OCC 2001–12

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Bank-Provided Account Aggregation Services

Description: Guidance to Banks

TO: Chief Executive Officers and Chief Information Technology Officers of National Banks, Federal Branches, and Service Providers; Department and Division Heads, and Examining Personnel.

PURPOSE

This bulletin discusses the risks of bank-provided account aggregation services, and suggests control mechanisms banks should consider when they offer aggregation services.

KEY POINTS

- Aggregation services may provide banks with an opportunity to expand and deepen their customer relationships by leveraging their position as trusted financial intermediaries.
- Aggregation business models and services are evolving, as are the underlying legal and operational structures. That evolution accentuates strategic, reputation, transaction, and compliance-related risks.
- Key controls involve security, compliance, vendor management, data gathering and use, contracting, and customer education, disclosures, and service.
- Banks should implement risk management controls to safeguard customer information, to select and monitor vendors, to comply with legal and regulatory requirements, and to educate and disclose information to customers.
- Banks that provide aggregation services should establish procedures to monitor market and regulatory developments to keep pace with changing requirements.

BACKGROUND

Account aggregation is a service that gathers information from many Web sites and presents that information in a consolidated format to the customer. The information gathered can range from publicly available information to personal account information (*e.g.,* credit card, brokerage, and banking data). Typically, the aggregator obtains the personal account information by using customer-provided usernames and passwords to enter Web sites. Emerging capabilities include offering customers the ability to initiate transactions, obtain financial advice, and use shopping services to scan the Web for products. Many experts believe banks that provide aggregation

services have the opportunity to deepen their customer relationships by leveraging their position as trusted financial intermediaries.

Typically, a bank provides an aggregation service under its brand name through a third-party service provider. That service provider serves as a prime contractor, specializing in gathering, storing, protecting, and presenting information to the customer. The third-party service provider, in turn, may outsource some of its features, such as bill payment, to other specialists. The bank or third-party service provider also may provide or outsource software that analyzes customer behavior and suggests financial products for that customer. Aggregated financial information often comes from other Web sites, the owners of which may not be aware that they are providing content, and thus lack contracts or agreements with the aggregating bank or service provider.

TABLE OF CONTENTS

RISKS

Banks that offer aggregation services ("aggregator banks") typically are exposed to the following risks.

Strategic Risk. Because aggregation is at an early stage of development and customer acceptance is low, banks should consider how evolving standards and customer acceptance for aggregation services may affect electronic banking strategies. Further, reliance on third-party service providers introduces strategic risks that banks should consider. For example, some third-party service providers may be financially unstable or unable to provide reliable service. Others may develop or market services in ways that are incompatible with the bank's goals. Further, some arrangements, such as co-branding, may make it more difficult to change providers, if problems arise.

Reputation Risk. The viability of aggregation services depends heavily on meeting customer expectations, including availability, confidentiality, data integrity, and overall service quality. Moreover, as customer acceptance grows, customers are likely to expect aggregator banks to innovate and provide additional services. Failure to meet customer expectations (whether

provided by the bank or a third-party provider) can undermine customer confidence and trust. This could hinder the bank's ability to retain existing customers and to offer other electronic banking products and services in the future.

Transaction Risk. Aggregation relies on data transmission from various Web sites through the aggregator's Web site to the end customer's Internet browser. If the integrity of the data is compromised or if the data is not current, the customer could receive erroneous or dated information, which could adversely affect customer decision making. Timely and correct information is especially important in environments where purchases, sales, and asset transfers take place.

Information security is critical because aggregators centralize the storage of usernames and passwords that provide access to other Web sites, as well as personally identifiable customer information from many other Web sites. 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.

Inadequate authentication measures may expose aggregator banks to liability if these inadequate authentication measures weaken the security of other Web sites. Because both the aggregator and the customer typically enter the target Web site using the same username and password, the target Web site may not be able to identify the true system user (*i.e.,* customer or aggregator), diminishing the effectiveness of its access controls and record keeping. Additionally, entry to the target Web site may be gained automatically at the aggregator's Web site, effectively bypassing some of the target Web site's protections against fraud and theft of authentication devices.

Aggregators that receive and facilitate transactions have the additional risk of liability for unauthorized or disputed transactions. In situations where a dispute arises after an aggregator communicates a request from the customer to another Web site, the aggregator may need to trace the transaction. If the aggregator could not prove the customer originated the transaction and could not demonstrate that the transaction was transmitted correctly, the aggregator might be held liable.

Gathering information from other Web sites also presents risks. In some cases, aggregators may be blocked from gaining access to information from target Web sites. For example, target Web sites may change the location of information on a Web page or change passwords. Additionally, the target Web sites may have data integrity problems that they report on their Web page. This information may not be captured by the aggregator's information collection mechanisms and reported to the bank's customers. Such situations may result in failing to meet customer expectations and may result in inaccurate or incomplete information. Another challenge facing aggregators is the interpretation and accurate presentation of the data gathered from other Web sites. For example, aggregators may discover similarly named data elements have different definitions. An incorrect presentation of data could result in customer confusion and incorrect decisions.

Compliance Risk. Aggregation services raise three key compliance risks issues: the application of Regulation E, asset management, and privacy.

