NEWS RELEASE

Comptroller of the Currency
Administrator of National Banks

NR 2001-39

FOR IMMEDIATE RELEASE

Contact: Robert Garsson
(202) 874-5770

Remarks by
Julie L. Williams
1st Senior Deputy Comptroller and Chief Counsel
Office of the Comptroller of the Currency
Before the
American Banker's
2nd Account Aggregation Conference
"The Impact of Aggregation on the Financial Services Industry"
Tysons Corner, Virginia
April 23, 2001

I am going to talk this morning about issues and challenges that banking organizations face in providing account aggregation services. Technology innovations, such as aggregation, make possible today the creation, transfer and manipulation of information in ways we didn't even dream of 10 years ago. Because the financial industry is fundamentally information-based and driven, advances in technology have had and will continue to have a profound affect on financial services and particularly on the evolution of the banking business. Aggregation services are a perfect illustration of both the promise and the new challenges that technology present for the banking industry.

First I'll describe how account aggregation services are a manifestation of a fundamental change in how financial products and services are being created and delivered. Then, viewed from that context, I'll highlight two issues that will be key to successful provision of account aggregation services by banking organizations: (1) management and oversight of relationships with third parties that perform aggregation functions on behalf of the organization, and (2) fulfilling the organization's responsibilities for protecting customer privacy.

To begin, it is important to recognize that account aggregation is an example of a broader phenomenon that I call "deconstruction," which is occurring throughout the financial industry. By "deconstruction," I mean the process of separating or segmenting the components or attributes of a product or an activity.

Today, we see this process permeating the entire business of banking and finance. Deconstruction of the banking business means the separation or segmentation of products, services, operations and *information* into component parts or processes so they can be provided or obtained separately. A deconstructed perspective permits an organization to analyze the

components of the business it does -- or wants to do -- what it does well, and where it may have a particular advantage in conducting an activity or providing a product. This, in turn, provides new options for firms to decide what activities to conduct themselves and how best to use third party providers and services.

Technology has vastly enhanced the ability of banking organizations to deconstruct and segment their business. In some respects, technology also enables highly advanced deconstruction of activities or information that results in the creation of entirely new products or services. On the flip side, from the perspective of banking organizations, technology also enables nonbanks to deconstruct functions or activities traditionally performed by banks and cherry-pick portions of those functions. It also makes possible *involuntary* deconstruction of a bank's activities and *information*, as in the case of account aggregation initiated by *customers* of the bank.

Account Aggregation As An Example of "Deconstruction" of Financial Functions and Activities

Account aggregation exemplifies two dimensions of deconstruction: First, account aggregation is a service banking organizations typically provide under the bank's brand name. But the product offering has actually been deconstructed because, behind the scenes, the aggregation function actually is being performed by a third party service provider. Second, as I noted above, aggregation represents deconstruction of information -- and, from the perspective of the possessor of the information, the deconstruction may be *involuntary*. Here, technology enables a customer to authorize an aggregator to access and replicate the customer's information in the possession of another source, effectively depriving that source institution of control over its own information about is own customers. The information is then reconstructed to form a new product offered by the aggregator -- the account aggregation service -- built with the information components from source institutions, but presented with a new look and new functionality.

Early reactions by the banking industry to aggregation services were characterized by fears of disintermediation, concerns regarding the integrity of bank web sites, and the uncertain legal, liability and security ramifications of how aggregated information was being obtained and used. These concerns were magnified by the involuntary nature of how banks' customer information was being deconstructed when aggregators compiled information from web sites through screen scraping. Not only did the source institution lose control of its confidential customer information, but it might not even know that its information had been deconstructed -- "scraped" -- much less what was being done with it.

Now, banking organizations increasingly have recognized the importance of being the *aggregator* rather than the *aggregated*. Not only does account aggregation provide a new level of convenience to the online customer, but it has the potential to deepen a bank's relationship with its customers by providing access to a more complete financial picture of them. Banks may find opportunities to assist customers in strengthening their financial portfolios by suggesting appropriate products, or they may find occasions to market products on more competitive terms than other financial products or services the customer may already have.

The value to a banking organization of providing its online customers with account aggregation services is highlighted by a recent survey by Booz, Allen & Hamilton. The survey found that nearly half of those individuals who aggregated their accounts at nonfinancial institutions spent less time at the web sites of the financial institutions where they had their actual accounts. These findings suggest that banks could lose important opportunities and face some risk of being relegated to mere data providers if they do not make account aggregation available to customers who are in the market for such services. Put starkly, the choice for banking organizations may be to aggregate, or be aggregated.

So, where does account aggregation fit in a deconstructed banking world? Aggregation services demonstrate both how deconstruction has enabled competitors to challenge traditional banking functions -- mainly the management of customer account information -- and conversely, how banks have been able to respond to the competition by capitalizing on their strengths. While others, such as Internet service providers and Internet portals may have been first out of the box to offer aggregation services, banking organizations appear well-positioned to exploit their core competencies -- their reputation as trusted repositories, their existing customer base, their experience in data processing and information management, and their financial expertise -- to be successful in providing these services.

