

The Industry Need for Risk Calculation Models

Catherine A. Allen

CEO

BITS

The Data Governance Risk Calculation Forum

NYU Stern School of Business

New York, NY

October 31, 2006

© BITS 2006.



Why the Need for Risk Calculation Models

- Demand from boards of directors and senior executives for better tools
- Increase in fraud and security breaches
- Growth of cross-channel payments risk
- Sophistication of “bad guys” requires enterprise perspective
- Impact on cost savings and efficiencies

Audit Committee Leadership Network in North America Recommendations

- **Boards should focus on three key information technology (IT) related risks**
 - Compliance and control risks (Section 404)
 - Business continuity risks
 - Security and privacy risks
- **Add technology expertise to boards via membership, advisory boards or special committees**
- **IT risk oversight should be at the board or audit committee level**
- **Develop appropriate enterprise wide risk management policies, procedures and controls**

What Is the Financial Services Industry Doing?

- **Realigning business silos and increasing communications across them**
- **Introducing enterprise risk management policies and procedures**
- **Exploring risk calculation tools**
- **Creating shared data bases and broader information sharing opportunities**
- **Working with others in the industry**
- **Working more closely with law enforcement**

Unintended Consequences

- **Class action lawsuits**
- **New rules of evidence requirements**
- **End-to-end customer protection**
- **Customer ownership of data**

A Bit About BITS

- **Technology and business strategy group of 100 of the largest U.S. financial institutions**
- **Focuses on emerging technologies, business strategies, and risk management**
- **Works with members, critical infrastructure sectors, government organizations, technology providers, and other industry associations to accomplish its goals**

Market Forces that Drive FIs

- Security breaches and related incidents that run the risk of eroding public confidence
- Rapid growth of ID theft and fraud, including international crime rings
- Concerns about terrorism, interdependencies of critical infrastructures and business continuity
- Concerns related to software and data vulnerabilities
- Changes due to electronification and intermediaries
- Increasing needs for regulatory efficiencies
- Concerns about security, privacy and business continuity practices of third party service providers
- Rapid development/deployment of new technologies
- Maintaining and transitioning legacy systems

BITS Core Initiatives for 2006

■ Security and Risk Assessment

- Enterprise Risk Management
- Data Transport Security
- Software Security
- Management of IT Service Provider Relationships
- Financial Institution Shared Assessments Program

■ Fraud Reduction

- Rising Fraud Risks
- Shared Data Bases
- Successful Strategies

■ Industry Coordination

- CEO Payments Council Focus on Cross Channel Risk
- Crisis Management Coordination

Examples of BITS Deliverables

- BITS Key Considerations for Securing Data in Storage and Transport
- BITS Internal Fraud DataBase
- BITS Calculator: Key Risk Measurement Tool for Information Security Operational Risk
- BITS Patch Management Best Practices
- BITS Fraud Protection Toolkit: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation
- BITS Consumer Confidence Toolkit: Data Security and Financial Services
- Voluntary Guidelines for Consumer Confidence in Online Financial Services
- BITS Critical Success Factors for Security Awareness & Training Programs
- BITS/FSR Identity Theft Assistance Center (ITAC)

Examples of BITS Deliverables, cont.

- ChicagoFIRST (with partner organizations)
- Financial Institution Shared Assessments Program
- BITS Guide to Business-Critical Telecommunications Services
- BITS Product Certification Program
- BITS Payments Roadmap
- Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy
- BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Framework)
- BITS IT Service Providers Expectations Matrix
- BITS Phishing Prevention and Investigation Network (hosted at the FS/ISAC)
- E-Scams White Paper Series

Statistics on Fraud and Security— The Current Environment

- As many as one in five customers leave an institution following a data security breach, while another 40 percent consider cutting their ties. (*Ponemon Institute Study*)
- In 2005, the FBI's IC3 processed more than 228,400 different fraud types that involved a financial loss on the part of the complainant.
 - The total dollar loss from all referred cases of fraud was \$183 million - a \$68 million increase in total losses in 2004.

Statistics on Fraud and Security— The Current Environment

- The number of phishing sites rose to 14,191 in July 2006, an 18 percent increase over May 2006. (*Anti Phishing Working Group*)
 - 9 out of 10 phishing sites are aimed at the financial services sector.
 - In July 2006, fraudulent sites mimicked 154 brands – a 20% increase from June 2006.
 - Online criminals are also targeting smaller FIs, ISPs and government agencies.
 - Technical sophistication of phishing attacks is also increasing.

Statistics on Fraud and Security— The Current Environment, cont.

