

BITS

FINANCIAL SERVICES
R O U N D T A B L E

**BITS VOLUNTARY GUIDELINES
FOR
AGGREGATION SERVICES**

JANUARY 2004

A PUBLICATION OF THE BITS AGGREGATION SERVICES WORKING GROUP

BITS
1001 PENNSYLVANIA AVENUE NW, SUITE 500 SOUTH
WASHINGTON, DC 20004
(202) 289-4322 WWW.BITSINFO.ORG

BITS VOLUNTARY GUIDELINES FOR AGGREGATION SERVICES

TABLE OF CONTENTS

THE BITS AGGREGATION SERVICES WORKING GROUP	3
ABOUT BITS	5
I. INTRODUCTION	
A. Background	6
B. Aggregation Services Today.....	6
C. The BITS Aggregation Services Working Group	7
D. How the Guidelines Were Developed	7
E. For Additional Information.....	8
II. SECURITY, TECHNOLOGY AND STANDARDS	9
A. Overview.....	9
B. Security Guidelines for Trusted Aggregation Services	9
III. GUIDELINES FOR AGGREGATION AUTHENTICATION AND DATA FEEDS	20
A. Overview.....	20
B. System-Level Guidelines	21
C. Authentication Solutions.....	21
D. Data-Feed Solutions.....	22
E. Use-Case Level Guidelines	23
IV. CUSTOMER EDUCATION	25
A. Overview.....	25
B. Assumptions.....	25
C. Guidelines and Recommendations.....	25
D. Consumer Tips.....	29
E. Security Tips for Online Financial Services Accounts.....	31
V. LEGAL AND REGULATORY FRAMEWORK	32
A. Overview.....	32
B. Matrix	32
VI. AGGREGATION AND SECURITY GUIDELINES	39
A. Overview.....	39
B. Security of Certain Customer Data.....	39
C. Security Guidelines.....	39
D. Security Requirements and Other Financial and Non-Financial Regulators	40
VII. PRIVACY AND INFORMATION USE	42
A. Overview.....	42
B. Assumptions.....	42
C. Guidelines	42
VIII. LONGER-TERM SOLUTIONS FOR AGGREGATION SERVICES AUTHENTICATION	45
A. Overview.....	45
B. Solutions	45
APPENDIX I INDUSTRY ENCRYPTION STANDARDS	50
APPENDIX II BANKING AND BROKERAGE ACCOUNT HOLDINGS SUPPORTED BY AGGREGATION	51
APPENDIX III GLOSSARY OF TERMS	53

THE BITS AGGREGATION SERVICES WORKING GROUP

CHAIR: Gayle Wellborn, Bank of America Corporation

SUBGROUPS

- **Security, Technology and Standards**, Co-Chaired by Roger Callahan, Bank of America Corporation, and Dan Schutzer, Citigroup Inc.
- **Customer Education**, Chaired by Gayle Wellborn, Bank of America Corporation
- **Legal and Regulatory Framework/Privacy and Information Use**, Chaired by Brad Ipema, Wachovia Corporation

CHARTER

The BITS Aggregation Services Working Group seeks to identify and implement industry actions to enable safe, secure, private and efficient aggregation services for consumers.

STRATEGIC GOALS

- Work with regulators, aggregators and other industry groups to develop an industry approach for financial aggregation services;
- Assess and recommend privacy and security criteria for aggregation software and services; and
- Educate consumers on risks and advantages of aggregation services.

SHORT-TERM OBJECTIVES

- Minimize the risks associated with “screen scraping”:
 - Authentication/authorization process
 - Data feed/data collection
 - Customer education
 - Minimum security requirements
 - Business practices
- Identify and assess relevant laws and regulations

LONG-TERM OBJECTIVES

- Facilitate the development of a more robust aggregation infrastructure that includes the necessary features for authorizing and auditing fund transfers while simultaneously addressing safety and soundness, privacy, and efficiency issues.
- Include the following issues:
 - Identification and authentication (to validate customers, financial institutions, and bill presenters)
 - Authorization (de-authorization)
 - Validating and tracing transaction requests
 - Audit and non-repudiation
 - Corrections process
 - Efficient data-feed model
 - Liability resolution
 - Appropriate business rules
- Encourage pilot efforts to validate and refine feature specifications.

PARTICIPATING ORGANIZATIONS

Access My Money
Access Softek, Inc.
AeroBank.com
American Bankers Association
Bank of America Corporation
The Bank of New York Company, Inc.
Bank of Tokyo-Mitsubishi Trust Company
BANK ONE CORPORATION
BB&T Corporation
Business Logic
ByAllAccounts
Canadian Bankers Association
Capital One Financial Corporation
Cash Edge, Inc.
The Charles Schwab Corporation
Chevy Chase Bank
The Chubb Corporation
Citigroup Inc.
Citizens Financial Group, Inc.
Comerica Incorporated
Compass Bancshares, Inc.
Corillian Corporation
Edward Jones
Ettache.com
FDIC
Federal Reserve Bank
Federal Reserve Bank of New York
Federal Reserve Board
Federal Reserve System
Federal Trade Commission
Fidelity Investments
Fincentric Corporation
First Tennessee National Corporation
Fiserv, Inc.
FleetBoston Financial Corporation
Foley Hoag, LLP
FSTC
The Goldman Sachs Group, Inc.
Government of the District of Columbia
Guaranty Financial Services
Hibernia Corporation
Household International, Inc.
HSBC USA Inc.
Independent Community Bankers of America
Intuit, Inc.
J.P. Morgan Chase & Co.
Kinexus
LaSalle Bank Corporation
M&T Bank Corporation
Marshall & Ilsley Corporation
MBNA Corporation
Mellon Financial Corporation
Mercantile Bankshares Corporation
Merrill Lynch & Co., Inc.
Microsoft Corporation
Morgan Stanley Dean Witter
National City Corporation
Northern Trust Corporation
Office of Federal Housing Enterprise Oversight
Office of the Comptroller of the Currency
Office of Thrift Supervision
Online Business Systems
Pacific Century Financial Corporation
(Bank of Hawaii Corporation)
Paytrust.com
The PNC Financial Services Group, Inc.
Princeton eCom
RBC Financial Group
Regions Financial Corporation
Solomon Smith Barney
State Farm Insurance Companies
SunTrust Banks, Inc.
Synovus
Teknowledge
U.S. Bancorp
uMonitor, Inc.
USAA
The Vanguard Group
Visa U.S.A., Inc.
Wachovia Corporation
Wells Fargo & Company
Whitney Holding Corporation
Yodlee, Inc.
Zeichner Risk Analytics
Zions Bancorporation

ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee, BITS Advisory Group and BITS Council.

BITS' mandate is to:

- Facilitate the growth of electronic banking and financial services
- Facilitate development of superior, market-driven technologies
- Maintain the industry's role at the heart of the payments system as e-commerce evolves
- Sustain consumer confidence and trust by ensuring the safety, soundness, privacy and security of financial transactions
- Leverage resources and infrastructure across the industry

BITS focuses on those areas that are most pressing to the financial services industry. Current priorities involve issues related to Crisis Management Coordination, Operational Risk, Fraud Reduction, IT Service Providers, Security and Risk Assessment, Payments Strategies and Identity Theft. BITS serves an education and monitoring role with its Patent Issues and Privacy initiatives and is scheduled to complete work related to Authentication and Aggregation in 2003. BITS and The Financial Services Roundtable have a joint Identity Theft Prevention and Consumer Assistance initiative. Additionally, the BITS Product Certification Program provides the industry with a self-regulatory measure for addressing technology risk. BITS' results range from published business requirements to a communications strategy for industry CEOs in times of crisis.

To learn more about BITS, please visit the BITS website, www.bitsinfo.org.

I. INTRODUCTION

A. Background

In its infancy, online financial aggregation involved collecting the consumer's financial data from multiple sources and presenting that information in a consolidated format. Third-party vendors, many with little financial services experience, provided the screen-scraping technology implementation that made aggregation possible. Financial services institutions (FIs) did not offer the service, were uniformly on the receiving end of scraping efforts, and lacked the ability to control key aspects of the aggregation process.

As industry and technology have evolved, two major changes have taken place: First, FIs are now the preferred providers for financial aggregation services, having assumed integral roles in the aggregation process either by contracting with third parties to offer aggregation services to their customers or by bringing the aggregation process in house. Second, simple consolidation services are moving toward a more sophisticated aggregation model which, by its nature, introduces more risk into the process. Examples include offering advanced financial advisory services based on a customer's consolidated portfolio and integrating aggregation services with other key self-service capabilities, such as inter-company funds transfers.

Aggregation today still requires the sharing of authentication secrets among multiple parties. The resulting security, business and reputation risks are causing growing concerns given the changes taking place in aggregation services. Higher-risk operations require stronger controls, both to protect the consumer and optimize the technology's value. Without more robust forms of authentication, customer usernames and passwords will continue to provide an unintentionally wide gateway to account data for parties beyond those intended by the customer. Also critical to the improved security and accuracy of aggregation services is the ability to exchange information securely based upon open and interoperable direct data-feed standards. Aggregators, account-holding financial services firms, and technology vendors face these challenges together and share a vested interest in enhancing the safety and soundness of all aspects of aggregation. This common bond was a driving force in producing this revised *BITS Voluntary Guidelines for Aggregation Services*.

B. Aggregation Services Today

While early predictions for adoption of aggregation services have not been reached, more than 100 major financial services firms are offering aggregation services. Market segmentation is increasingly driving today's aggregation functionality, with a number of financial firms catering to the high-net-worth client whose relatively complex portfolio is better suited for more sophisticated applications. Some firms have opted to provide aggregation as a staple to online banking services, integrating aggregation functionality with existing home banking services. The lion's share of the industry's aggregation technology and software is in turn provided by one or two firms.

As of 2Q03, a leading purveyor of aggregation services reports that data feeds are in place at approximately 30% of the financial sites supported. However, the percentage of large financial organizations that support data feeds is disproportionately lower, indicating that the industry has a good deal of progress to make in this area.

Robust direct feeds incorporating timely data will improve the aggregator's ability to develop new uses, especially professional financial advisers who demand the reliable data that direct feeds can provide. Direct feeds provide the real-time power required to support account analysis with a robust funds transfer and investment capacity. Going forward, aggregators hope to rely on direct feeds to provide clients with dynamic statements of their net worth that include the full spectrum of assets from cash to complex financial instruments.

C. The BITS Aggregation Services Working Group

At the end of 1999, a critical mass of BITS members experienced screen scraping of their customer's online accounts by aggregators, and voiced concerns about issues ranging from service disruptions, security breaches, privacy and legal uncertainties, and the need for consumer education around nascent aggregation services. In April 2001, BITS published the initial *BITS Voluntary Guidelines for Aggregation Services*. The *Voluntary Guidelines* applied to the most common form of aggregation—screen scraping—and provided best practices for mitigating risks associated with the service from a technical and security standpoint, as well as from a legal, privacy and customer-education perspective. The *Voluntary Guidelines* provided a framework for aggregators and financial services firms, and served as a template for structuring contracts between FIs and aggregation service providers. They have drawn international attention from financial services organizations in the U.K., Canada, Australia and Japan, as well as from international regulators through the Organization for Economic Cooperation and Development (OECD), Bank for International Settlements (BIS) and Basel Committee on Banking Supervision.

Given the importance of continued risk mitigation in an environment in which more comprehensive and complex aggregation use is envisioned, the BITS Aggregation Services Working Group developed this expanded and updated set of *Voluntary Guidelines* that takes into account both screen scraping and more sophisticated aggregation technologies. With a goal of establishing best practices around authentication processes that do not require the consumer to share his or her password with a third party, and a safer, more robust approach to data collection, this revised edition of the *BITS Voluntary Guidelines for Aggregation Services* provides guidance with respect to aggregation services technology, legal and regulatory concerns, and consumer education. Privacy issues, addressed separately in the April 2001 edition, are incorporated into the Legal and Regulatory Framework section of this 2003 edition.