But, while account aggregation presents new opportunities, it also poses substantial challenges for banking organizations that offer the service. In fact, account aggregation exemplifies two of the most important challenges for facing modern financial service providers: (1) management and oversight of relationships with third parties that perform aggregation functions on behalf of the organization, and (2) fulfilling the organization's responsibilities for protecting customer privacy. I will address each of these issues in turn.

Management and Oversight of Third Party Relationships

Typically, banks have opted to use third parties to perform the aggregation functions the bank offers to its customers. The aggregation service provider may serve as a prime contractor, specializing in gathering, storing, protecting, and presenting information to the customer. The third-party service provider, in turn, may further outsource some of the aggregation service features, such as bill payment, to other specialists. Yet, to the end user -- the bank customer -- the aggregation service is seamless. When the bank customer logs onto the aggregation web site, the customer sees only the bank's brand name. The use of a third party to provide the functions behind account aggregation may be completely invisible to the customer.

In an era of deconstructed financial services, banking firms have the opportunity to exploit their advantages by offering aggregation services to their customers -- their reputation, their existing customer base, and their expertise in handling customer financial information -- with the assistance of third parties that provide the requisite technology. The use of third parties also allows a bank to provide aggregation services to its customers without making major capital expenditures to develop and maintain the technology.

But, when banking organizations deconstruct the function of providing aggregation services and rely on third parties to provide the technology that supports the service, they must address the risks of outsourcing these functions. The OCC recently issued a Bulletin detailing these considerations,[1] and the Federal Financial Institutions Examination Council also issued guidance on the risks associated with outsourcing technology. This guidance was included in a recent OCC Advisory Letter.[2]

As discussed in the guidance, responsible management of third party relationships typically requires four essential elements: (1) understanding the risks associated with the outsourcing arrangement; (2) exercising due diligence in selecting the service provider; (3) ensuring that written contracts address key risk factors associated with the activity; and (4) overseeing performance by the service provider.

Let's look at each of these factors as they apply to banking organizations using third party aggregators.

Risk assessment: The board of directors and senior management of an organization relying on third parties to perform functions on its behalf should fully understand the risks associated with each outsourcing arrangement and ensure that practices are in place to address those risks. Outsourcing aggregation services will involve risks that are similar to those that a bank would face if it performed these services directly, as well as some additional risks. For instance, because aggregation involves the manipulation and transfer of confidential data over the Internet, as well as the collection of customers' passwords, there are clearly risks associated with the security and privacy of customer information. Further, because aggregation relies on data transmissions from various web sites, there are risks with respect to the integrity and accuracy, and currency of the data that ultimately reaches the customer.

To the extent that third party aggregators facilitate transactions, there is the additional risk of unauthorized or disputed transactions and the resulting liability. While these risks would be present if a bank provided the aggregation services directly, banks must consider the additional risks associated with the use of third parties, such as the third party's financial stability, the reliability of the service provided by the third party, and the possibility that the third party may develop or market services in ways that are not compatible with the bank's goals or reputation.

Due diligence: Banking organizations must exercise due diligence in the selection of third party service providers. Among other things, that involves assessing the service provider's competence or expertise in offering the service, the extent to which the servicer relies on other third parties to provide the service, the effectiveness of the third party's internal controls, and its financial condition.

---

[1] OCC Bulletin 2001-12, "Bank-Provided Account Aggregation Services," February 26, 2001.

[2] OCC Advisory Letter 2000-12, "Risk Management of Outsourced Technology Services," November 28, 2000.

A paramount concern for a bank selecting a third party aggregator should be the aggregator's ability to safeguard the bank's customer information. In this regard, banks should familiarize themselves with the banking agencies' final guidelines on the safeguarding of confidential customer information, issued in February. These interagency guidelines -- referred to as the "501(b) guidelines" after the section in the Gramm-Leach-Bliley Act that required the agencies to issue them -- require banks to exercise due diligence in selecting service providers, have in place contractual provisions that address how the third party will safeguard customer information, and provide for appropriate oversight of the third party.

To satisfy the due diligence requirements under the 501(b) guidelines, banks should generally review the measures each service provider takes to protect customer information, even when the information is in the hands of a subservicer.

Contract provisions: A bank's contract with a third party aggregator should address both business requirements and key risk factors. Again, a key risk inherent in aggregation services is security, and therefore a bank's contract should address the aggregator's program for safeguarding bank customer information in accordance with the 501(b) guidelines. Because the guidelines afford third parties flexibility in designing their own security programs, a servicer's program may differ from that of the bank on whose behalf the servicer is processing customer information.

Oversight: When a banking organization relies on a third party service provider, it should implement an oversight program that, among other things, monitors the third party's financial condition and reviews compliance with the contract. The 501(b) guidelines also require banks to exercise an appropriate level of oversight over a service provider to confirm that the provider is actually implementing its security program. A bank need only monitor outsourcing arrangements if such oversight is indicated by the bank's own risk assessment. As a result, not every outsourcing arrangement between a bank and a third party will be subject to ongoing oversight. However, due to the extremely sensitive nature of the activity third party aggregators perform, the relative newness of the service, and the at least partially unregulated status of some aggregators, banks should consider this a high risk area warranting thorough oversight.