- 60% of companies never encrypt data backed up to tape regardless of high-profile events involving the loss of tapes or disks. (*Enterprise Strategy Group*)
- U.S. companies lose an estimated 5% (\$652B) of annual revenues to employee fraud. (*ACFE*)
- 70% of employee theft is committed by employees who have been with the company for less than 30 days. (*Unicru Inc.*)
- Average fraud scheme lasts 18 months before being identified, reducing the opportunity to recover funds. (*Bankers Ideanet*)
- Only 8% of internal fraud perpetrators had prior convictions. (*ACFE*)

Operational Risk

- Defined by the Basel Committee on Banking Supervision as the potential for “risk or direct or indirect loss resulting from inadequate or failed internal processes, people, and systems.”

Growing Concern About Operational Risk

- **Perceived increase in risk**
 - Growing reliance on technology to support operations
 - Expanding market bases including growth in the international sector
- **Reaction to major loss events**
 - Accounting scandals
 - Rogue trading incidents
- **Regulatory imperative**
 - New Basel Accord and pending U.S. capital regulations
 - Increased scrutiny and expectation for the management of operational risk

Operational Risk Working Group

■ Goals:

- Information exchange around enterprise-level operational risk challenges
- Development of resources and tools to help financial institutions address OpRisk issues in terms of risk management and regulatory compliance

Operational Risk Working Group Initiatives

- Reconciliation of Regulatory Overlap Study
- The Calculator- Key Risk Measurement Tool for Information Security Operational Risks
- Key Risk Indicator Guidance

Operational Risk Working Group Deliverables

■ Reconciliation of Regulatory Overlap Study goals:

- Identify areas of duplication or discord among key pieces of regulation pertaining to operational risk
 - Sarbanes Oxley Act of 2002 (Sarbox)
 - Gramm-Leach Bliley Act of 1999 (GLBA)
 - Federal Deposit Insurance Company Improvement Act of 1991 (FDICIA)
 - Proposed Basel II Capital Accord
- Establish methods of eliminating redundancies and streamlining the compliance process

Operational Risk Working Group Deliverables, cont.

- **Reconciliation of Regulatory Overlap Study**
 - White paper and matrices detailing regulatory overlap among key operational risk regulations
 - Presented to the regulatory community
 - Available online at www.BITSinfo.org

Operational Risk Working Group Deliverables, cont.

- **The Calculator - Key Risk Measurement Tool for Information Security Operational Risks**
- **Goals:**
 - Allows institutions to measure and prioritize information security risks
 - Supports the institution's enterprise wide risk assessment and mitigation efforts

Operational Risk Working Group Deliverables, cont.

■ The Calculator

- Narrative
 - Background and instructions
- Spreadsheet tool
 - Lists common information security threats, vulnerabilities and controls for risk mitigation
 - For use across the enterprise (audit, information security, operational risk, etc.)
 - Scores and prioritizes threats

■ Available online at www.BITSinfo.org

Operational Risk Working Group Deliverables, cont.

- **Key Risk Indicators (KRI) subcommittee goals:**
 - Identify and document current practices for establishing and using KRIs
 - Develop best practices for a process to identify leading KRIs
 - Determine means of quantifying and weighing individual KRIs
 - Consider building a library of leading KRIs

Operational Risk Working Group Deliverables, cont.

- **Developing a KRI Program: Guidance for the Operational Risk Manager**
 - Available online at www.BITSinfo.org

Fraud-Related Shared Data Bases

■ National Shared Account Data Base

- Encouraged members to participate in legacy PPS data base that now includes 213 million + accounts

■ Phishing Prevention and Investigation Network

- Created to share phishing attack information, house contact information necessary for shutting down sites, and develop and show trend analysis that will aid in shutting down fraud rings
- Developed by BITS eScams Subcommittee
- Hosted by the FS/ISAC

Fraud-Related Shared Data Bases, cont.

■ Internal Fraud Prevention Service

- Database of former financial services employees released for cause due to fraudulent acts committed against financial institutions
- Developed by BITS Shared Data Base Working Group
- Hosted by Early Warning Services, LLC

Identity Theft Assistance Center (ITAC): Data Sharing Agreements

- Data sharing agreements provide weekly feeds of identity theft case data to:
 - Federal Trade Commission
 - Consumer Sentinel Data Base and accessed by 1,400 local, state and federal law enforcement agencies around the country
 - US Postal Inspection Service
 - Financial crimes data base is used by postal inspectors all over the U. S.