These *Voluntary Guidelines* represent sound business practices that can increase the safety and soundness of the aggregation process today and in the near future. While it is not expected that every institution would meet every one of these guidelines, it is recommended that businesses implement as many of these as is commercially reasonable. Individual practitioners may well choose to implement more stringent processes. The *Voluntary Guidelines* often suggest specific target outcomes and then present several different approaches to achieving those results. This deliberate structural device (1) recognizes that there are often different means of achieving a specific goal and (2) provides the reader with some sense of the range of alternatives that might achieve a desired end.

D. How the Guidelines Were Developed

The BITS Aggregation Services Working Group solicited responses to a request for information (RFI) from developers and vendors of aggregation and related authentication technologies in order to establish guidelines grounded in current and evolving technology. Details relating to the technology, standards and services were requested in order to provide the Working Group with direction on the structure of data-feed and authentication services and the technologies and standards driving their development. With an appreciation for the financial services industry's concerns, vendors were offered several architectural structures to consider and were asked to consider requirements for interoperability, open standards, more robust authentication and data-exchange capabilities. Key concerns to be addressed were:

- **Security** – Aggregation service providers store a large number of access credentials, which create a lucrative target for exploitation. It has become increasingly difficult to apply consistent control mechanisms to protect that information.
- **Auditability** – When payments or other activities are initiated directly or indirectly from aggregation sites and customer confirmation is not a *de facto* requirement for confirming accuracy, transactions can potentially be based on incorrect data transfer, resulting in errors and financial injury. In such instances, it is important to be able to reassemble data flows to establish the source of the error.

- **Desired Data Attribute** – Screen scraping involves a constant struggle with changing source data, website designs, data placements and formats, blocked user passwords, and other disruptions that support the development of new solutions that would more readily provide consumers with the consistent and integrated view of their accounts that aggregation promises to provide.

Based on the RFI responses, Working Group subcommittees expanded and updated the *BITS Voluntary Guidelines for Aggregation Services* to promote safety and soundness as well as more scalable solutions and increased adoption. A high-level outline of the changes made to the 2001 *Voluntary Guidelines* by subcommittee section is noted below.

- **Technology and Security** – Additions to this section of the *Voluntary Guidelines* are designed to look beyond the limits and risks associated with screen scraping. Recommendations are made for safe and sound business practices for data-feed and authentication technologies. They focus on processes for account provisioning, data exchange, and encryption, data-feed and security architecture.
- **Legal and Regulatory** – Legal issues include the Federal Reserve Board’s Regulation E, the application of the Gramm-Leach-Bliley Act (GLBA) and associated privacy and security regulations, the Fair Credit Reporting Act, and liabilities that arise in a data-feed environment. Work conducted previously by the Privacy and Information Use subgroup has been incorporated into the Legal and Regulatory section and updated as appropriate. The focus is on achieving a state in which regulations apply equally to all providers of aggregation services. Success has been achieved on this front in all cases except with respect to Regulation E. The Federal Reserve has not issued a formal opinion on the applicability of Regulation E to aggregators.
- **Consumer Education** – The transition to data-feed technologies requires consumer education about a range of issues related to product functionality and changing legal ramifications. This section of the *Voluntary Guidelines* makes recommendations regarding disclosures on policies and procedures that pertain to all aspects of the consumer experience with online aggregation.

E. For Additional Information

For additional information about the *BITS Voluntary Guidelines for Aggregation Services* and BITS’ work related to aggregation services, contact BITS Director Leslie Mitchell at 202-289-4322, leslie@fsround.org or BITS Senior Consultant Gary Roboff at 914-478-9360, gary@fsround.org. Those interested may also contact Gayle Wellborn, Senior Vice President, Bank of America, and Chair, BITS Aggregation Services Working Group, at 704-388-0968, gayle.wellborn@bankofamerica.com.

II. SECURITY, TECHNOLOGY AND STANDARDS

A. Overview

Objectives

- Suggest guidelines for the collection and storage of customer account information.
- Develop a set of guidelines and recommendations for aggregation service providers, aggregation technology providers, third-party vendors, and institutional account holders with respect to identification and authentication.
- Identify the need for authentication and information exchange between aggregation service providers.

Assumptions

The security requirements follow from a set of core security principles recommended for all application development:

- Security is the responsibility of everyone within the organization. Each employee is accountable for ensuring that information-security principles are implemented and followed.
- Appropriate security controls should be designed into every system, application and business process. All systems shall include appropriate security controls (e.g., authentication, auditing).
- Security controls should correspond to the value and/or sensitivity of the underlying information. Each application system should be assessed for sensitivity, integrity and criticality as a prerequisite to defining and managing risk.
- Access should be restricted on a need-to-know basis under the principle of least privilege. Authorization for access to information should be driven by the sensitivity of the information and the user's need to know.
- Security is most effective when implemented in a complete and consistent manner, and when all known vulnerabilities are addressed. Information is an asset and should be protected from unauthorized access, disclosure, destruction, modification or loss, whether accidental or intentional.

Guidelines

The following guidelines, which implement these objectives, are:

- Security Guidelines for "Trusted" Aggregation Services; and
- Guidelines for Aggregation Authentication and Data Feeds.

B. Security Guidelines for Trusted Aggregation Services

Overview

Aggregation services are being performed by a number of companies on the Internet. The nature of these services, if not properly implemented and trusted, can pose significant security risks to the customers of these services (end users), the institutions whose customer information is being aggregated (institutional account holders), and the companies providing aggregation services (aggregation service providers).

Guidance from various sources, such as the American Institute of Certified Public Accountants (AICPA), addresses control practices that should be considered. The security guidelines in this document focus on specific implementation considerations. They have the most value when used in conjunction with a full range of security practices and processes related to internal management controls, including those for development, quality control, change management, vulnerability assessments, virus protection, monitoring, response, and recovery.

General Security Architecture/Framework

There is more than one way to implement an aggregation service. This document discusses alternatives based on a general framework for secure implementation for a “trusted” aggregation service by use of multiple servers, as one example. Multiple servers are best implemented in protected layers. This layered approach is used to protect the most sensitive information from direct Internet access, to reduce impacts from a single compromise of a server, and to limit exposure and authorized access to servers containing the most sensitive information. These concepts, coupled with multiple data and system protection technologies, are often referred to as a “defense in depth” approach.

The aggregation service provider’s customer accesses the aggregation service over the Internet using a standard Web browser client. The Internet-facing Web server contains the “presentation layer” for the aggregation service. This server interacts not only with the customer but also with a notional “business application layer” server. The business application servers also interact with other corporate systems that generally house customer data.

Presentation layer servers (of the aggregation service) should provide for access right limitations and be protected from the Internet by firewall technology as well as monitored by an intrusion detection system (IDS). The firewall platforms’ operating systems should be hardened so that only those operating system services necessary to operate the firewall are used or even installed, and only those services necessary to run the Web application are enabled through the firewall.

In addition to operation system hardening, the business layer server should be further isolated from the presentation layer through use of another firewall layer in what is often termed a “demilitarized zone” (DMZ) or similar system and/or use of proxied services. The goal is to assure that any compromise of the presentation layer server system does not inherently provide a vehicle to compromise the business application layer servers. Additionally, sensitive customer or customer credential data are best housed outside of the application logic. Protection and access to customer data by separation of one layer from another is recommended.

Specific Security Requirements

Through the BITS Product Certification Program (BPCP), BITS has established specific security profiles for aggregation applications. Providers of aggregation services are encouraged to meet the criteria in the application product profiles published on the BITS website and pursue BITS Certification. Additionally, vendors pursuing Common Criteria (CC) Certification should include the BITS CC profiles in their product testing plans.¹ Providers of aggregation services should also address the following aspects of security (as outlined in the subsections below): data security, application security (including passwords and application development), network security, firewall security, physical security, and operations security (including audits, disaster recovery, personnel security, and subcontractors). In case of inconsistencies between the BITS application product profile and this document, in the case of aggregation products, this document will supercede the profile.

There are certain basic system-level guidelines that are applicable in the aggregation infrastructure. These include:

- All financial data transport, throughout all aggregation-related processes on public or unprotected networks including end-user presentation, should be encrypted as described in Appendix II, Industry Encryption Standards.
- Customer authentication credentials should be encrypted during storage and transmission using industry-accepted standards. Customer nonpublic personally identifiable information gathered through aggregation should at a minimum be protected as required by industry laws and regulations, such as GLBA.

¹ For more information about the BITS Product Certification Program, go to www.bitsinfo.org/fslab.html.

- The process should provide for audit support in a manner agreed to by the respective parties. Such audit-support solutions may include signatures, transaction IDs and public time-stamps.
- All security guidelines should be enforced during migration processes when those involved in providing the aggregation service or other parties change technology providers.

Further, the security guidelines fall into five categories:

- Data Security
- Application Security
- Network Security
- Physical Security
- Operations Security

Each of these areas is explored in greater depth in the following sections.

Data Security

Public and widely used or financial industry standards for encryption (see Appendix II) should be used for the communication of all sensitive, personally identifiable or security-sensitive customer and account information. Storage of passwords, PINs and account numbers should be encrypted using public and widely used standards or financial industry standards. These types of data are best stored and managed in an encrypted form throughout the entire system and only decrypted at the end point of use. All personally identifiable and security-sensitive customer or account information should be encrypted. Additionally, greater compartmentalization of information should be implemented through the use of multiple encryption keys, so that a compromise of a single key does not provide access to all other information.

Neither customer passwords nor PINs should be available for viewing or for reporting by administrative or customer support personnel at the aggregation service provider. Additionally, developers should neither have access to, nor use, actual customer passwords or PINs in the process of developing and testing applications. (This does not include those test accounts or customer accounts that have been approved or established for troubleshooting purposes.)

Operating policies, application and database software implementations and operating system features should ensure that old, deleted, or inactive account data do not remain in the active data repository. Customer credential information should remain encrypted in backup and archive media. Specific procedures for assuring the security of backup media, both logical and physical, should be documented and periodically audited.

All aggregation service provider customer enrollment/de-enrollment and customer profile or account information changes should be logged. Tracking information such as user ID, time stamp, account number, and type of change identification should be included in logged records. Personally identifiable customer information in logged information should be accessible only to authorized individuals requiring such access to perform their duties.

In summary:

- All authentication credentials should be encrypted, including:
 - **Master credentials**, which are used to protect access to aggregated information at the aggregator website.
 - **Site-specific credentials**, which are used to protect access to account-holding financial institution websites, but are stored in the aggregator data store to enable aggregation.
 - **Operational credentials**, which are passwords used by operational personnel to manage and maintain systems running the aggregation system.
- Master passwords should be one-way hashed to further protect compromise.
- Industry-accepted encryption key management processes should be deployed.

- Encryption keys may be stored in tamper-resistant hardware security modules (TRSM).
- For further protection, data-expiration policies should be documented and implemented.

Application Security

In addition to the points noted below, aggregation service providers should also follow the general security tips for online financial services accounts developed in conjunction with the BITS Product Certification Program. (See page 10.)

Access to customer services should be controlled through protected authentication and authorization processes, and should incorporate the following:

- Customer information access should be protected by authentication credentials, such as username and password or other credentials of similar strength.
- Such authentication should be timed out after a predetermined period of inactivity.
- The timeouts may be implemented on both the client side and server side to protect user information in the case of unattended workstations.
- Password controls should include:
 - Password construction.
 - Minimum length requirements for all users of at least six (6) characters.
- Passwords should contain a mix of upper and lower case letters, numbers and special characters. Specifically, passwords may:
 - Be constructed of uppercase letters, lowercase letters, numbers (0-9) and the special characters !, @, #, \$, %, ^, &, (,) and *.
 - Be required to contain characters from at least two of the three sets above.
 - Be required to be case-sensitive for optimal security levels.
- Passwords may be required to be changed within a set time period.
 - Password change timeframe may be set to 180 days for optimal security levels.
- When passwords are changed, they may be required to be different from some predetermined number of previous passwords.
 - This number may be set to 3 for optimal security levels.
- The application should lock users out upon a predetermined number of invalid password attempts.
- Credentials should be masked when displayed, entered or printed.

Administrator controls should be provided to only a limited number of authorized individuals. Such administrative control should be accessed only via enhanced access control and authentication with special attention to any remote administration. It is important to log all administrator actions.

