

Managing the Risks of Data Aggregation

NORM BARBER AND JOEL LANZ

NORM BARBER is a technology risk consulting partner in the New York office of Arthur Andersen LLP. He is responsible for leading the eBusiness, security and IT infrastructure management services practice.

JOEL LANZ is a technology risk consulting partner in the New York office of Arthur Andersen LLP. He is responsible for leading the bank technology risk consulting practice.

We live in a world where the term 24/7 applies to just about everything in our lives. The Internet has brought both convenience and immediate access to consumers who are looking for better ways to keep track of their credit card balances, bank balances, investments—even their frequent flier miles. Now consumers are driving the need for convenience even further.

While many financial institutions provide customers with access to personal information through the Internet, consumers have been required to go to each Web site and enter unique information contained in identification numbers, PIN numbers, and passwords. If an individual needed a complete view of his or her finances, he or she often had to log into each account separately, retrieve the information, and then summarize it in an electronic spreadsheet or handwritten schedule. What was initially designed to be unlimited and easy access has turned into a challenge for Internet-savvy consumers.

Within the last 18 months a new business model called data aggregation services (sometimes referred to as screen scraping) has been introduced. Data aggregation services (DAS) allow the consumer to access one provider to collect this myriad of information. Once the object of lawsuits by financial institutions, DAS is now being embraced by these same organizations. This article explores the risks and rewards that financial institutions

may face with DAS, explains the reasons why many initially fought DAS and are now embracing the technology, and identifies the issues related to controls, laws, and regulations that the financial institution involved with DAS providers must address.

HOW DOES DATA AGGREGATION WORK?

A DAS is an Internet-based, third-party service that can be accessed electronically, normally through a Web site. The service stands between the consumer and the consumer's personal information that is stored in various databases of various financial and non-financial institutions. The DAS acts as a single-sign-on facility because the consumer only accesses the DAS. The DAS contains all the sign-on information for the customer's multiple Web sites.

An interesting and important point to understand is that, even when a financial institution offers the service, what is actually being provided is access to a DAS. For example, Chase (ChaseOnLinePlus) and Citigroup (MyCiti.com) are not offering their own DAS, but instead are providing access to Yodlee, a California-based DAS. There are also aggregation sites that have been created as a financial portal such as OnMoney that have chosen New York-based VericalOne for the data aggregation technology. These sites are not part of a traditional

EXHIBIT 1

Arthur Andersen eBusiness Risk Model™



financial institution. Whether via a co-branding approach where the DAS provides the look and feel of the partnering financial institution or a financial portal with its own service, a DAS stores access information (for example, log-on IDs, password, PINS), accesses the individual's data electronically, and stores the data accessed in the DAS database.

THE MECHANICS OF DATA AGGREGATION

There are basically two ways a DAS can obtain the consumer's data: through the back-office systems (direct link) or through the front-office systems (Web site on the Internet). To accomplish a direct link to the back-office system of the consumer's financial institutions, the DAS must have an agreement with the financial institution to

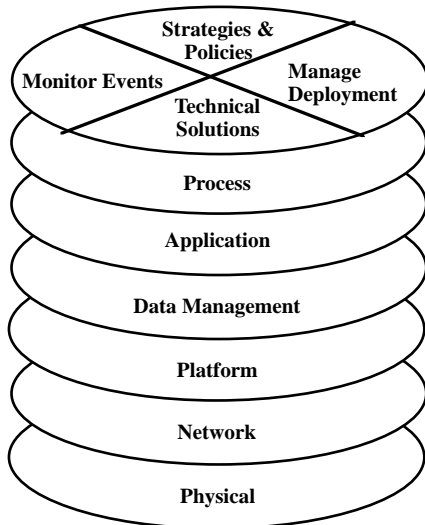
access the data through a direct connection using an agreed-to format. To obtain information through a Web site, the DAS must only have the customer's passwords.

A DAS stores access information, accesses the individual's data electronically, and stores the data accessed in the DAS database.

A common protocol for exchanging data for use in a DAS environment is the Open Financial Exchange, or OFX, a format developed through the efforts of CheckFree, Microsoft, and others. OFX is a standard for

EXHIBIT 2

Arthur Andersen Information Security Framework™



data formats in transmissions among businesses and financial institutions and is now being employed by DAS providers. For OFX to be used in the DAS business model in a direct link, all the parties involved must agree to the specifics of what can be exchanged and have permission to access the systems from which the data must be extracted. This permission for a DAS is not always forthcoming.

