	
		ONLINE BRAND RATING		BRAND MARKING	
		Down-Stream Risks		DATA PROTECT	
		MESSAGE LABS		REG 2006A	
		ANTI-PHISHING WORKING GROUP		IDENTITY THEFT TERRORISM FUNDING SOURCE	
		MCAFFEE- PHISHING		CONSUMER IDENTITY THEFT ATTACKS	
		CERT ALERTS		OPERATIONAL RISKS	
		5% of 4th Q NI, '05		OPERATIONAL LOSSES	
		12% of 4th Q NI, '05		5% of 4th Q NI, '05	
		12% of 4th Q NI, '05		12% of 4th Q NI, '05	
MATRIX E: IP Governance: Operational Risk Management © Copyright 2007 by IP Governance Task Force. All Rights Protected					

32	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

IP Governance Task Force Intellectual Property & Information Security Governance

33	Board of Directors: Information Security Governance Scorecard	Matrix E1
----	---	-----------

Consolidating the foregoing information into a quarterly Information Security Governance Scorecard (Matrix E1) for review by a Board of Directors overcomes inefficiencies now embedded in corporate silos and the current "IT Governance" paradigm (Matrix E) and enables a Board to:

1. analyze the allocation of relevant resources that include marketing and IT budgets.
2. analyze operational losses and operational risks.
3. establish Board-approved risk tolerance metrics and corresponding remediation budgets for:
 - a. IT Ratings from the FFIEC.
 - b. IP Ratings such as the Online Brand Rating model for brand/domain name risk levels.
4. manage these metrics as required by Basel II based on quarterly progress reports.
5. disclose the metrics within the model Privacy Statement, "we use security measures that comply with federal law," so consumers can easily assess degrees of compliance.

Information Security Governance Scorecard- Matrix E1		BOARD OF DIRECTORS			Budget
Information Security Governance (Matrix C)		Information Security Governance			
Identity Theft		IP GOVERNANCE		IT GOVERNANCE	
Reputation Risk		TRADE SECRETS	TRADEMARKS		
FDIC COMPLIANCE HANDBOOK	Extent of Board oversight/involvement in assuring compliance with consumer protection & fair lending laws & regulations.	Customer Identifying Information	IP ASSET FRAUDS Domains => fake web sites, email		
Information Security Governance (Matrix C)		IP PERIMETER		IT PERIMETER	
Risk Management		At Risk	At Risk		
Risk Monitoring		At Risk	At Risk		
Risk Control		At Risk	At Risk		
Risk Remediation		See Basel	See Basel		
Risk Reporting		At Risk	At Risk		
Risk Rating/Tolerance: Board Approval (\$5)		Online Brand Rating		IT Ratings	
Disclosure Policies		At Risk	At Risk		
PART 384—STANDARDS FOR SAFETY AND SOUNDNESS		DISCLOSURES	DISCLOSURES	DISCLOSURES	
FDICIA Section 11P - Section 38 Appendix A to Part 383—Guidelines and Interpretations Annual Reporting Requirements (6.363.2) 1. 8. Management Report. 9. Safeguarding of Assets. 10. Standards for Internal Controls. 12. Compliance with Laws and Regulations. GLBA Safeguards Rule: 501(b); 521; 523 GLBA Privacy: 503 FTC's UDAP (Section 5a): Deceptive & Unfair Practices Submission of Suspicious Activity Reports		Annual Board Approval			
		Matrixes D, D1, E	Matrixes D, D1, E		
		Matrixes D, D1, E	Matrixes D, D1, E		
		Matrixes D, D1, E	Matrixes D, D1, E		
		Matrixes D, D1, E	Matrixes D, D1, E	Matrixes D, D1, E	
		See Below	See Below		
		See Below	See Below		
		Not in Compliance	Not in Compliance		
		Not in Compliance	Not in Compliance		
		Annual Board Approval			
		Misleading, Unfair	Unfair Practice		
		Misleading Practice	Misleading Practice		
		Quarterly	Quarterly		
		Pillar 3	Pillar 3		
Economics (91 Financial Firms)					
Marketing Budget: 2004-2005		\$1,869,625,674		\$1,869,625,674	
IT Budget		\$		\$	
IP Investment (Domain Name Registrations): 2004-2005		\$39,610		\$39,610	
Operational Losses		Matrix A	Matrix A	12% of 4th Q NI '05	
Operational Risks		Matrix B	Matrix B	5% of 4th Q NI '05	
Current Ratings		"F" Online Brand Rating		IT Ratings	
Target Ratings		"A" Online Brand Rating		IT Ratings	
Risk Remediation: IP Investment (IPI)		.36% to .05% of NI, '04 & '05			
Risk Remediation (IPI)/Marketing Budget 2004-2005		.46% to 3.71% of Marketing Budget, '04 & '05			
© Copyright 2007 IP Governance Task Force					