Development Process

Application source code should be developed on a separate server from production executables. A quality assurance process should be established and followed to evaluate, monitor and control the establishment of production code and implementation of changes. An independent group should perform code reviews and audits of security critical features. Such reviews should be performed before new code is released into production environments.

For purposes of problem resolution, application log printouts should be designed to minimize divulging customers' personal information. For example, debug printouts should produce truncated information of sensitive account number information.

Troubleshooting, debugging or performing any other support role can be done in a production and a non-production environment.

Session cookies should be implemented in a manner that will not compromise sensitive information or authentication services. If the cookies contain user-identifiable information, the information should be encrypted.

The application should be developed in accordance with the following:

- All confidential data passed to the browser should have the highest level of encryption generally available.
- All pages containing confidential data (including any secure entry pages that have Web forms for logins) should be set not to be cached and to expire immediately.
- The method used for all sensitive parameter-driven requests sent to an aggregator should always be POST. This minimizes the appearance of confidential data in browser history lists.
- No authentication data should appear in the page source in clear-text form. This means that when a user displays the page source, the user should not see an unencrypted PIN or CODEWORD, or any other authentication data displayed in clear-text form within the page source.
- All information received from a browser should be validated based on information stored on internal known and trusted aggregator data repositories. Information received from the client should not be trusted.
- Cookies are vulnerable to attack, so care should be taken in their generation and use. In general, cookies should be encrypted, and set to expire within a normal browser session. With confidential transactions, the application may verify that the cookie was not stolen. This can be accomplished by verifying that the browser environment variables have not changed since this previous interaction in a session.
- The method used for all requests sent to an aggregator should always be <POST> Furthermore, the POST technique is strongly recommended for application-to-application communication. However, if <GET> is used, the following guidelines should be followed: <GET> should be used only for application-to-application communications that reside within the same security infrastructure. (Note: The GET method should not be used for any application-to-browser communications.)
- All fields fed into the application, including hidden fields, from the browser **must** be centrally checked and filtered for dangerous patterns, for example, cross-site scripting attacks and other vulnerabilities.
- None of the parameters that are at all specific to a customer or to any type of authentication or authorization should be included in the URL as part of a query string. If the management of variables cannot be handled strictly at the application server level, once initial entry is made, then encrypted hidden fields in Web forms should be used.
- Application failures should not degrade security controls. Applications should fail securely.
- Active server pages, Active X, Java, and Java scripting best practices are outside the scope of this security document. Application developers should document all security assumptions used for these types of implementations. A documented process and application-development methodology and standards are recommended for code development based on current, good security-development practices.

Network Security

- SSL should be used when obtaining data feeds.
- Client certificate authentication may be used to add another factor to the authentication process between the aggregation service provider and the institutional account holder.
- Network traffic between components should be encrypted whenever carrying personal information, even within data centers.
- Encryption and authentication between server components (i.e., presentation, application and data servers) should be used if not co-located in a protected physical environment.

- Each server layer within the framework should be protected and services should be enabled to prevent a single breach from compromising the entire system.

Firewalls

For aggregation service dedicated firewalls, the perimeter firewall should be configured to allow only hypertext transfer protocol (HTTP) and Secure Socket Layer (SSL) enabled connections, i.e., HTTPS, to designated externally visible IP addresses. No exceptions to this rule should be permitted, unless additional specific services are part of the aggregation service and are securely addressed in the design process.

- The perimeter firewall and other server components should use internal IP addresses only, in order to reduce the possibility of detection and subversion of the components.
- Remote access to firewall areas via the Internet for support purposes should use virtual private networking (VPN) and multi-factor authentication.

Development Processes

- Regular external/internal network penetration assessments should be performed to identify changes or new weaknesses in boundary networks, as well as the internal networks. This should be included as part of any certification process.
- Access by service personnel is best authenticated using multi-factor authentication. This access should be limited to the appropriate support groups.

The Demilitarized Zone

A Demilitarized Zone (DMZ) protects the logical boundary between two networks of different security models. The Internet DMZ separates the Internet from the main internal network. It is actually a collection of networks, and each has a security policy based upon the sensitivity of the applications or data on the component machines. The DMZ was designed to conform to the most stringent security tenets while still allowing legitimate commerce.

Basic DMZ Tenets

- Access is denied by default. What is not explicitly allowed is denied.
- Multiple layers of defense are used to increase the effort required to compromise a system or systems and to increase the probability of detection.
- All Internet traffic is monitored and incoming connections are, by design, accepted ideally only at specifically authorized ports. Services available at the Web server should be only the absolute minimum required.
- Responsibility is separated in all aspects of system and process design. This separation increases the number of people and machines it takes to fully compromise the system and decreases the probability a malicious user may cause extensive harm without additional resources.
- The rule of least privilege provides individual machines/processes/users with the minimum amount of privileges needed to conduct their function.
- Auditability provides continuous and permanent monitoring and auditing capability to minimize the impact of an intrusion through quick detection, and increases the probability of successfully tracking and prosecuting an intruder.
- Physical security ensures that the DMZ environment is accessed only by those who need it.
- Internal and external defense mechanisms should be established. Appropriate measures should be taken to minimize risk of insider access to production data.
- Passwords are confidential data. As such, they should not be stored or transmitted in the clear-text form anywhere in the system.
- A tiered architecture should be implemented for aggregation systems.

- An aggregation system is unique in that it has two different interfaces to the Internet:
 - **End-users' browsers connecting to front-line servers.** This is an inbound connection. End users access their data from the aggregation system using this connection. This interface should be placed in a separate tier and needs to be separated from the “data access layer” that has access to the “data store” where the end-user information is stored. This separation is achieved through the use of DMZ or similar separation that provides the same assurance to keep the front-line servers from the data access layer.
 - **Data gathering servers connecting to other financial institution websites or data feeds.** This is an outbound connection. The aggregation systems use this interface to communicate with other information providers or service providers to gather data to be aggregated. This interface also needs to be placed in yet another tier and needs to be separated from the “data access layer” through the use of a DMZ or similar separation.

Physical Security

- Policies should restrict data-center and server access to authorized personnel only. Controls for escorted visitors should be implemented and followed. The following policy traits are recommended:
 - Education and awareness training should be provided for employees to ensure they understand policies and practices.
 - Practices should be posted that show steps taken to ensure restricted access.
 - Practices should be posted that show conditions under which employees have access to data.
- Facilities protection measures should be designed to prevent physical access by unauthorized individuals and detect, with a high degree of probability, unauthorized access attempts and unauthorized accesses.
- All access to facilities hosting aggregation should be monitored via video surveillance and protected with, at a minimum, card access.

Operations Security

Development, quality assurance (QA), and production operating environments should be physically separate and maintained separately. Preproduction (development) hosts should not also be used as QA hosts, nor should QA hosts be used for a production environment and or for production hosts.

Separation of responsibility should be maintained. In other words, there should be separate groups of people who write code vs. those who review QA and approve it for production.

Some form of multi-factor authentication should be used to control updates and access into production from any location (including QA).

Only authorized personnel should have server access. Access to the server should be only by encrypted management protocols (i.e., SSH, SCP, SSL-enabled Web-management interfaces, and VPN solutions), in order to safeguard the encryption of sensitive clear-text protocol information. It is considered a best practice to employ encrypted communications, even over a trusted network. More formalized access management and tracking with detailed access reports offers enhanced security management.

Servers should require multi-factor authentication before remote access is authorized. Administrators should not have the ability to generate passwords for new users. (Note: Established passwords should be system-generated, for one-time use, and set/reset only after authentication.)

Customer support for forgotten passwords should be accomplished through an automated password reset mechanism, and not by any display of decrypted passwords to tech-support personnel.

Super user privilege accounts should be limited and accessed by supervisor administrator personnel or through the use of trusted operating systems requiring multiple persons with different levels of privilege to accomplish sensitive operations in a production environment.

Separate access (by different people) on data repositories and key repository servers (i.e., separation-of-duties principle) should be implemented.

Procedures for regular configuration reviews of the rule set for the firewall should be implemented. Host-based and network intrusion prevention/detection should be deployed, with monitored reporting. Centralized logging of hosts via secure channels (i.e., encrypted silo) should be employed. File integrity checks should be in place to identify changes to files systems to aid in the detection of unauthorized changes.

An emergency response process should be part of standard operating procedures for responding to compromises in security. Notification of appropriate parties (including any affected financial institutions), enhanced logging, capturing system log backups, and investigations should all be part of the response process.

Detailed build documents for every component of the application, including hardening scripts for every operating system (OS) used in the production environment, should be placed into “code and document escrow.”

All security patches for system components or application vulnerabilities identified by vendors should be assessed through a risk evaluation process, and those assessed as critical for the given environment should be tested and implemented in an expedited manner. Those of potentially lesser impact should be implemented within a reasonable period.

Audit logs for transactions, customer information changes, and critical security-related events should be maintained in a protected manner for problem resolution and problem alerting. Records, especially those involving the buying or selling of securities, should be maintained in accordance with regulatory and established financial industry practices.

All events involving the following activities should be logged:

- User enrollment
- User permissioning
- User de-enrollment
- User or agent data access
- User or agent transaction initiation

In each of the above cases the appropriate aspects should be logged in order to enable the following actions:

- Establish the location of user when initiating operation
- Establish association of user permission with above operation
- Establish time and date of user permission within a reasonable window of time (5 minutes)
- Correlate and retrace user action through various levels of the system

The following events should be audited in all systems storing confidential data:

- Security profile changes (including adds, deletes)
- Logon access failures
- Privileged use
- Audit configuration changes
- Resource access failures

- Software installation
- Disk mounting/dismounting
- Backup
- Restore
- System configuration changes
- Cryptographic key generation
- Revocation of cryptographic keys

In addition to the list above, the following system events should be audited:

- System time changes
- Successful logon
- User logoff

Auditing for the following system events is optional:

- Auto logoff
- Password change
- File opens
- Program initiation/image activation
- Deletion of objects

The following information, at minimum, should be recorded for each event:

- Event time – Date and time that the event occurred
- Event type – Category or type of event (e.g., logon failure, account update)
- Event status – Result of the event; if failure, reason included
- Object attributes – Description of the object(s) affected by the event
- Originator user ID – Identity of the user who initiated the event or action
- Subject ID – Identity, if applicable, of the subject/object impacted by the event (e.g., user ID, filename, queue)
- Process user ID – Identity, if applicable, of the system process performing the event

In addition to the guidelines listed above, the following guidelines should be used for system level auditing: Where possible, system audit logs should be stored on an alternate system. Production audit logs should not be widely accessible. The separation of the development QA and production environments should protect the production audit logs from widespread access.

- System audit logs should be retained a minimum of six months or as required by regulation or statute either online or secured backups. Hardcopy storage is not desirable due to difficulty in searching for specific records or events.
- System audit logs should be backed up as part of routine system backups.
- System audit logs should have adequate access controls (e.g., file protection) to protect against unauthorized modification or deletion. Audit data should be considered confidential. Encryption of extremely sensitive audit data may be desirable.
- System audit log sizes should be monitored to ensure availability of sufficient disk space.
- System time should be synchronized with a time service. If time service synchronization is not possible, procedures should exist to check for and correct variations on a monthly basis.

- Procedures should be defined for each system indicating what type of activity will be reviewed on a regular basis, who will perform the reviews, and escalation procedures if suspicious activities are detected.

The specific events that should be audited at the application level will, by nature, vary depending on the application. The following list of data elements should be used as guidelines for developing application-specific audit capabilities:

- Date/time stamp – Date/time the event occurred
- Transaction ID – A unique identification string permanently assigned to a transaction during its lifetime
- Account number – Customer account number
- Account type – Account type (e.g., DDA, CAP, savings, brokerage)
- Source/channel – Identification of where the transaction was initiated (e.g., remote banking channel, terminal ID)
- Originator ID – Identity of transaction originator (customer account number, PSR user ID, branch employee user ID)
- Application ID designator
- Transaction type/function – Transaction type (e.g., stop payment, funds transfer, statement inquiries, etc.)
- Transaction status – Transaction status (success, fail) and any relevant information
- Transaction-specific elements – Data elements specific to the transaction (e.g., to/from account numbers for funds transfer, merchant ID for bill payment)

In addition, the following guidelines should be included for application-specific auditing:

- Where possible, application audit logs should be stored on an alternate system.
- Application/transaction audit logs should be retained a minimum of two years or per legal or regulatory requirements.
- Application/transaction audit logs should be backed up as part of routine application data backups.
- Application/transaction audit logs should have adequate access controls (e.g., file protection) to protect against unauthorized modification or deletion. Audit data should be considered confidential.
- Application/transaction audit log sizes should be monitored to ensure adequate disk space exists.
- System time should be synchronized with a time service. If time service synchronization is not possible, procedures should exist to check for and correct variations on a monthly basis.