Because OFX or another direct access method is not always approved, the alternative method to obtain data for a DAS is to go through the front door, or Web site, through a method called screen scraping. In screen scraping, no permission is typically needed from the bank or brokerage house that stores the data. As noted above, the customer must store his or her password information with the DAS to use this approach.

HOW DOES SCREEN SCRAPING WORK?

Normally, when users go to a particular Web site, they either click on a link to the site or type in an address that normally starts with www and ends with .com. This is the address, or Universal Resource Locator (URL), that brings them to the site. They then move the cursor to some form of button that takes them to a secure login screen, or they may login on the initial screen. The login normally consists of a user ID and a password.

Once they complete the log-on procedure, a new Web page is usually returned to the browser through the

Internet indicating that they are free to navigate through the secure site now that has now authenticated. The path normally used to get to a user's personal information is called a navigation path. The navigation path differs from financial institution to financial institution and, even within a single financial institution, changes often as companies redo their Web sites for marketing or security reasons.

A DAS using screen scraping as the method to obtain the customer's data must virtually simulate the customer's keystrokes and mouse movements to obtain the data it uses. This method involves having the right URL to start with, knowing how to simulate the mouse movements and keystrokes to get to the password login screen, and entering the IDs and passwords in their proper locations. The DAS must simulate the navigation path. This is an ongoing maintenance process, particularly if the financial institution that stores the data is not in favor of having data accessed this way by a third party DAS.

The Initial Response to Screen Scraping

A number of financial institutions initially tried to block screen-scraping and direct-link agreements by DAS providers. For example, in December 1999 First Union filed a lawsuit against Secure Commerce Services, which provided the Paytrust Smartbalance feature. In February 2000, however, First Union dropped the suit; by April 2000, First Union had announced its own plan to provide a DAS for its customers.

By now, many leading financial institutions have jumped on the bandwagon of data aggregation and are announcing their own sites, often co-branded with a third-party DAS, or a relationship with a named DAS. While some may question the long-term viability of the DAS business model, for the present it is an eBusiness model that financial institutions must consider.

WHY FINANCIAL INSTITUTIONS PURSUE DATA AGGREGATION SERVICES

Financial institutions have given numerous reasons for pursuing the DAS strategies.

Helps Prevent Customers from Going Elsewhere

Although many businesses tend to resist strategies that are viewed as defensive in nature (preferring to implement proactive strategies to increase profitability), eco-

conomic reality has forced the issue in this case. By providing its own DAS service, the financial institution recognizes the customers' desire for such a service and is hoping to capture the customers before they go to other financial institutions or other DAS providers.

Get to Know the Customer Better for More Efficient Marketing

A DAS site may contain significant amounts of customer financial information (for example, checking, credit cards, mortgage, investments, insurance) as well as non-financial information (for example, frequent flyer miles and birthdays). Having a more complete picture of the customer enables the financial institution to recommend comprehensive financial planning solutions. For example, knowing the customer's net asset position and insurance profile may enable the financial institution to recommend estate-planning services. This could result in the financial institution providing high-margin wealth management services such as trust services (fees), cash value insurance products (high commissions), and asset management (fees). This also fosters a value-added long-term relationship with the customer that will increase the profitability of the customer relationship.

Reemphasizes the Financial Institution's Role as a Trusted Financial Service Provider

A question much on the mind of consumers is whether they can trust any aggregator with the completeness of the information included as part of the DAS process. It is this concern that provides financial institutions with an enormous opportunity to capitalize on the banking industry's reputation for confidentiality and trustworthiness over customer information. Due to the robust security and confidentiality programs that financial institutions have instituted over a long period of time, consumers appreciate the financial service industry's ability and capacity to properly mitigate consumer's fears.

Customers Have Many Reasons to Return to the Financial Institution's Web Site

Because all their financial (and, in some cases, non-financial) information is kept at the financial institution's Web site, customers frequently return to the financial institution Web site even if they are not conducting financial institution business. These repeat visits allow the

financial institution to profit from banner ads and other messages that are shown to visitors to the Web site.