33	IP Governance Task Force 5100 Tamiami Trail North – Suite 105, Naples, Florida 34103 t-239-777-4638 – f-239-643-3996 www.ipgovernance.com – info@ipgovernance.com	© Copyright 2007-2005 All Rights Reserved.
----	---	---

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Comparative Review and Conclusion:

A comparative review of our Information Security Governance, Compliance and Metrics Model for Basel II with the [2006 Guidance for Board of Directors and Executive Management, 2nd Edition, Information Security Governance](#) by the IT Governance Institute reveals our model complements their model by measuring enterprise-wide regulatory compliance with information security and consumer protection laws for financial firms with a special concentration on intellectual property operational risks and operational losses.

We appreciate the opportunity to provide commentary on the two NPR's and will be pleased to answer any questions arising from our analysis and recommendations for unifying and creating an enterprise risk management model for Information Security Governance per Basel II for financial firms of all sizes, globally.

Beckwith B. Miller, President
IP Governance Task Force
5100 Tamiami Trail North
Naples, Florida 34103
239.777.4638
miller@ipgovernance.com

Paul W. Kruse, Esq.
Bone, McAllester Norton PLLC
511 Union Street - Suite 1600
Nashville, Tennessee 37219
615.238.6300
pkruse@bonelaw.com

Patrick J. Whalen, Esq.
Spencer, Fane, Britt & Browne, LLP
1000 Walnut Street, Suite 1400
Kansas City, MO 64106-2140
816.292.8237
pwhalen@spencerfane.com

**IP Governance Task Force
Intellectual Property & Information Security Governance**

Footnotes:

¹ GLBA

[Section 501 of the GLB Act, 15 U.S.C. § 6801](#), whereby financial institutions are to implement administrative, technical, and physical safeguards -

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

[Section 521 of the GLB Act, 15 U.S.C. § 6821](#), Privacy protection for customer information of financial institutions

(a) Prohibition on obtaining customer information by false pretenses. It shall be a violation of this subchapter for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person -

- (1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution;
- (2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution; or
- (3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.

(b) Prohibition on solicitation of a person to obtain customer information from financial institution under false pretenses

[Section 523 of the Gramm-Leach-Bliley Act \(15 U.S.C. 6823\)](#) makes it a crime to obtain customer information of a financial institution by means of false or fraudulent statements to an officer, employee, agent or customer of a financial institution. Section 523 of the Gramm-Leach-Bliley Act also makes it a crime to request another person to obtain customer information of a financial institution, if the requester knows that the information will be obtained by making a false or fraudulent statement. (Source: FRB [SR 01-11](#))

² FTC enforcement cases involving phishing: [FTC vs. GM Funding](#); [FTC v CJ](#); [FTC v. Zachary Keith Hill](#)

³ [Department of Justice's BiNational Report](#), page 15.

⁴ [Department of Justice's BiNational Report](#), page 6.

⁵ [BSA/AML Examination Manual](#), 2006, page 12 of 367.