Business Continuity (Disaster Recovery)

A business continuity plan and procedures should be documented and tested once a year, at a minimum.

Backups

Backups of system, application, and data should be conducted in accordance with established procedures, with customer-related data backed up daily and system and application backups at each change.

- All backups should be removed to secure and bonded storage at a different physical location at predefined regular intervals.
- Audits should be performed to assure procedures and controls are functioning as designed.

Personnel Security

- Background checks should be conducted for all personnel with access to the systems and information.

- Maintain a list of all authorized personnel with access to servers. Access authorization should expire and have to be renewed as part of the standard procedures. This should be defined in an application security plan and validated by third-party auditors.
- Aggregation service-provider policies and ethics statements detailing employee liabilities and responsibilities to protect customer data should be signed by each employee. Background screening checks are suggested for those with sensitive access or management approval responsibilities.

Third-Party Integration and Subcontractors

- Third parties or subcontractors providing services that require access to the system in support of the aggregation service are also responsible for complying with security requirements established in this document. Specific applicable requirements should be identified and risk assessment should be conducted based on the proposed service or subcontracted responsibilities and implementation. The aggregator remains responsible for assuring minimum security requirements are maintained among these relationships and should include such guidelines in the applicable contracts or agreements. Third-party or subcontractor compliance audits should be conducted on a regular basis, not less than annually.
- Third parties should maintain a list of all authorized personnel with access to servers. Access authorization should expire and have to be renewed as part of the standard procedures.
- Aggregation service providers should ensure that their security policies concerning their liabilities and responsibilities to protect data are agreed to by contractors.

Policies

The aggregation service provider should establish a management-approved information security policy and a compliance program supported by independent audits conducted on an annual basis.

Audit/Certification

All operational development and infrastructure controls should be independently verified through industry-accepted audit processes such as SAS70 or ISO 1799 standards and protocols.

III. GUIDELINES FOR AGGREGATION AUTHENTICATION AND DATA FEEDS

A. Overview

The April 2001 *BITS Voluntary Guidelines for Aggregation Services* focused on defining those characteristics that would establish safe and secure Web-based screen-scraping systems. While screen-scraping systems will likely continue to play an infrastructural role for the foreseeable future, the industry recognizes the need to migrate toward stronger authentication systems and more structured data-transfer mechanisms. Thus the expanded and updated *Voluntary Guidelines* provide recommended characteristics of alternative authentication and structured data-transfer mechanisms.

The *Voluntary Guidelines* are divided into two broad categories: system-level guidelines and use-case level guidelines, as explained below.

System-Level Guidelines

System-level guidelines apply to all aggregation service providers of the system in all its forms and use cases. Aggregation architecture should support open and interoperable standards and provide for the interoperability of authentication solutions with multiple data collection techniques, i.e., screen scraping and data feeds. The BITS Aggregation Services Working Group has defined “open protocols and standards” as those published by organizations with the following characteristics:

1. A governance body that is open for anyone to join under the same terms and conditions and voting privileges.
2. A democratic governance structure that is controlled by all members on a nondiscriminatory basis and enables all members to have a voice in:
 - Proposing new standards and governance.
 - Proposing or considering changes to existing standards and governance.
 - Reviewing proposals originated by anyone else in the organization.
3. Intellectual property is available to all entities on the basis of reasonable and nondiscriminatory terms.

There are a number of protocols and standards in use today in the aggregation space, which form the basis of the solutions recommended in the *Voluntary Guidelines*. These protocols and standards originate from bodies with varying degrees of openness, and the Working Group encourages:

- Individual financial institutions and other aggregators to explore the governance structures of those standards they may wish to consider in implementing proposed solutions.
- Governance bodies to continue modifying governance structures to ensure that users have a guaranteed role in evolving the standards. There has been meaningful progress in this regard, and the industry can only benefit if that momentum continues.

Examples of data-exchange protocols that may form the basis of data-feed solutions include IFX and OFX, and YML. Examples of standards and protocols that may, in whole or in part, form the basis of authentication solutions include SAML, YAAML, Liberty Alliance, and XACML.

Examples of standards that are relevant to security solutions can be found in Appendix I.

Use-case Level Guidelines

Given the specific nature of the revised *Voluntary Guidelines*, there is a need to identify ideal characteristics in each of the various phases of operation or use cases and provide proposed alternatives to authentication and data-feed protocols.

These *Guidelines* are not meant to prescribe one specific solution over another, but rather to describe in some depth the characteristics that are desirable in any implementation solution. They should be viewed as the minimum characteristics that would support the kind of robust aggregation functionality envisioned by the Working Group.

The *Guidelines* below describe the recommended characteristics of authentication solutions and data-feed solutions across the entire set of use cases in which they may be used.

B. System-Level Guidelines

Aggregation systems should adhere to the following general overall system guidelines and include specific solutions:

- Aggregation architecture and system implementation should be based on open and interoperable standards for both authentication and data-feed solutions.
- Migration of current authentication and data-collection risks should be able to be addressed independently, allowing for flexible implementation options.
- The solution needs to support and provide interoperability with both screen-scraping models and open data-exchange solutions.

C. Authentication Solutions

A basic framework for the desired authentication system is provided below. BITS may further develop these guidelines at a later time.

Overview

The current practice employed by aggregation service providers to access their end users' online accounts on their behalf raises two major identification and authentication issues:

- It is usually necessary for end users to surrender their personal primary authentication credentials (such as username and PIN) for a given site to the aggregation service provider and/or third-party vendor in order to allow the access their accounts.
- Institutional account holders have no practical and reliable way of tracking whether a particular access to an account was initiated directly by the end user owning the account or through an aggregator, and, if the access was through an aggregator, the identity of this aggregation service provider/third party vendor.

Both of these issues should be addressed by any candidate solution for a next-generation authentication system.

Desired Characteristics

This section defines a set of guidelines and recommendations for aggregation service providers, aggregation technology providers, third-party vendors, and institutional account holders with respect to aggregator identification and authentication.

For the next generation of authentication systems, the following characteristics should be part of any candidate system:

- Can interoperate with legacy scraping systems as well as open data-exchange solutions.
- Based on industry standard security technologies (SAML, WS-Security, etc.).
- Does not require the user to share credentials with anyone other than the account-holding financial institution.

- Enables users to authorize particular accounts and particular views to be aggregated.
- Is auditable for access and authorization at both the financial institution and aggregator.

D. Data-Feed Solutions

Overview

The current method of aggregation services involves simulating user behavior to access the website of an institutional account holder and scrape account summary information from the HTML. There are significant problems with this approach, including concerns about performance, overhead, timeliness and accuracy of the data.

The first tier of solutions for feeding institutional account holder data to an aggregator more reliably than currently achieved through screen scraping requires some institutional account holder development effort. Ultimately, existing data-transfer protocols should interoperate with the recommended authentication solutions. In today's environment, open and proprietary standards compete for aggregation utility. This situation is complicated by the functional breadth of financial services products that are part of the aggregation landscape. All aggregators and institutional account holders are encouraged to support the development and use of broad-based, openly governed standards. It may be desirable for the industry to achieve interoperability through a single aggregation data-transfer standard in the long term; the current goal is to focus on reducing the number of standards.

Desired Characteristics

A data-transfer solution should:

- Support batch mode request and response for aggregation-like transfers.
- Support institution-level in addition to user-level authentication.
- Support international currencies and instruments.
- Provide classification of transaction type, e.g., buy/sell, dividend, inquiry, etc.
- Provide support for a unique transaction ID for each transaction.
- Provide support for incremental data-transfer requests.
- Be natively XML.
- Have SOAP bindings for use over Web Services.
- Support independent authentication model to enable use of alternate authentication and permissioning systems.
- Support the banking and brokerage account types, holdings, and other products listed in Appendix II.

Solutions also may support publish subscribe mode if possible.

Ultimately, all existing data-transfer protocols should be expanded and should interoperate with the authentication solutions above. All aggregators and institutional account holders are encouraged to support these methods for exchanging data and messages between institutional account holders and aggregators. Initially, many institutional account holders will not be able to support these methods. Over the long term, we recommend moving to as few interoperable standards and protocols as possible that are compatible with prevailing Web services standards.

Interim Approach to Data Feed Exchange Via Structured Downloads

While the above characteristics of data-feed solutions are desired, no existing protocol supports all of these characteristics. Therefore, today's most readily available structured file download mechanisms should be leveraged

to move away from screen scraping. All aggregators and institutional account holders are encouraged to support the development and use of broad-based, openly governed standards.

This transition to a structured data-feed format is likely to take place gradually. In the interim, BITS recommends the use of open-standard structured data-transfer mechanisms wherever available. Most online banking services provide a feature for PFM users' ability to request and receive data in a static download format that is more reliable because it utilizes a fixed-data structure. This process includes but is not limited to the use of OFX/QIF downloads that allow an aggregator to download a file representing positions and transactions in a standard format such as XML-compatible versions of OFX and IFX. This clearly addresses many page-layout issues. But because it still involves logging in and page-level navigation, the same reliability issues stemming from screen scraping arise. That is, a download may fail due to layout changes (URLs may change), site availability problems, etc. Our recommendations regarding file downloads include the following:

- OFX downloads should be made available if requested by the aggregation service provider/third-party vendor and supported by the institutional account holder until a more robust structured data-transfer mechanism can be made available. However, it should be noted that most OFX/IFX formatted information today is insufficient to run aggregation applications, and is often supplemented with scraped information.
- Downloads should be stateless, i.e., they should not be affected by previous requests or influence subsequent requests.
- Downloads can be performed without affecting a subsequent download performed by the user.
- Data are at least as up-to-date as the data provided by the website.
- Performance should be comparable to the speed of viewing account activity on the website.
- Data provided in downloads should be expanded to include all information described below under IFX or OFX server support, or available via any other channel available to the user (website, PFM tools, ATMs, etc.).

E. Use-Case Level Guidelines

- In addition to providing the privacy policy as part of the enrollment process, the aggregator should also clearly explain its responsibilities for data collection and correctness.
- The authentication method used to perform the auto-logon feature should equal in strength the method that might be developed for the authentication solutions suggested in Section C.
- Aggregators should not directly conduct financial exchange transactions on the institutional account holders' websites. If transactional functionality is provided, the aggregator should use those functions developed internally or must have an agreement with the bank whose transaction system it plans to use.

Customer Enrollment with Aggregation Service Provider (Initial relationship setup)

- The technology should enable the aggregation service provider's privacy policy to be provided as part of the enrollment process.

Account Provisioning

Account provisioning involves creating a relationship between the end user, the aggregation service provider and the institutional account holder that enables the aggregation service provider to obtain authorization to access a particular account (or set of accounts) held at the FI. Account provisioning should consider the following:

- Accounts need to be provisioned before any data transfer takes place between the aggregation service provider and the data provider.
- The provisioning protocol should enable end-user authorization prior to enrollment of accounts with the account at the aggregation service provider.

- The aggregation service provider should identify itself to the data provider on behalf of the end user. As a corollary, data providers should uniquely identify both the aggregation service provider and the end user prior to providing the requested data.
- Authentication and authorization credentials should be unique among the aggregation service provider, institutional account holder, and the end user, respectively, and should not require users to reveal any components of their primary authentication credentials to any entities beyond the issuing party.
- The process should provide audit support for account provisioning in a manner agreed to, when possible, by the respective parties.
- The process should ensure that exchange of credentials is not easily subverted.
- When auto logon is offered, an end user at an institutional account holder's site should be able to link to and logon to the data provider's website without requiring the user to share his or her data provider ID and password with the aggregation service provider.