Customers Are Willing to Pay for Consolidated Information

Numerous studies and various pricing experiments have indicated that customers are willing to pay for the ease and convenience of aggregated information. Because DAS services are renewed at a high rate, this service represents a customer-value-added opportunity that delivers steady streams of fee income to the financial institution's bottom line.

Establishes a New Channel for Identifying Potential Customers

Providing DAS services enables the financial institution to attract new visitors to its Web site and identify future customer opportunities. Citibank's recent introduction of MyCiti.com is an excellent example of how a financial institution can increase sales from both existing and new customers. As reported in a recent *Computerworld* article, "A month after New York-based Citibank launched its free online account DAS service, some positive results have begun filtering in. For example, half the users aren't Citibank customers... Even though it isn't generating any revenue from the site, Citibank plans to use MyCiti.com to cross-sell mutual funds and other products to its existing customers and market those services to noncustomers." ("Citibank's Aggregator Portal a Big Draw," *Computerworld* [Sept. 18,2000]: 40.)

Partner, Rather than Compete, with Aggregator

Last winter, bankers exhibited much apprehension toward aggregators. First Union's concerns with screen scrapers were typical of the concerns that bankers have in protecting their franchise and the confidentiality of their customers' interests. Today, the approach is different. Aggregators such as Yodlee are now partnering with financial institutions to enable the latter to enhance service and revenues. As described in a recent *US Banker* article, "Since June, all of the nation's biggest banks and brokerages—and many smaller ones—have either announced deals, or are striking deals, to offer account DAS services of their of their own." ("Aggregator, Aggravation," *US*

Banker [October 2000].) By partnering with technology enablers (for example, aggregators) such as Yodlee instead of fighting them, banks are enhancing their customer satisfaction and retention levels. A lot changes in a year.

Aggregators are now partnering with financial institutions to enable the latter to enhance service and revenues.

Blocks Out New Technology Players

With the new partnerships described above, a strong DAS presence may limit the ability of new technology companies to repeat the successes of the early aggregators. Newer technology developments, such as the OFX standard, require that financial institutions provide permission to aggregators to enable the aggregator to obtain data from the financial institution's site. Leveraging this standard, financial institutions can establish rules with which they expect aggregators to comply. For example, First Union established a number of rules for aggregators that required, among other things, that aggregators protect customer's authentication data, allow First Union to identify and track aggregator activities, and protect the confidentiality and security of customer data. These types of rules, established by the financial institution, enable First Union to continue to comply with various laws and banking regulations. ("Web Aggregators Pros & Cons for Banks," *Bank Systems and Technology* [April 2000].)

Facilitates CRM and e-CRM Initiatives

Given the various opportunities offered by DAS, it is not surprising that the latter would facilitate customer relationship management (CRM) and e-CRM initiatives. Earlier CRM initiatives focused on customer retention by effectively identifying customer needs and comparing those needs to existing products or services provided by the institution and, in some cases, offering a personalized product to satisfy the customer needs. E-CRM focuses on the "challenge of integrating web-specific customer delivery channels with older, more traditional bricks-and-mortar delivery channels." ("Financial Firms Grapple with e-CRM, an Evolving Concept,"

Wall Street and Technology [July 2000]: 18.) By aggregating the customer's financial data, the financial institution is in a better position to identify relevant needs and acquire or enhance customer relationships.

Ensures Industrywide Efforts and Cooperation

By embracing the DAS technologies, the industry is in a better position to ensure that technology-based companies are held to the same consumer protection standards as financial institutions. These objectives are being accomplished through lobbying efforts in Congress and with the Federal and state banking regulators and through efforts by the Bank Industry Technology Secretariat to establish voluntary industry guidelines. In these matters the banking industry appears to be cooperating in developing responsible approaches to satisfying the consumer demand and consumer concerns with respect to these services. Thus, it is hoped that all of the players in the financial services industry will be bound by the same rules and standards.

WHAT FINANCIAL INSTITUTIONS DON'T LIKE ABOUT DATA AGGREGATION SERVICES

While there are numerous positive implications to initiating a DAS, bankers have expressed a number of concerns with the new services.