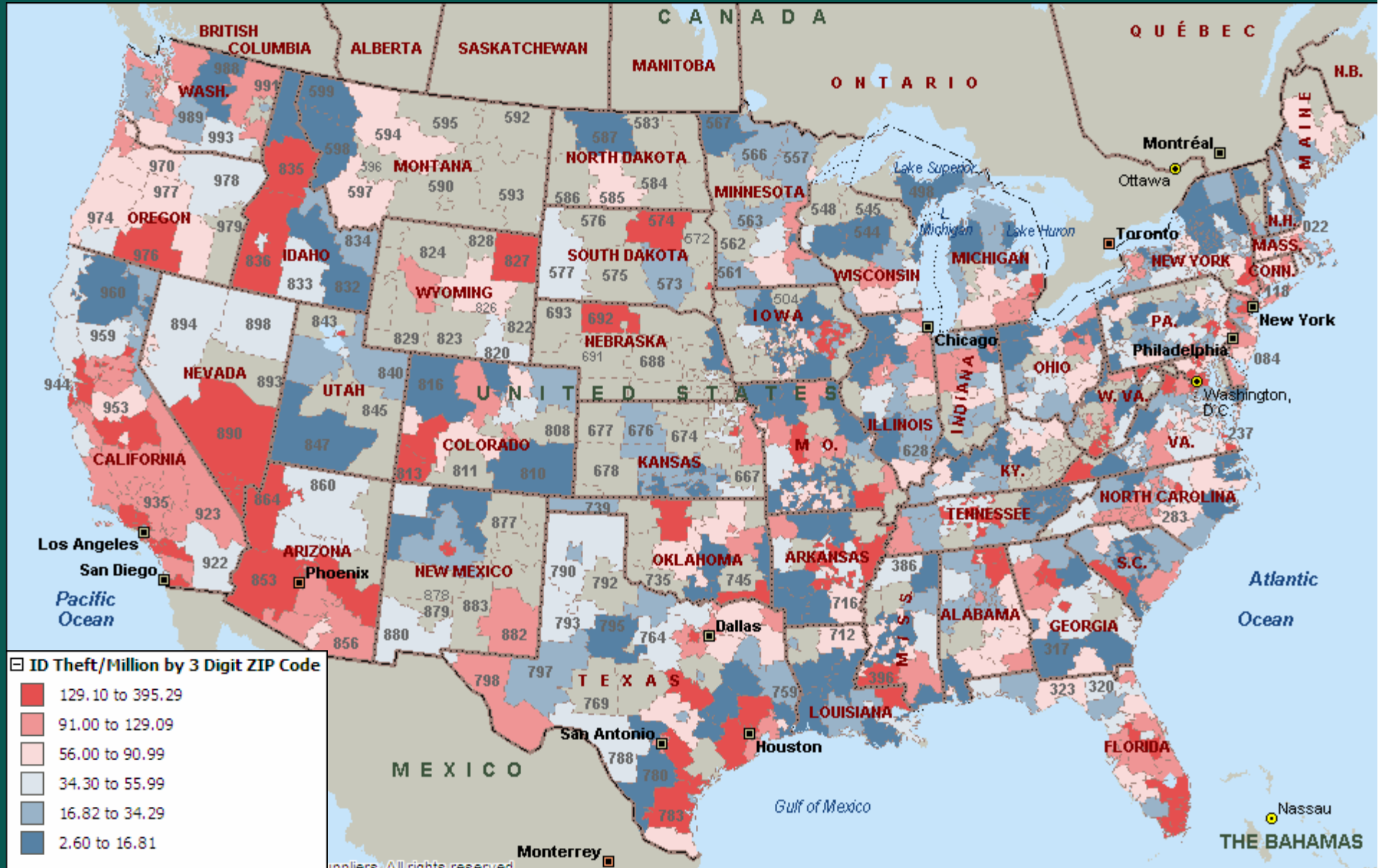
Identity Theft Assistance Center (ITAC): Data Analysis

- Analysis of 10,000 cases in ITAC data base allows member companies and law enforcement to identify trends and patterns
- High quality data
 - Victim's identity and facts of case verified by ITAC member
 - National in scope
 - Cases from 20+ companies
 - Credit card, debit card, loan and investment lines of business

Perpetrator Locations



Cases by 3 Digit Zip per Million People



Security Context for FIs

- **Economic and national security relies on the security, reliability, recoverability, continuity, and maintenance of information systems.**
- **IT security has a direct and profound impact on the government and private sectors, on the nation's critical infrastructure, and on international economies.**
- **Security is fundamental—a first priority for the financial services industry.**

Security Context for FIs, cont.