Data Exchange (Transfer of account data and other data between the account-holding FI and the aggregation service provider)

- The data-exchange system should allow the exchange of an end-user specified subset of the customer's information at an account. This assumes that those account-level groupings are available at the data source.
- The data-exchange solution should allow the aggregation service provider to act on behalf of the end user. Such actions should be specified in the disclosure of agency being granted to the aggregator by the end user and supported by the institutional account holder.
- The data exchange should be audited, including tracking transactions and data access.
- The solution should allow data exchange to be employed independent of the user interface the aggregation service provider and the FI use to communicate with their customers.
- In the case of screen scraping, the end user should be informed of the nature of the information being gathered, and that process should comply with GLBA.
- Data-feed protocols should be used for transferring user statements on all available retail financial services instruments as offered by the FI, to eliminate screen scraping.
- Data-feed protocols should support international assets and liabilities.

IV. CUSTOMER EDUCATION

A. Overview

In creating the *Voluntary Guidelines*, the BITS Aggregation Services Working Group's Customer Education Subgroup identified issues and developed recommendations for educating end users about aggregation services. These recommendations apply to the institutional account holder, FI, and the aggregation service provider. The topics, explained in this section, include aggregation relationship disclosure, PIN-sharing policies, end-user protection, customer service, data accuracy, disclosure distribution, privacy, marketing messages, security, service discontinuation, and the use of user data for development/test purposes.

B. Assumptions

- An institutional account holder may provide aggregation services as an aggregation service provider. In this case, the institutional account holder should communicate with the end user from both the institutional account holder and aggregation service provider perspectives, making these separate roles clear.
- Aggregation services may be available at a third-party vendor site, even though no contractual relationship exists between the institutional account holder/FI and the third-party vendor. However, because they are able to obtain their institutional account holder/FI account information, end users often assume that a contractual or operational relationship exists in these situations. The end user may also assume that no risk is involved, reasoning that the institutional account holder/FI would not allow such transactions if they were not safe.
- Customer service representative training in aggregation services at the FI/third-party vendor/aggregation service provider should include a definition of aggregation, an explanation of how it works, and the following potential customer service issues:
 - Designation of whom to call for service and data-integrity issues (for example, for information aggregation services, the aggregation service provider's only responsibility is to verify that the information it presented to the end user was identical to the information taken from the institutional account holder; thereafter, the end user should be directed to the institutional account holder, and the aggregation service provider should have no further responsibility); and
 - Definition of error-resolution procedures (for example, instructing the end user to update or refresh the information).
- FIs should state their level of participation regarding aggregation services. For example, an active participant may communicate to the end user that it has "selected the following aggregation vendor or service in order to enhance the end user's online experience," and ask end users to review the agreement and click an "I accept" button at the bottom of the disclosure. Alternatively, a zero-tolerance institution may provide a cautionary sentence and FAQs for end users regarding aggregation at their online banking sign-on page.

C. Guidelines and Recommendations

The following are recommendations for all participants in aggregation services. Participants are strongly encouraged to abide by these *Voluntary Guidelines*. The *Guidelines* are intended to enhance customer relationships and serve educational purposes.

Overall Recommendations

- Provide end users with a high-level description of aggregation.
- Provide end users with a high-level description of authentication options.
- State the functionality the service provides.
- Require end users to accept the disclosure before he or she completes the aggregation application process.
- Guide end users in what to look for in an aggregator service.
- Notify end users of any changes in the end-user aggregation agreement.
- As end users apply for online services at the FI, suggest measures they can take to safeguard their account information when signing up and terminating service with an aggregator that is not the institutional account holder.

PINs

- State the PIN sharing policy.
- Remind end users that if they change their PINs with the FI, they will need to change it on the aggregation service site as well.
- Recommend to end users that if they terminate service with the aggregation service provider, they should change their PINs with the FI.

End-User Protection

- Provide steps for end users to take if they identify an error on their account.
- Identify regulations in effect to protect consumers.
- Clearly communicate any end-user protection policies unique to the end user's FI.
- Provide end-user service contact information.
- Inform end users that the security procedures used by aggregation service providers (e.g., how their account PINs are stored and protected) may vary, and may be different than those used by their institutional account holder.

Customer Service

- **Point of Contact:** Identify whom the end user should contact for service questions regarding incorrect or missing information and incorrect or non-enacted transactions.
- **Self Help:** Provide FAQs on the site for end-user self help (e.g., provide a technical how-to).
- **Correcting Errors:** Establish and maintain procedures by which customers may correct inaccurate information. Aggregation service providers should disclose these procedures in a timely manner.
- **Resolving Complaints:** Clearly advise end users about the complaint-resolution process.

Data Timeliness

- Provide the end user with a disclaimer about the accuracy and completeness of information available through the service.
- Disclose the timing of updates and/or date and time stamp of balances.
- Disclose that the aggregator may not have information about or control over the timeliness of aggregated data because the frequency of data updates will vary among sources.
- Disclose the impact to financial decisions based on data timeliness.
- Inform the end user that the service may be unavailable during maintenance hours.

Security

- Provide the end user with a high-level description of the possible risks associated with aggregation services.
- Suggest the end user ask whether the aggregation service provider is voluntarily complying with aggregation industry security guidelines.
- List the BITS Security Tips for Online Financial Services Accounts on your website and in collateral materials. (See section IV E.)
- Note that username/password information is stored separately from financial data.

Privacy

- Post a privacy statement at the website and on the aggregation-enrollment page. (This posting may be different from the privacy statement of the sites being aggregated.)
- Specify how the customer's information may be used by the aggregator or affiliates.
- Include a marketing opt-in/opt-out option in the registration process.

Disclosure Distribution

- Remind end users that aggregation service providers may not provide disclosures from the institutional account holder website and that end users may want to periodically check it themselves.

Service Discontinuation

- Recommend that end users change their PIN when canceling the aggregation service.
- Provide the account-termination policy and procedure.
- State policy for length of time information is maintained after service termination.

Customer notice and options surrounding choice should comply with all relevant regulations, recognizing that certain state laws may supercede GLBA (and are subject to permissible exceptions under GLBA):

- The end user should be notified of any sharing by the aggregation service provider of nonpublic personally identifiable information with third parties.
- The end user should be given the option to opt-out of the sharing by the aggregation service provider of nonpublic personally identifiable information with third parties for marketing purposes. This choice should be available when the subscription begins and anytime that the aggregation service is being used.
- The end user should be notified of any sharing by the aggregation service provider of non-experience information with affiliates (as defined by the Fair Credit Reporting Act).
- The end user should be given the option to opt-out of the sharing by the aggregation service provider of non-experience information with affiliates (as defined by the Fair Credit Reporting Act).
- If an aggregation service provider offers end users the opportunity to choose to participate in marketing programs (*not* a suggested guideline), and if those options are not specified on a channel-specific basis (e.g., marketing by phone, mail, or email), then the aggregation service provider should honor the choices across *all* channels (unless explicitly directed otherwise by the end user). When the aggregation service provider and institutional account holder are not the same entity, these choices should be made available separately from the choices the end user may have made as an institutional account holder (financial institution) customer.

The following information-use guidelines are also recommended:

- Nonpublic personally identifiable information obtained by an aggregation service provider or institutional account holder at the direction of an end user should be shared by the aggregation service provider or the institutional account holder, according to its privacy policy standards and the choices the end user has made under that policy.

- An end user's request that an aggregation service provider obtain information about his or her accounts with an FI or initiate a transaction on his or her behalf constitutes customer authorization for the institutional account holder to share that information with the aggregation service provider or initiate the transaction. The aggregation service provider should be prepared to warrant that it has received the end user's authorization, such as by having authorization procedures that would limit the transaction to the customer.
- Any exchange of information among institutional account holders and aggregation service providers that results from an end user requesting or authorizing one party to perform specific actions/transactions on his or her behalf should be governed by explicit language included in the terms and conditions to which the end user agrees when initiating the relationship with that party.
- With further reference to the authority required in these transactions, each aggregation service provider should obtain approval from the end user (e.g., power of attorney in the end-user agreement) to act as the end user's agent and access nonpublic, personally identifiable information through the website of the end user's institutional account holder.
- The reuse (or secondary use) of information by an aggregation service provider or institutional account holder must be governed by the privacy policy and choice options of that institution, and the choices that the end user has selected, as well as applicable regulations.
- Information obtained by an aggregation service provider or institutional account holder about an end user in a manner not related to a specific transaction/action authorized by that end user must be used in accordance with that institution's stated privacy policy, the choices that the end user has selected, and all applicable regulations.

D. Consumer Tips

The following provides sample language for educating consumers who use aggregation services.

WHAT CONSUMERS SHOULD KNOW BEFORE ENTERING INTO AN AGGREGATION SERVICES AGREEMENT

Before providing your authentication information to a third-party site, you should understand:

- The terms and conditions of the account agreement.
- The features and functionality provided with the aggregation service.
- The account disclosures.
- How the aggregator safeguards your account passwords, PINs, and other secret information when you enroll in and terminate service with the aggregator.

You may be advised that in order to use the service you must do so “at your own risk.” This means X...

You should ask your aggregation provider about its PIN-sharing policy, understanding that:

- If you change your PIN at the aggregation site, you will also need to change it at the financial institution site.
- If you discontinue your aggregation service, you should change all your PINs at the financial institution sites.

Regarding your privacy and the use of your information, you should:

- Understand that the security measures used by your aggregator may be different from those used by your financial institutions.
- Know your rights if your account information has been compromised and whom to contact.
- Understand the security measures in place at the aggregation site to protect your information.
- Understand the privacy policies of your aggregator, financial institution and non-financial institution sites, as they may be different.
- You need to know what regulations are in effect to protect you such as Regulation E and FDIC insurance.
- Two core concepts in privacy are “notice” and “choice”.

The aggregation site’s Frequently Asked Questions (FAQs) may be a helpful guide for understanding these policies and practices.

You should review the aggregator’s disclaimer regarding the accuracy and completeness of information available through the service, including:

- The timing of updates and/or date and time stamp of balances and transactions.
- How timeliness of your account data affects your financial decisions.
- Service maintenance and down times.

You should know:

- Whether or not you will receive email messages from the sites that are being aggregated for you. If you will not receive messages, you may need to check with your original service provider site for any special notices or advertising offers, as applicable.

- That your aggregation provider may not “pass through” disclosures from your financial institution’s website, so you should check your financial institution’s websites periodically.
- The terms of service policy and procedures.
- How long the aggregator will maintain your information after you discontinue the service.



E. Security Tips for Online Financial Services Accounts

General Online Security Tips for Consumers

- Use a current browser that supports secure and private transactions.
- Install and regularly update antivirus software.
- Do not allow unauthorized access to your computer.
- Do not install pirated software or software from an unknown source.
- If using cable modems for Internet access, do not keep the connection active when not in use. Installing personal firewall software is recommended.
- Do not open email attachments from unknown sources.

Consumer Tips for Securing Online Financial Transactions

- Conduct financial transactions first in any online session. After completing financial transactions online, including a credit card purchase, log off before conducting other online activity. This may help to protect your confidential data (account numbers, passwords, etc.).
- Protect your PINs and passwords. Create alphanumeric PINs and passwords that do not use readily identifiable information like names, birth dates, phone numbers or other familiar words or numbers.
- When applying online for any financial account, ensure that you are dealing with a reputable, federally insured institution with secured Web pages.
- Learn about your financial institution's capabilities for secure online financial services. All online contact with the institution should be through its secured Web pages.
- Notify your financial institution immediately of any changes in your account information.

Examples of Ways Financial Institutions Continue to Secure their Online Environments

- Making security information easy to find on the institution's website through hotlinks or Frequently Asked Questions
- Educating end users and employees on security vulnerabilities and ways to create more secure online environments
- Using updated virus scanning software packages on all file servers and PCs
- Ensuring all network connections are properly secured
- Ensuring desktop modems used by employees are secured and properly registered
- Using real-time, inbound scanning systems for electronic mail and attachments
- Employing strong internal password processes and controlling password changes
- Masking end-user account number information from online banking screens
- Providing a timed logout feature on online banking sites
- Providing remote access security systems for employees and business partners that would dial in to corporate networks
- Conducting periodic tests of security from the viewpoint of someone trying to hack in
- Continuing to work to ensure the highest in industry security standards

V. LEGAL AND REGULATORY FRAMEWORK

A. Overview

The objectives of the Legal and Regulatory Framework subgroup are to:

- Identify legal and regulatory issues related to aggregation services.
- Analyze the issues from the standpoint of all parties involved in providing the services.
- Determine what steps need to be taken on any issue to clarify the impact on aggregation services.
- Prioritize issues in order of importance.