Accessing Customer Information Without the Bank's Permission

Given traditional industry concerns over customer confidentiality and protection of customer data and given the recent explosion in privacy concerns, it should come as no surprise that banks would be very concerned about any third party accessing its customer information without the bank's knowledge. In fact, this concern was paramount in bank's earlier threats and suits against screen scrapers and other data aggregators. These concerns relate not only to threats against a bank's reputation but also to potential legal action if the bank were to be found negligent in protecting the data.

Erosion of Brand Name and Loss of Control of Web Experience

By no longer having to visit a unique bank's Web site to obtain or process seemingly proprietary financial infor-

mation, aggregators put banks at risk of becoming commodities dealers. Using current technology, the aggregator could bring competitive products and pricing information to the attention of the bank's customer. Because the interactive relationship shifts to the aggregator, the customer's loyalty may also shift to the aggregator and away from any particular bank. Also, as customers gain confidence in the aggregator, they may be more likely to consider and act on the competitive offers and information that the aggregator brings to them. Aggregators can actually differentiate themselves through the type and quality of these opportunities and offers.

Uncertainty Over Disputes

As with any new product or development, new issues or uncertainties arise. What happens if a customer loses money as a result of using an aggregator? If the customer has furnished an aggregator with IDs and passwords, and the customer suffers a loss either through this information being mishandled or through a transaction initiated by the aggregator, who is liable? Does the bank have liability to the customer? Does the aggregator have responsibilities to the customer or to the bank? How are disputes between the parties resolved when the parties are not subject to an agreement? What is the impact on the bank's regulatory compliance program and privacy initiatives? While answers to these questions are critical to banks and consumers, such answers do not currently exist.

Increase in Infrastructure Expense

Whether a bank does or does not support DAS efforts, there are infrastructure expenses. Banks actively involved in DAS efforts must be able to support the additional customer information that will be acquired through the system. The information must be accessible and protected. The network must be designed to accommodate additional customer and bank employee requests. For banks that choose not to participate in the DAS technology, systems must be developed to identify DAS related activities. As banks prepare to comply with the expanded privacy rules necessitated by the passage of the Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLB) and ever-expanding state privacy rules, new systems must be designed to include concerns raised by the DAS technologies. For some banks, the technology costs may be justified as a part of a larger strategy; for other banks, the technology costs may prove to be a significant burden.

Impact on Privacy Initiatives

As noted above, a major challenge facing the financial services industry today is the burgeoning privacy initiatives related to the implementation of GLB and various state privacy initiatives. Questions arise as to a bank's legal responsibility if the bank's systems are not adequate to discern and monitor DAS activities and if those activities are at odds with their customers' representations to the bank concerning the handling of private information maintained by the bank.

Know Your Customer

In a reverse twist on the increased knowledge to be gained from having more information available on their customers, some bankers are concerned that the regulators may require them to use the increased knowledge to better analyze their customers' transactions for regulatory compliance. Such concerns arise in part from the controversy surrounding the know-your-customer initiatives previously proposed by the regulators.

Lack of Technology to Detect and Control Access

Another concern of bankers is the lack of technology tools to monitor and detect DAS activity. If aggregators access their sites, bankers want to be in a position to identify that a DAS activity has occurred, who performed the DAS, and what activities were performed.

MEASURING THE RISK

Financial institutions that are considering offering a DAS need to carefully analyze a number of risks. Using two of Arthur Andersen's risk models, namely the eBusiness Risk Model™ and the Information Security Framework™, a number of specific risks emerge as key challenges. The steps that a bank must consider in their analysis of the risks are outlined below.

DAS Vendor Information Technology Processes and Procedures

- Discuss the information technology (IT) policies of the data aggregation service, review for completeness and alignment with regulatory guidance, best practices, and corresponding procedures and organization structure.

- Identify and review the privacy policy regarding user account information.
- Verify service level agreements are quantifiable and a management-reporting mechanism exists and is functioning properly.

Regulatory Risk

- Identify the subsidiaries and products that will interface with the data aggregation process.
- Understand the data aggregation process flow and identify banking-related regulatory risks associated with such processes.

System Development and Change Management

- Review to ensure that the controls are designed to prevent ad hoc or unauthorized changes to the systems environment, including application, database, or network and security configuration changes.
- Verify that appropriate management approvals are obtained and recorded for major branding/functional changes. Sample a number of changes to review proper sign-off.
- Review how screen-scraping procedures/functionality are updated at the DAS, subsequent to any changes to the bank Web site.
- Verify that well-defined phases of development exist and are segregated appropriately (for example, development, testing, quality assurance).
- Identify system-level controls for auditing and logging (that is, tracking accountability) of changes.
- Verify that coordination occurs between security administration and operations management for all significant system changes.