- Security breaches, loss of data and related incidents affect the public's perspective and run the risk of eroding public confidence.
- Arguably, the financial services industry is ahead of other sectors in its robust risk management systems.
- FIs depend on the safety and soundness of other critical infrastructure sectors including software providers, ISPs, telecoms, and power.
- Financial services is a highly regulated industry with increasingly complex compliance standards.

Data Security and Outsourcing Regulatory Requirements for FIs

- **Gramm-Leach-Bliley Act (GLBA) and implementing regulations:**
 - Specifies elements of a risk-based, comprehensive information security program
 - Requires FIs to notify customers in response to a security breach if there is risk of harm to the consumer
 - Requires robust oversight of third party service providers
- **Sarbanes-Oxley Act**
- **Basel II**

Data Security and Outsourcing Regulatory Requirements, cont.

- FFIEC booklets covering all aspects of information technology and detailed examination procedures
- FRB/OCC/SEC's "Sound Practices" Paper outlining business continuity requirements (in a post 9/11 environment)

What US Financial Regulators Do

- Supervise and examine financial institutions and major service providers on an ongoing basis.
- Promulgate regulations and supervisory guidance jointly thru the Federal Financial Institutions Examination Council (FFIEC).
 - FFIEC is formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the FRB, FDIC, NCUA, OCC, and OTS and to make recommendations to promote uniformity in the supervision of financial institutions.
- Enforce regulations and guidance.

Public and Private Sector Innovation and Leadership Are Needed

■ Recommendations for financial services sector:

- Approach information security issues on an end-to-end and enterprise-wide basis, including all relationships with third party service providers.
- Recognize the dependence of all critical infrastructures on software operating systems and the Internet.
- Maintain rapid, reliable and diverse communications.
- Encourage collaboration and coordination among and across sectors and government agencies to assure the security and reliability of all critical financial services infrastructures.
- Apply industry best practices.

Public and Private Sector Innovation and Leadership Are Needed

■ Recommendations for other sectors and government:

- Encourage providers of software to the financial services industry to accept responsibility for the role their products and services play in supporting the nation's and the world's critical infrastructure.
- Establish improved coordination procedures across all critical infrastructures and with international bodies as well as federal, state, and local government when events occur.
- Encourage law enforcement to prosecute cyber criminals and identity thieves on a world-wide basis, and publicize efforts to do so.
- Reduce regulatory redundancy and increase efficiencies among the appropriate US regulatory agencies and harmonization of or international regulations.

For More Information:
BITS@fsround.org; Tel. (202) 289-4322
www.BITSinfo.org

BITS Staff Contacts

Catherine A. Allen, CEO, cathy@fsround.org

Tanya Bailey, Senior Director Meetings, tanya@fsround.org

Wattie Bennett, Executive Assistant, wattie@fsround.org

John Carlson, Senior Director, john@fsround.org

Cheryl Charles, Senior Director, cheryl@fsround.org

George Forsberg, Controller, george@fsround.org

John Ingold, Director, johni@fsround.org

Carrie Neckorcuk, Director of Human Resources and Administrative
Affairs, carrie@fsround.org

Ann Patterson, Director, ann@fsround.org

Matt Ribe, Project Manager, matt@fsround.org

Gary Roboff, Senior Consultant, gary@fsround.org

Heather Wyson, Director, heather@fsround.org

Appendix

BITS Committee

Chair:

William A. Osborn

Chairman and CEO

Northern Trust Corporation

Thomas A. Renyi

Chairman and CEO

The Bank of New York Company, Inc.

David C. Weinstein

Chief of Administration

Fidelity Investments

James E. Rohr

Chairman and CEO

The PNC Financial Services Group, Inc.

Carl E. Jones

President and CEO

Regions Financial Corporation

Edward B. Rust, Jr.