B. Matrix

The following matrix was created to address the questions most commonly asked by aggregators, FIs, and others providing—and potentially regulating—aggregation services.

AGGREGATOR MATRIX – SUMMARY OF LEGAL RESPONSIBILITY TO CONSUMER

DOES REGULATION E APPLY TO AGGREGATION ACTIVITIES?

Type of Institution	Screen Scraping, where account accessed is not held at aggregator (no EFT services)	Data Feed, where account accessed is not held at aggregator (no EFT services)	Where electronic fund transfers are performed (in addition to aggregation services)	Where aggregator holds consumer account
Financial institution	No*	No*	Regulation E applies unless the Federal Reserve Board concludes that aggregators are not covered by Reg E. ²	Yes
Non-financial institution	No*	No*		N/A (not permitted to hold accounts)

²Reg E does not apportion liability between two or more liable parties. Accordingly, where there is an agreement for EFT services in place with an aggregation service provider, both the account holding financial institution and the aggregation service provider may have Reg E liability. The consumer could choose to pursue either party for Reg E coverage. If Reg E liability exists, those two parties must determine between themselves, possibly through litigation, which party will be ultimately responsible/liable.

AGGREGATOR MATRIX – SUMMARY OF LEGAL RESPONSIBILITY TO CONSUMER

WHO IS RESPONSIBLE FOR THE ACCURACY OF DATA?

Type of Institution	Screen Scraping, where account accessed is not held at aggregator	Data Feed, where account accessed is not held at aggregator	Where electronic fund transfers are performed (from within the aggregation services)	Where aggregator holds consumer account
Financial institution	Responsibility could rest with either the aggregator or the account-holding FI, depending on the source of the error.	Responsibility for accuracy of data is allocated between aggregator and FI in data-feed agreement.	With screen scraping, responsibility could rest with either the aggregator or the account-holding FI, depending on the source of the error.	FI/Aggregator
Non-financial institution	The aggregator may attempt to disclaim liability in the user agreement.	The aggregator may attempt to disclaim liability in the user agreement.	With data-feed, responsibility for accuracy of data is allocated between aggregator and FI in data-feed agreement. The aggregator may attempt to disclaim liability in the user agreement.	N/A (not permitted to hold accounts)

Note: An entity’s ability to disclaim liability may be limited by Regulation E and the Electronic Fund Transfer Act (EFTA). Section 909(e) of EFTA provides that a consumer incurs no liability from an unauthorized electronic fund transfer except as provided in the consumer liability protection provision of that Act and Regulation E. In addition, Section 914 of the EFTA provides that “[n]o writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or cause of action created the [EFTA].” If Regulation E does not apply to the aggregation activities, then these statutory limitations should not apply to an aggregator’s disclaimers of responsibility or liability in its consumer agreements and disclosures.

AGGREGATOR MATRIX – SUMMARY OF LEGAL RESPONSIBILITY TO CONSUMER

IS THE AGGREGATOR REQUIRED TO COMPLY WITH THE PRIVACY PROTECTION LAW?

Type of Institution	Screen Scraping, where account accessed is not held at aggregator	Data Feed, where account accessed is not held at aggregator	Where electronic fund transfers are performed (in addition to aggregation services)	Where aggregator holds consumer account
Financial institution	Yes, Regulation P*	Yes, Regulation P*	Yes, Regulation P*	Yes, Regulation P*
Non-financial institution	Yes, FTC GLB rules**	Yes, FTC GLB rules**	Yes, FTC GLB rules**	N/A (not permitted to hold accounts)

*Regulation P is the name given by the Board of Governors of the Federal Reserve System (FRB) to its GLBA privacy regulation. Each of the other federal financial institution examining agencies (OCC, FDIC, OTS, NCUA) has enacted a privacy regulation that is substantially similar to Regulation P. The five federal financial institution regulators issued notices of proposed rule making to implement Fair Credit Reporting Act (FCRA) provisions regarding sharing of information among affiliated companies, attempting to conform FCRA practices to GLBA requirements. 65 FR 63120 (October 20, 2000) (OCC, OTS, FRB, FDIC; comments were due December 4, 2000); 65 FR 64168 (October 26, 2000) (NCUA; comments were due December 26, 2000). On March 27, 2001, FFIEC (to be confirmed) published an update advising financial institutions to publish their privacy notices in accordance with the privacy regulations and FCRA without delaying compliance until publication of a final FCRA rule. 66 FR 16624 (March 27, 2001).

**The FTC published an advance notice of proposed rulemaking and request for comment, including comment on “the range of financial institutions to which the [FTC’s Safeguards Rule under GLBA] should apply.” 65 FR 54186 (September 7, 2000). On October 6, 2000, the FTC extended the comment period. 65 FR 59766 (October 6, 2000). However, the rule remains a proposed rule without publication of a final rule or implementation date.

Citations for privacy regulations: FTC: 16 CFR Part 313 (65 FR 33646 (May 24, 2000)); FRB, FDIC, OTS, OCC: 12 CFR Parts 216, 332, 573, 40 (65 FR 35162 (June 1, 2000)); NCUA: 12 CFR Part 716 (65 FR 31722 (May 18, 2000)); SEC: 17 CFR Part 248 (65 FR 40334 (June 29, 2000)).

AGGREGATOR MATRIX – SUMMARY OF LEGAL RESPONSIBILITY TO CONSUMER

WHO HAS AUTHORITY TO EXAMINE THE AGGREGATOR?

Type of Institution	Screen Scraping, where account accessed is not held at aggregator	Data Feed, where account accessed is not held at aggregator	Where electronic fund transfers are performed (in addition to aggregation services)	Where aggregator holds consumer account
Financial institution	Federal Reserve Board (FRB) = State member banks and bank holding companies FDIC = State non-member banks (not members of the Federal Reserve System) OTS = Federal savings associations OCC = National banks NCUA = Federal credit unions SEC = Brokers or dealers States = State banks, thrifts, and credit unions; and insurance companies Each of these examiners visits each regulated entity regularly to review compliance.			
Non-financial institution	Federal Trade Commission = All others FTC has enforcement power but does not conduct regular or spot examinations to review compliance. State regulatory authorities (fraud, mini-FTC)			N/A
Non-financial institution acting as bank service provider	Federal Financial Institutions Examination Council (FFIEC)* under the Bank Service Corporation Act 12 USC. Sec. 1861 et. seq.			N/A

*The FFIEC is an umbrella organization through which the FRB, FDIC, OTS, OCC and NCUA seek to coordinate regulatory efforts.

AGGREGATOR MATRIX – SUMMARY OF LEGAL RESPONSIBILITY TO CONSUMER

WHAT IS A “FINANCIAL INSTITUTION”?

1. Traditional definition	A financial institution is an entity that holds accounts that are insured by the FDIC or NCUA. This is the narrowest definition.
2. Regulation E (Electronic Fund Transfer Act) definition	A financial institution is (1) traditional FI plus (2) any person that (a) directly or indirectly holds an account belonging to a consumer, or (b) issues an access device and agrees with a consumer to provide electronic fund transfer services.
3. Gramm-Leach-Bliley Act (GLBA) (privacy and security) definition	“Financial institution” is defined in the context of both “insured” and “uninsured” institutions. For insured institutions, section 509(3) of GLBA defines “financial institution” as “any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956” (Section 39(a) of the Federal Deposit Insurance Act, as indicated above). For uninsured institutions, 509 (3) of GLBA relies on the Federal Reserve’s administrative authority to define relevant parameters, i.e., “any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956.” The definition covers entities “significantly engaged” in such activities. “Financial activities” are broad, including providing financial information aggregation, as well as investment or economic advisory services, providing financial data processing and transmission services. This is meaningful for entities that have “consumers” or establish “customer relationships.”

VI. AGGREGATION AND SECURITY GUIDELINES

A. Overview

This section examines the security requirements imposed by law and regulatory guidance, with particular focus on the requirements imposed by Section 501 of the Gramm-Leach-Bliley Act (GLBA) on financial institutions engaged in aggregation activity.

B. Security of Certain Customer Data

A significant component of the GLBA legislation is the affirmative and continuing obligation for a “financial institution” to “respect the privacy of its customers.” As part of this privacy-related obligation, Congress explicitly includes a responsibility to *protect* certain data—namely the “*security and confidentiality of those customers’ nonpublic personal information.*” Specifically, Section 501(b) directs federal functional regulators to establish appropriate standards for the financial institutions, subject to their jurisdiction relating to administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information, which could result in substantial harm or inconvenience to any customer.

C. Security Guidelines

In accordance with this Congressional requirement, five of the federal functional regulators (Banking Agencies) issued preliminary and final guidelines implementing Section 501 security requirements (collectively the “security guidelines”): (1) Federal Reserve Board of Governors, (2) Federal Deposit Insurance Corporation, (3) Office of the Comptroller of the Currency, (4) Office of Thrift Supervision, and the (5) National Credit Union Administration.³ Although each of the Banking Agencies issues separate rules in the Code of Federal Regulations, similarities allow for several conclusions:

- The GLBA security guidelines include a range of risk-management obligations focused on implementing the congressional policy of protecting customer data. Most financial institutions are already required to adhere to similar practices, such as those required by the Bank Secrecy Act.
- The GLBA security guidelines are highly “process” oriented; that is, the rules require companies to develop and implement corporate governance philosophies, policies, and programs to secure customer data. In this sense, the GLBA security guidelines do not mandate specific standards or technologies that must be used to protect systems, business methods, or related processes for the delivery of financial services, such as aggregation. While implementing regulations generally do not provide specific standards, and there is no requirement to provide a description of technical information about the manner by which a financial institution safeguards information, implementing regulations do require disclosure of policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. Not all of the Banking Agencies agree on the issue of whether the GLBA security guidelines are voluntary or what penalties might be issued when financial institutions do not adhere to them.

D. Security Requirements and Other Financial and Non-Financial Regulators

³ *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Proposed Rule*, 65 Fed. Reg. 39472 (June 26, 2000) (“Notice of Guidelines Publication”); final rules published at 66 Fed. Reg. 8615-8641 (February 1, 2001).

In addition to the security guidelines issued by the five Banking Agencies listed above, the Securities and Exchange Commission (SEC) as well as the Federal Trade Commission (FTC) are required to issue rules for “financial institutions” under their jurisdiction.