Data Integrity and Protection

- Verify and review the location of user account and password information. Review how account information is segregated from other content partner account information. Verify how account information is stored within the database.
- Discuss and review the aggregation procedures for data transfer from content partner systems (for example, your systems) to the web-based dis-

semination system (for example, DAS). Identify completeness, integrity, and security controls.

Detailed Data Storage and Encryption

- Verify that access to content partner data is appropriately segregated and controlled within the database(s). Review data storage procedures, for example, length of time data is stored, who is allowed to access data on site.
- Identify database encryption controls for user IDs, password, client account numbers, client account balances, and Social Security numbers.
- Identify and review the validity of user IDs defined to the database.

Security Administration and Operations

- Review current policies and processes for granting, updating, and removing user IDs and passwords, including those for system administrators, DAS users, system developers, and portal business partners.
- Identify how DAS system testers are granted access to production servers and data.
- Identify any business continuity planning issues.

OTHER REGULATORY ISSUES: AN ACTUAL RISK ASSESSMENT

Using the eBusiness Risk Model™ and the Information Security Framework™, Arthur Andersen recently conducted a risk assessment of a leading DAS. The assessment identified a number of potential regulatory issues, in addition to the operations and security risks noted above, that any financial institution should consider if a DAS capability is being considered.

Gramm-Leach-Bliley and Related SEC Rules

As a result of the GLBA, the Securities and Exchange Commission implemented Privacy of Consumer Financial Information final rule (Regulation S-P), which became effective on November 13, 2000. Compliance becomes mandatory on July 1, 2001. The purpose of this regulation is to place restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. This review focused on Federal regulations and did not encompass state laws.

The final rule requires financial institutions to restrict the use of information among third party nonaffiliated companies. These restrictions can be limited if the financial institution adequately describes its practices in a notice to the customer and allows the customer the right to opt out of such practices.

With this particular DAS, the vendor reserved the right to use the information collected and would not allow the use of the product if consumers were given and had exercised a right to opt out of information-sharing practices. As a result, this could lead to any of the following situations:

- The financial institution could potentially be in noncompliance with Regulation S-P. Under Regulation S-P, financial institution third-party nonaffiliates are prohibited from using information that is derived from nonpublic personal information unless the consumer was notified of the information sharing practices and given the right to opt out.
- A financial institution's privacy policy with respect to the data aggregation services may not adequately state how nonpublic personal information is collected and disclosed.

In addition, the particular DAS stated that it was not certain how information collected was going to be used. It was also not clear that a process had been created to require the DAS to obtain approval from the financial institution on how it modified the data collected. Under Regulation S-P, financial institutions are required to revise and redisclose to consumers as additional data collection and disclosing strategies develop. In addition, the redisclosure is required to provide the customer with a new opportunity to opt out.

Electronic Funds Transfer Act

The Electronic Fund Transfer Act (EFTA) was enacted on November 10, 1978. The EFTA provides a basic framework for establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer (EFT) systems. Its primary objective is the protection of individual consumer rights in their dealings with these systems.

It appears that in certain instances a DAS would be required to have controls to ensure compliance with the EFTA. As a result of some confusion in the industry on the responsibility of the EFTA, the Federal Reserve Board asked for feedback regarding specific issues involving data aggregators and EFTA in June 2000. The comment period expired in August 2000; to date, the Federal Reserve has not issued new regulatory interpretations.

Although it could be interpreted that a DAS is required to comply with the EFTA, this particular DAS indicated that it would not accept any responsibility. Before proceeding with a DAS, a review should be conducted to assess training, procedures, disclosures, and controls to ensure compliance is adequate with respect to the EFTA.

A RISK-BASED APPROACH TO DATA AGGREGATION

Data aggregation services have the potential to dramatically improve consumer convenience related to providing one-stop shopping for financial information. As financial institutions continue to embrace the DAS concept, a risk-based approach should be adopted to ensure that all the critical risks have been identified and risk-mitigating strategies are developed in a disciplined and structured manner.