Responsibilities for Protecting Customer Privacy

The successful resolution of issues surrounding security and privacy of customer information will be essential to widespread customer acceptance of account aggregation. Yet, the essence of aggregation -- a concentration of nonpublic customer financial information from various sources at one source -- increases the magnitude of privacy issues that may arise, and the consequences if something goes wrong. Given the extent of the information held, lapses in security, or breaches in privacy of customers' aggregated financial information, could be devastating.

There are enough privacy issues presented by account aggregation to compose an entire speech on that subject, but I will focus on two key regulatory issues. Then, I'll conclude by discussing why its important for banking organizations to think about privacy in terms of

customer expectations, rather than simply compliance with rules and regulations. These two points are inextricably linked.

As I am sure you are aware, banking organizations and financial services firms that provide aggregation services are subject to privacy regulations that implement the privacy provisions of the Gramm-Leach-Bliley Act. Two essential features of that Act and the new rules, which will become effective this July 1st, are (1) the requirement that institutions provide notice of their privacy policies and practices to their customers, and (2) the prohibition on disclosure of customers' nonpublic personal information to unaffiliated third parties unless the institution has first provided customers with notice of the type of disclosure the institution may make, and the type of parties to whom the information may be disclosed, and has given its customers an opportunity to "opt-out" of having their information disclosed in that manner.

From the perspective of banking organizations that offer aggregation services, this means privacy policies must adequately and accurately reflect the types of information collected as part of the aggregation service. The point to watch here is that the privacy policy and privacy notices a banking organization provides to customers of *its financial products* probably would not address the broader types of information it receives when aggregating information from other sources on behalf of a customer of its aggregation services. Thus, banking organizations need to ensure that their privacy policies and notices are sufficient to encompass the scope of information they may receive as account aggregators, or else consider separate privacy policies tailored to their aggregation customers.

A more complex regulatory issue is presented by the interaction of the basic customer notice and opt-out features of the privacy rules and the reuse and redisclosure limits of the rules. Most of the information a banking organization will collect in connection with performing aggregation services will come from other financial institutions, which are also subject to the privacy rules. These rules include provisions that limit the ability of a bank, or any other entity for that matter, that receives nonpublic personal information about a customer from a financial institution, to subsequently use or disclose that information.

Where, as here, an aggregating bank receives information about a customer from another financial institution so that the bank may provide the aggregation service, in general, the reuse/redisclosure limits would provide that the aggregating bank may only use that information or disclose it to third parties as needed to perform the aggregation service. In other words, the aggregating bank may not sell the information for marketing purposes, and may not use the information for its own purposes if that exceeds the scope of the aggregation service.

Now, you may be thinking that I just told you about the basic provisions of the privacy rule requiring notice to customers of an institution's privacy policies, disclosure of the types of information collected, and the ability of a firm to share customers' nonpublic personal information with third parties, subject to the customer's opportunity to opt-out. What if a banking organization's privacy policies appropriately describe the breadth of information it may collect in performing account aggregation, and indicate that such information may be used or shared for certain purposes -- and an aggregation customer does not opt-out of that information

sharing? Which prevails, the reuse/redisclosure limitations that apply to information obtained from the source financial institution, or the bank's ability to disclose the information freely since its aggregation customer has declined to exercise his or her opt-out right?

The answer is not clear from the regulations, and that brings me to my final point. This issue is a perfect example of why it is important to think about privacy issues that arise in connection with aggregation services in terms of customer expectations, rather than simply compliance with rules and regulations.

Given uncertainty in this area and the sensitivity of the customer information at issue, institutions would be wise to fully explain in their agreements with customers the precise nature of the services they intend to perform in conjunction with aggregating the customer's information. Obtaining a customer's informed consent to any specific information sharing practices the bank contemplates may well be deemed to be within the scope of and consistent with the aggregation services, and thus would not run afoul of the limits on reuse and redisclosure.

A "no surprises" approach is clearly in order for customer relationships concerning aggregation services. Account aggregation is still in its early stages but clearly holds tremendous promise. The activities involved offer potential for new dimensions in customer convenience and enhancement of customer relationships, but they are based on functions -- transfer and manipulation of sensitive customer information -- that also hold the potential for significant backlash if breaches in security or customer privacy abuses occur.

Not long ago, consumer privacy in the financial services arena was governed largely by self-regulatory approaches. Remember what prompted the GLBA privacy legislation? Learn a lesson from that experience. Go the extra mile to make sure customer interests are respected and protected.

Account aggregation provides new opportunities for banks to serve their customers, indeed, being an *aggregator* rather than being *aggregated* may become a business imperative. The industry's key challenge is to offer these services in a way that capitalizes on, and preserves, a hallmark of banking organizations -- their reputation as trusted protectors of consumers' most valued assets.

Thank you very much.

# # #