Chairman and CEO

State Farm Insurance Companies

James H. Blanchard

Chief Executive Officer

Synovus

Richard M. Kovacevich

Chairman and CEO

Wells Fargo & Company

BITS Advisory Board

Doug Smith	Corporate Information Security Executive	Bank of America Corporation
Donald Monks	Vice Chairman of the Bank	The Bank of New York Company, Inc.
Harvey Koepfel	Chief Information Officer	Citigroup, Inc.
John R. Beran	Executive Vice President & CIO	Comerica Bancshares, Inc.
Jon Aliber	Executive Vice President	Jon Aliber
Susan J. Webb	Executive Vice President	JPMorgan Chase & Co.
Louis Rosenthal	Executive Vice President	LaSalle Bank Corporation
Susan Vismor	Senior Vice President	Mellon Financial Corporation
Diane L. Schueneman	Senior Vice President	Merrill Lynch & Co., Inc.
Timothy J. Theriault	President, Business Unit Head of Worldwide Operations	Northern Trust Corporation
Timothy G. Shack	Senior Vice President & CIO	The PNC Financial Services Group, Inc.
Barbara Koster	Senior Vice President & CIO	Prudential Financial, Inc.
John R. Dick	Chief Information Officer	Regions Financial Corporation
Sharon Tarvin	Assistant Vice President	State Farm Insurance Companies
Lisa L. White	E-Commerce Executive	Synovus
William L. Chenevich	Vice Chairman	U.S. Bancorp
Gerald A. Enos, Jr.	Sr. Executive Vice President	Wachovia Corporation
Kevin Dabney	Executive Vice President	Wells Fargo & Company

Roundtable/BITS Members

- ACE INA Holdings, Inc.
- AEGON USA, Inc.
- Affiliated Managers Group, Inc.
- Allianz Life Insurance Company of North America
- Allied Capital Corporation
- The Allstate Corporation
- American Express Company
- American International Group, Inc.
- AmSouth Bancorporation
- Aon Corporation
- Associated Banc-Corp
- Assurant, Inc.
- AXA Financial, Inc.
- BancorpSouth, Inc.
- BancWest Corporation
- Bank of America Corporation
- Bank of Hawaii Corporation
- The Bank of New York Company, Inc.
- Barclays Capital, Inc.
- BB&T Corporation
- Capital One Financial Corporation
- The Charles Schwab Corporation
- The Chubb Corporation
- Citigroup Inc.
- Citizens Financial Group, Inc.

Roundtable/BITS Members, cont.

- City National Corporation
- Comerica Incorporated
- Commerce Bancshares, Inc.
- Compass Bancshares, Inc.
- Countrywide Financial Corporation
- Cullen/Frost Bankers, Inc.
- Edward Jones
- Federated Investors, Inc.
- Fidelity Investments
- Fifth Third Bancorp
- First Commonwealth Financial Corporation
- First Horizon National Corporation
- Ford Motor Credit Company
- Fulton Financial Corporation
- General Electric Company
- Genworth Financial
- GMAC Financial Services
- Guaranty Financial Services
- H&R Block, Inc.
- Harris Bankcorp, Inc.
- HSBC North America Holdings, Inc.
- Huntington Bancshares Incorporated
- ING
- John Deere Credit Company
- John Hancock Financial Services

Roundtable/BITS Members, cont.

- JPMorgan Chase & Co.
- KeyCorp
- LaSalle Bank Corporation
- Legg Mason, Inc.
- Lincoln National Corporation
- M&T Bank Corporation
- Marshall & Ilsley Corporation
- MassMutual Financial Group
- MasterCard International
- Mellon Financial Corporation
- Mercantile Bankshares Corporation
- Merrill Lynch & Co., Inc.
- National City Corporation
- Nationwide
- New Century Financial Corporation
- Northern Trust Corporation
- The PNC Financial Services Group, Inc.
- Popular, Inc.
- Principal Financial Group
- Protective Life Corporation
- Prudential Financial, Inc.
- Raymond James Financial, Inc.
- RBC Centura Banks, Inc.
- Regions Financial Corporation
- Sky Financial Group, Inc.

Roundtable/BITS Members, cont.

- Sovereign Bancorp, Inc.
- State Farm Insurance Companies
- State Street Corporation
- SunTrust Banks, Inc.
- Synovus
- TD Banknorth, Inc.
- TIAA-CREF
- Toyota Motor Credit Corporation
- UBS
- UnionBanCal Corporation
- United Bankshares, Inc.
- UnumProvident Corporation
- U.S. Bancorp
- USAA
- Wachovia Corporation
- Waddell & Reed Financial, Inc.
- Washington Mutual, Inc.
- Wells Fargo & Company
- Western & Southern Financial Group
- Whitney Holding Corporation
- Zions Bancorporation
- Zurich Financial Services

BITS Affiliate Members

- **American Bankers Association (ABA)**
- **Association for Payment Clearing Services (APACS)**
- **Canadian Bankers Association (CBA)**
- **Canadian Payments Association (CPA)**
- **Chevy Chase Bank**
- **The Clearing House**
- **Credit Union National Association (CUNA)**
- **The Depository Trust & Clearing Corporation (DTCC)**
- **Financial Services Technology Consortium (FSTC)**
- **Independent Community Bankers of America (ICBA)**
- **NetBank, Inc.**