- **The SEC** issued its final security requirement as part of the Privacy Rules promulgated under Section 504 of the GLBA. The SEC security requirements adopt the broad policy objectives as written in the Section 501 security requirements. The SEC requires that financial institutions under its jurisdiction implement “policies and procedures” in response to these policy objectives. The SEC does not delineate a series of risk-management practices and processes similar to the GLBA security guidelines published by the Banking Agencies. Rather, the SEC requires financial institutions under its jurisdiction to adopt policies and procedures “reasonably designed” to meet the policy objectives in the Section 501 security requirements.
- **The FTC** intends to issue its final safeguard rules for financial institutions not currently under the jurisdiction of the five Banking Agencies or any other agency or authority listed in Section 505(a)—which includes both federal and state authorities.
- To what extent will aggregation be captured under these regulations? The FTC final Safeguard Rules will apply to uninsured financial institutions, as defined by the Federal Reserve, and include any institution the business of which is engaging in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956. For uninsured financial institutions, the Federal Reserve has traditionally adopted a broad functional definition of “financial activity.” Aggregation service providers fall within the definition of “uninsured financial institutions.”
- If aggregation service providers fall within the scope of the FTC’s Safeguards Rules, how might aggregation service providers analyze possible differences between the Banking Agencies’ and the FTC Safeguards approach? Until the FTC issues its final Safeguard Rules, it is not possible to answer this question.
- Generally, banking regulators are aware of some of the security risks associated with aggregation. As noted in the Office of the Comptroller of the Currency’s guidance regarding Bank-Provided Aggregation Services (OCC Bulletin 2001-12), “[a] security breach could compromise numerous customer accounts. Because sensitive information is centralized, attackers may be more likely to target the aggregator’s systems. A bank acting as an aggregator should carefully consider its potential liabilities and assess whether it and its third-party providers have adequate security.” As well, the aggregation of certain information may invite regulation by other non-financial institution regulators. For example, the implementing regulations for protecting medical patient data published pursuant to the Health Insurance Portability and Accountability Act of 1996 include specific standards. See, e.g., Health Insurance Reform: Standards for Electronic Transactions, 45 CFR Parts 160 and 162 (Rule adopts specific standards for the electronic transfer of information in health care sector). See also Standards for Individually Identifiable Health Information, 64 Fed. Reg. 59918 (November 3, 1999), as amended 65 Fed. Reg. 427 (January 5, 2000). found at 63 FR 43245 through 43259. The rule requires that each covered entity (as now described in § 160.102) engaged in the electronic maintenance or transmission of health information pertaining to individuals assess potential risks and vulnerabilities to such information in its possession in electronic form, and develop, implement, and maintain appropriate security measures to protect that information.
- State law may affect the security requirements of financial and non-financial institution aggregators. For example, California Civil Code § 1798.82 and § 1798.29 (effective July 2003) require that businesses take additional measures to protect the privacy of California residents. In particular, businesses that (1) transact with California residents, and (2) own or license computerized data that contains the personal information of California customers, must notify those customers of any breaches of data security where the California customer’s unencrypted personal information was, or reasonably could have been, taken by an unauthorized person. Notice must be given in “the most expedient time possible and without unreasonable delay.” Whether such notice is required to be given by both financial institution and non-

financial institution aggregator is unclear. However, where possible, financial institutions should address notice, escalation and customer-impact issues in their agreements with aggregation service providers.

VII. PRIVACY AND INFORMATION USE

A. Overview

The goal in developing the Aggregation Privacy and Information Use Guidelines detailed below was to provide voluntary principles that recognize the impact of new information functionality and a more complex supplier environment, compared to traditional consumer financial services products. These guidelines are intended to be relevant to the aggregation services environment in the United States.

B. Assumptions

- All providers of financial aggregation services (whether or not the provider is a regulated financial services organization) should consider themselves to be financial institutions under Title 5 of the Gramm-Leach-Bliley Act (GLBA) and therefore subject to GLBA Regulation P, Regulation S-P, or FTC regulations, as appropriate. Additionally, to the extent that the Electronic Funds Transfer Act (EFTA) and the Fair Credit Reporting Act (FCRA) or other laws or elements of those laws are applicable to categories of institutions acting as an aggregation service provider, then all aggregation service provider program participants should agree to abide by those regulations, even in advance of a regulatory determination that they are in fact covered under such statutes.
- From a GLBA privacy regulation perspective, all consumers using aggregation services are considered to be customers (end users) of the aggregation service provider, as well as of the institutional account holders who maintain the underlying accounts.
- Different aggregation service providers and institutional account holders are likely to have different privacy policies, information-use practices, and marketing practices; and they may provide different customer choices.
- End users may be expected to make different choices regarding information sharing and marketing practices across their relationships with institutional account holders and aggregation service providers.
- Aggregation technology providers will be bound by the terms of contractual agreements with their customers and all applicable statutes and regulations. An aggregation technology provider should clearly indicate the circumstances under which it cannot be responsible for the behavior of an unaffiliated institutional account holder or aggregation service provider that violates the aggregation technology provider's privacy policy. Additionally, the aggregation technology provider cannot be responsible for an unaffiliated institutional account holder or aggregation service provider that maintains a poor privacy policy, or that violates its own policies.
- Aggregation service providers and institutional account holders should endorse and comply with privacy and information-use guidelines adopted by the financial services industry through industry organizations such as the American Bankers Association, America's Community Bankers, BITS, the Consumer Bankers Association, The Financial Services Roundtable, and the Independent Community Bankers of America.

C. Guidelines

Two core concepts to incorporate in protecting privacy require giving notice to participants of the information needed to make successful choices in interacting with the program, and then granting the power of choice among a variety of options. Below are elaborations on ways to include the concepts of "notice" and "choice."

Notice

Each aggregation service provider will:

- **Meet all applicable regulatory notice requirements**, e.g., FED, OCC, FTC, OTS, FDIC, SEC, states.
- **Provide privacy policies** (set by the aggregation service provider).
 - The policy should be no more than one click away (on toolbar or footer).
 - The policy should be written in clear, concise, customer-friendly language.

- The policy should indicate that the aggregation service provider’s privacy policy only applies to it, and that the end user should read the privacy policies of all the companies from which the end user’s information will be sourced.
 - When relevant, the policy should explain to end users that the aggregation service provider’s privacy policies *may* be different from the privacy policies relating to other, non-aggregation products within the same parent company.
 - The aggregation service provider’s notice shall be in full compliance with all applicable notification statutes or regulations and should be provided annually, whenever a new customer relationship is formed, and when there is material change to the privacy terms of an existing customer relationship.
 - The policy should be provided when the consumer subscribes to the aggregation service.
- **Provide disclosure for sharing of information.**
 - This disclosure should be part of the privacy policy.
 - The disclosure should be updated and explained any time a new service materially changes the use of information.
 - The disclosure should be updated and explained any time a privacy policy is materially changed.
 - Each aggregation service provider should disclose its policy for the length of time information is maintained by the aggregation service provider under normal circumstances, after an aggregation relationship is terminated by an end user, and in an instance where—for any reason—an aggregation service provider ceases operations and/or sells its business.
 - Each aggregation service provider should identify the possibility of differences between data on the aggregation service provider website and information simultaneously displayed by an institutional account holder website due to timing/processing considerations, etc.
 - **Provide security.** The aggregation service provider should comply with all regulatory requirements and should encourage adoption of the security guidelines contained in “Security, Technology and Standards.”

Choice

Where an aggregation service provider will use or share information for purposes other than providing the aggregation service and for other reasons listed as exceptions in GLBA, the aggregation service provider should describe the options it makes available to end users to provide or restrict information flow within and outside of the aggregation service provider’s family of companies. The aggregation service provider should make it convenient for end users to choose among those options.

Customer notice and options surrounding choice should comply with all relevant regulations, recognizing that certain state laws may supercede GLBA (and are subject to permissible exceptions under GLBA).

- The end user should be notified of any sharing by the aggregation service provider of nonpublic personally identifiable information with third parties.
- The end user should be given the option to opt-out of the sharing by the aggregation service provider of nonpublic personally identifiable information with third parties for marketing purposes. This choice should be available when the subscription begins and anytime that the aggregation service is being used.
- The end user should be notified of any sharing by the aggregation service provider of non-experience information with affiliates (as defined by the Fair Credit Reporting Act).
- The end user should be given the option to opt-out of the sharing by the aggregation service provider of non-experience information with affiliates (as defined by the Fair Credit Reporting Act).

If an aggregation service provider offers end users the opportunity to choose to participate in marketing programs (*not* a suggested guideline), and if those options are not specified on a channel-specific basis (e.g., marketing by phone, mail, or email), then the aggregation service provider should honor the choices across *all* channels (unless explicitly directed otherwise by the end user). If the aggregation service provider and institutional account holder are not the same entity, these choices should be made available separately from the choices end users may have made as institutional account holder (financial institution) customers.

Nonpublic personally identifiable information obtained by an aggregation service provider or an institutional account holder at the direction of an end user should be shared by the aggregation service provider or the institutional account holder, according to its privacy policy and the choices the end user has made under that policy.

An end user's request that an aggregation service provider obtain information about his or her accounts with a financial institution or initiate a transaction on his or her behalf constitutes customer authorization for the institutional account holder to share that information with the aggregation service provider or initiate the transaction. The aggregation service provider should be prepared to warrant that it has received the end user's authorization, such as by having authorization procedures that would limit the transaction to the customer.

Any exchange of information among institutional account holders and aggregation service providers that results from an end user requesting or authorizing one party to perform specific actions/transactions on his or her behalf should be governed by explicit language included in the terms and conditions language to which the end user agrees when initiating the relationship with that party.

With further reference to the authority required in these transactions, each aggregation service provider should obtain approval from the end user (e.g., power of attorney in the end-user agreement) to act as the end user's agent and access nonpublic personally identifiable information through the website of the end user's institutional account holder.

The reuse (or secondary use) of information by an aggregation service provider or institutional account holder must be governed by the privacy policy and choice options of that institution, and the choices the end user has selected, as well as applicable regulations.

Information obtained by an aggregation service provider or institutional account holder about an end user in a manner not related to a specific transaction/action authorized by that end user must be used in accordance with that institution's stated privacy policy, the choices that the end user has selected, and all applicable regulations.

VIII. LONGER-TERM SOLUTIONS FOR AGGREGATION SERVICES AUTHENTICATION

A. Overview

Four longer-term candidate solutions are discussed below:

- Aggregation service provider/third-party vendor ID and pass phrase
- Authentication token approach
- Distributed, certificate-based solution
- Centralized utility solution

Except for the first solution, aggregation service provider/third-party vendor ID and pass phrases, these solutions address both authentication issues, namely:

- Eliminating the need for end users to surrender primary authentication credentials (such as username and PIN) for the institutional account holder's site to the aggregation service provider and/or third-party vendor in order to allow the aggregation service provider/third-party vendor to access its account.
- Providing the institutional account holder with a practical and reliable way of tracking whether or not a particular access to an account was initiated directly by the end user who owns the account, or through an aggregator and, if through an aggregator, what the identity of this aggregation service provider/third-party vendor was.

B. Solutions

Aggregation Service Provider/Third-Party Vendor ID and Pass Phrase

This solution addresses only the need for an institutional account holder to track when an aggregation service provider/third-party vendor is accessing customer accounts on the customer's behalf, and does not address eliminating the need for end users to surrender their primary authentication credentials.

The aggregation service provider/third-party vendor is provided an ID and pass phrase. Either the aggregation service provider/third-party vendor selects an ID and pass phrase during registration, or, alternatively, the institutional account holder issues an ID and pass phrase to the aggregation service provider/third-party vendor. The institutional account holder should support one of the two options when employing aggregation service provider/third-party vendor IDs and pass phrases.

Before accessing an individual user's account, the aggregation service provider/third-party vendor navigates to an aggregation service provider/third-party vendor identification page provided by the institutional account holder for this purpose and signs on with the aggregation service provider/third-party vendor ID/pass phrase obtained during registration. The page URL is provided to the aggregation service provider/third-party vendor during registration.

The identification page should permit the entry of an aggregation service provider/third party vendor ID/password. On successful validation of the ID/password, the institutional account holder's application should redirect the aggregation service provider/third-party vendor to the end-user login page. The aggregation service provider/third-party vendor signs on with the end user's primary authentication credentials (i.e., user ID and pass phrase). If a valid user ID/pass phrase is provided, the session proceeds like a normal user session; however the institutional account holder is now in a position to associate the aggregation service provider/third-party vendor's ID with this session. A similar process could be used by an aggregation service provider/third-party vendor to identify another aggregation service provider/third-party vendor.

When accessing an online account on an institutional account holder's website with which the aggregation service provider/third-party vendor has previously registered and for whom the aggregation service provider/third-party vendor has obtained an aggregation service provider/third-party vendor ID/pass phrase, the aggregation service provider/third-party vendor shall access the account only after submitting this ID/pass phrase to the aggregation service provider/third-party vendor identification page.

The aggregation service provider/third-party vendor shall submit its ID to the identification page each time before a user's account is accessed.

In cases where an aggregation service provider/third-party vendor is not presented with the expected user login page after submitting the aggregation service provider ID/pass phrase, the aggregation service provider/third-party vendor should assume that an exceptional or error condition has occurred and should discontinue access to the login page until after the exceptional condition has been resolved.

Authentication Token Approach

This approach is based on authentication tokens, which an institutional account holder issues, given permission by the end user, and which permit a specific aggregation technology provider/third-party vendor to access that end user's account with a specific level of access rights. The use of authentication tokens is based on the following assumptions:

- Institutional account holders and their customers maintain a one-to-one direct relationship. In particular, when customers identify themselves to an institutional account holder's online presence, they use a mechanism defined by the institutional account holder (passwords, one-time pass-tokens, digital certificates, etc.) and submit authentication credentials established between the end user and the institutional account holder.
- The user's primary authentication credentials should not be given to third parties.
- To perform their services for their end users, aggregation technology providers/third-party vendors need online access to these users' accounts with institutional account holders.
- Customers should be given a high degree of control over which aggregation technology providers/third-party vendors have access to their account(s) with what level of access rights. Furthermore, customers should be given the ability to selectively revoke access to accounts that they had previously granted to a particular aggregation technology provider/third-party vendor.
- Institutional account holders require that for each access/transaction performed on their online presence, the identity of the aggregation technology provider/intermediary who facilitates the transaction is known.
- There are many institutional account holders and a significant number of aggregation service providers/third-party vendors in the market. It may not be possible for each institutional account holder to establish a separate relationship with each aggregation service provider/third-party vendor (in order to establish a means of identifying the third-party vendor and determine which level of access to grant). The token approach augmented by either the distributed, certificate-based, or the centralized-utility approach should address this scalability issue.
- A solution should be deployable in stages such that an initial deployment does not depend on any future infrastructure to be in place, other than protocol standards.

This broad approach has received the most attention in various industry forums. There are multiple efforts currently in progress, both within industry consortia and between various industry players, to leverage this approach to secure aggregation data transfers.

Most notably, the Financial Services Technology Consortium (FSTC) has explored multiple alternatives to use this approach. Most recently, the FSTC has explored how SAML and Liberty Alliance protocols may be leveraged in the aggregation scenarios. Previously, the FSTC membership also released a document on how the FAST

protocol utilizing standards such as SAML maybe leveraged in order to create a token based authentication system. Both of these reports are available on the FSTC website, www.fstc.org.

Generally, most of these efforts have focused on the issuance of a token by banks to aggregators upon user authorization. All further data access is done by verifying this token.

While these tokens and the business rules surrounding their management vary by protocol, generally the tokens should satisfy the following properties:

- **Uniqueness:** All tokens issued by an institutional account holder must be unique (within the institutional account holder).
- **Unpredictability:** Tokens must be chosen out of a large space in a sufficiently random manner such that the possibility of predicting a valid token is sufficiently small.
- **Opaqueness:** To protect the user's privacy, tokens should not contain any data from which user-specific information can be derived by a third party. If a token does include such data (such as user IDs, account numbers, etc.), these components should be encrypted under a strong algorithm and under a key only known to the institutional account holder.

Further, any proposed solution should be scalable to address large numbers of users and data-access requests. To meet this growth, the solution should be:

- **Scalable** to support thousands of services across thousands of institutions, to support millions of customers;
- **Dynamic** to automatically integrate the players into the solution without requiring distinct relationship negotiations; and
- **Flexible** to support any variety of institution, technology or end-user preferences.

Generally, to implement these solutions, an institutional account holder needs to provide:

- Back-end support for associating multiple sets of authentication credentials or other authorization tokens with the same account (possibly with different levels of permission);
- Back-end support for tracking aggregation service providers/third-party vendors and tokens issued to each of them;
- A UI component, which allows a user to grant access to a token;
- Support for above token-based access in the data-access mechanism (either via data feed or website); and
- Mechanisms to verify the validity of issued tokens to enable the previous step.

An aggregation service provider/third-party vendor needs to implement:

- UI support for handing off a user to the institutional account holder's site for granting access to a token; and
- Support for token-based sign-on to an institutional account holder's system for data access.

While the above are generally common characteristics of token based solutions, each solution will have further unique characteristics specific to that particular solution.

The varieties of solutions vary in the structure and format of tokens, their content, and the verification mechanisms employed. Verifying tokens involves:

- Identification of the token issuer;
- Identification of submitter of token for data access; and

- Checking of authorization that the token indicates.

The mutual identification steps mentioned above require prior business relationships to be in place, and sharing of a standardized way of securely identifying each other. This could be done by using a shared secret approach, where each party shares a secret with the other. However, this requires a bilateral key management relationship to be set up, in addition to creating a business relationship.

One alternative to this identification problem that eliminates the need for such large numbers of bilateral relationships is to use a trusted public certificate authority (CA), and sign using certificates issued by trusted public CAs. (This solution was referred to in the Phase I guidelines as the “Digital Certificate Solution.”)

Another alternative to avoiding this need for large numbers of bilateral relationships is to use a central utility service that is trusted or certified by a large number of FIs or other industry consortia. This utility effectively acts as the institutional account holder to the aggregation service providers and acts as the aggregation service provider to the institutional account holders. This reduces the number of business relationships that need to be set up to create an effective system.

A central financial network hub or utility may be needed to eliminate redundancy, establish an audit trail, and accommodate a larger number of entities and users. Such a utility should be able to read any variety of passwords from any variety of interfaces or devices for any variety of accounts and data, either from a repository or dynamically. Characteristics of such a utility might include:

- A user at an aggregator would name a bank account he or she wants accessed (same as above).
- To keep password information in as few hands as possible, the common hub would serve the page for the user to fill in the needed account and password information.
- The hub would forward this information to the bank and maintain a log for the bank of the source of the request any time it is called.
- The hub would maintain this information to build a profile of the user and all of his or her points of access and the accounts to which the person connects.
- This hub and its customer profiles would be a single connection source, in order to minimize the need for maintaining multiple points of connection for both the banks and the aggregators and to maintain a needed audit trail to negotiate security requirements or controls.

This approach would reduce the number of redundant user identities and passwords banks have to manage and create a common language and negotiation resource for security, tracking and accountability between multiple parties. Other benefits would include facilitation of:

- Standardizing legal and regulatory compliance requirements (i.e., EFTA, Regulation E, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Computer Fraud and Abuse Act) and applicable federal and state laws;
- Implementing and control opt-out applications;
- Defining account-holder information to be aggregated and in what format;
- Defining usage of aggregation information;
- Defining how this information will be secured and transmitted (i.e., single standard for data feeds) as well as timeliness of information being provided;
- Defining “privilege” of use of copyright/trademark materials by participating aggregators;
- Defining risk and liability of participating financial institutions and account holders (i.e., account holders’ Bill of Rights and Responsibilities);
- Defining arbitration resolution practices;

- Defining audit requirements and procedures for all aggregation participants;
- Standardizing account-holder education strategies, disclosures/agreements, communications and termination policies;
- Defining a single standard for data presentment to account holders;
- Defining archival requirements; and
- Defining and implementing third-party certification indicating industry best practices achievement.

Other Solutions

End users may eventually rely only on a single (or a small number of) universal password(s) that all businesses will support. In such circumstances, the need for an active intermediary step will be eliminated. A bio-identifier (fingerprint scan), personal hardware (smart card), or other yet unknown item could emerge to fill this role. Next steps would be to fully define these alternative solutions, evaluate and validate them through selective prototype and pilots, and then develop a specification and build a reference implementation for the recommended solution.

APPENDIX I

INDUSTRY ENCRYPTION STANDARDS

Key management is a critical function. Encryption keys, at a minimum, should be stored separately. Customer account keys should never be stored in the same instance as the aggregated customer data repository. Hardware-based key generation, storage, and encryption are recommended, especially for primary encryption keys. Cryptographic keying materials should be stored in a tamper-resistant security module (TRSM). The key-management process should include detailed instructions on archiving, storage, destruction, disaster recovery, inventory, key custodian identification, and exchange. The process should allow for compromised keys to be replaced (detection of equipment theft, improper keys), procedures for distribution, changing, and creating keys, and emergency procedures and log maintenance (creation, review and resolution of keys at every stage, from quality assurance to a production process.)

For the purposes of this document, the terms “public and widely-used or financial industry standards” shall refer to the following items, as specified within this document.

Symmetric encryption algorithms	3DES, IDEA, RC4, RC5, AES Candidate Finalists (minimum 128-bit key length)
Asymmetric algorithms	RSA, D-H (minimum 1024-bit modulus), ECDH
Digital signature algorithms	DSA, SHA-1, MD5, ECDSA
Key management standards and protocols	CMP, PKCS standard, IETF PKIX standards

In the event that criteria specify that “only” these standards be supported, “these standards” shall be interpreted to refer to those standards, algorithms, and protocols listed above, as well as other relevant standards approved by the following standards organizations: IETF, ANSI X9, ITU-T, and ISO.

APPENDIX II

BANKING AND BROKERAGE ACCOUNT HOLDINGS SUPPORTED BY AGGREGATION

Aggregation services should support the following banking and brokerage accounts and other holdings.

Ownership Types

Ownership Type	Description
Individual	Individual account holder
Corporate	Business account
JTTIC	Joint account, tenants in common
JTWROS	Joint account with rights of survivorship
Community property	Joint account community property
Joint by entirety	Joint account by entirety
Conservatorship	Similar to custodial account, but not for a minor
Custodial	Custodial for a minor

Bank Account Types

Bank Account Type	Description
Checking	Checking accounts
Savings	Savings accounts
CD	Deposit accounts
Money market	Money market accounts
Sweep	Sweep account
Loans	Auto and other consumer loans
Mortgages	Mortgage accounts
Credit card	Credit card accounts
Lines of credit (e.g. home equity, DDA overdraft protection)	Line of credit

Brokerage Account Types

Brokerage Account Type	Description
Money market	Money market account
Sweep	Money market account
IRA	Individual retirement account
Roth	Roth IRA
Roth conversion	Roth IRA converted from a traditional IRA
Rollover	Rollover IRA from a 401(k) or 403 (b)
Educational	Educational IRA
Simple	Simple IRA account
SEP	SEP IRA account (5305)
Keogh	Retirement account
SARSEP	Salary reduction simplified employee pension plan

401(a)	401(a) FICA plan
401(k)	401(k) retirement plan
403(b)	403(b) retirement plan
457/Deferred compensation	Deferred compensation plan
529 plan	529 educational plan (different than Coverdell)
Coverdell	Coverdell
ESOPP	Employee stock option/purchase plan
PSP	Employee profit-sharing plan
MPP	Money purchase plan
Stock basket	Stock basket account
Trust	Trust account
Living trust	Living trust
Revocable trust	Revocable trust
Irrevocable trust	Irrevocable trust
Charitable remainder	Charitable remainder trust
Charitable lead	Charitable lead trust
Charitable gift account	Special accounts for charitable giving
UTMA	Custodial for minor UTMA
UGMA	Custodial for minor UGMA
Annuity	Annuity account
Tax deferred annuity	Annuity account
Separate	Separate accounts

Security Types

The following types of holdings should be supported:

Treasury bond
 STRIP
 Treasury bill
 Brady bill
 Eurodollar bill
 Municipal bond
 Corporate bond
 Common stock
 Preferred stock
 Warrants
 Rights
 REITs
 ETFs
 REMICs (Real Estate Mortgage Conduit)
 Options
 Employee stock options
 Futures
 Commodity
 UITs (Unit investment trusts)
 Mutual funds
 Cash
 CDs

APPENDIX III

GLOSSARY OF TERMS

Aggregation service provider – The entity with which a customer contracts to provide the aggregation service. The aggregation service provider may be a traditional financial services company, a third-party technology provider, a portal, or another provider. As an aggregation service provider, however, the relationship with the end-user customer is direct, with no intermediary.

Aggregation technology provider – The entity that provides software, hardware, and/or other enabling capability to the aggregation service provider to allow delivery of the service. The aggregation service provider and the aggregation technology provider may be the same entity.

Central utility – An infrastructure component that, if developed, would deliver common services throughout the aggregation business system. These services might include such functionality as counterparty authentication or switch connectivity.

Customer – May be a consumer or a business (retail or institutional) that enters into an aggregation services relationship.

End user – The customer who has contracted directly with the aggregation service provider that provides the aggregation service. It can be a consumer, business, or an institutional account holder.

FAQs – Frequently asked questions.

Institutional account holder – The financial institution that holds the end user's account and is an information source for the aggregation service. An institutional account holder may also be an aggregation service provider.

Third-party vendor – The vendor providing the aggregation service.