Regulation E. In aggregating customer information, banks should closely monitor regulatory changes in the application of Regulation E. Currently Regulation E, which implements the Electronic Fund Transfer Act, does not specifically address the responsibilities of aggregators. The Federal Reserve Board requested comments on this issue in June 2000. In the absence of guidance, bank management should be conservative when interpreting possible Regulation E compliance obligations in connection with aggregation services.

Aggregators that also provide electronic fund transfer services could come within the current coverage of Regulation E in two ways. If the aggregator is a bank, and holds consumer accounts in the bank, the aggregator is covered by Regulation E when it agrees with the consumer to provide electronic fund transfer services to or from the account. Aggregator banks that do not hold the consumer's account could also fall within the coverage of Regulation E. An aggregator bank may be covered if it issues a card, PIN, or other access device to the consumer and agrees to provide electronic fund transfer services with respect to accounts at other institutions. If the aggregator bank does not have an agreement with these other institutions concerning the electronic fund transfer services, a special set of rules under Regulation E for "service providers" will apply.

Banks and aggregation service providers should consider the possibility that providing customers with an automatic log-in feature to conduct electronic fund transfers on other entities' Web sites could trigger the application of Regulation E. The automatic log-in feature allows customers to click a hyperlink and thereby cause the usernames and passwords stored at the aggregator to be used to log into other Web sites. Banks that provide this feature might be considered to offer, in essence, an access device for electronic fund transfer services.

Entities that provide aggregation services subject to Regulation E must ensure that proper disclosures are given to customers (12 CFR Part 205). Further, banks that contract with third parties to offer these services should be careful to ensure compliance with Regulation E.

Banks that provide their customers with usernames and passwords for electronic banking should be aware of possible exposure to liability under Regulation E. The potential exposure arises when their customer shares those usernames and passwords with an aggregator. If an attacker then steals the usernames and passwords from the aggregator and performs unauthorized transactions, it is unclear under the current regulation which party would bear responsibility for an unauthorized transfer.

Asset Management. Aggregator banks that compile customers' asset management information should be aware of the various requirements that may apply. Asset management encompasses a broad range of activities, such as trust and fiduciary services, retail brokerage, and financial planning, where investment advice is provided for a fee or commission. In particular, banks aggregating clients' account information should ensure compliance with the Bank Secrecy Act, and, depending on the nature of the services provided in connection with aggregation of account information, applicable fiduciary standards imposed pursuant to 12 CFR Part 9 and the

Employee Retirement Income Security Act of 1974 (ERISA), and other applicable law, regulation, and policy.

In addition to aggregating account information, aggregator banks may provide links to affiliated and unaffiliated third-party Web sites that allow consumers to buy securities and insurance products directly. In these instances, banks should clearly distinguish on their Web sites between products and services that are offered by the bank and those offered by third parties. In general, the bank should indicate that it does not provide, endorse, or guarantee any of the products or services available through the third-party Web pages. For bank Web pages that provide links to third-party pages that enable bank customers to open accounts or initiate transactions for nondeposit investment products, the disclosures also should alert customers to risks associated with those products (*e.g.,* by stating that the products are not insured by the FDIC, are not a deposit, and may lose value).

Banks' aggregation services also may provide analytic engines or other automated tools for customers to use in making financial decisions, including information necessary to the decision-making process. These tools and accompanying information should be offered in a way that clearly defines any responsibility by the bank in the decision-making process. Also, banks may offer aggregation services that allow consumers to initiate transactions at the bank's Web site based on information provided. To the extent that a bank is engaged in the business of effecting transactions in securities for the account of others, the bank should consult applicable federal securities laws and regulations. In particular, effective May 12, 2001, banks will no longer have a blanket exemption from the definition of broker under the federal securities laws. Banks will only be exempt from registration with the Securities and Exchange Commission as a broker if their activities are within various exceptions found in 15 USC 78c(a)(4).

Privacy. Banks that provide aggregation services should be aware of various legal provisions protecting the confidentiality of consumer information that affect aggregation activities. It is critical that banks understand the application of the privacy provisions of the Gramm–Leach–Bliley Act (GLBA) and requirements of the Fair Credit Reporting Act (FCRA) to the consumer information they collect. Banks are strongly advised to evaluate the requirements of both laws in connection with the disclosure of consumer information received in connection with providing aggregation services. It is important to note that compliance with one statute will not guarantee compliance with the other. Beyond these legal requirements, moreover, banks are strongly encouraged to proceed carefully before disclosing consumer information acquired in connection with aggregation services for any purposes other than providing the aggregation services sought by the customer. Given the extent and sensitivity of the information about a customer that a bank may obtain in connection with providing an aggregation service, banks should recognize the significant reputation risks that may arise if the bank discloses that information for another purpose.

By July 1, 2001, banks are required to comply fully with the regulations that implement the privacy provisions of the GLBA, including providing their customers with notice of their privacy policies and an opportunity to opt out of their information sharing with nonaffiliated third parties. See OCC Bulletin 2000-21: Privacy of Consumer Financial Information–Final Rule (June 20, 2000). A bank that provides aggregation services should ensure that its privacy policy

accurately reflects the categories of information that it collects and discloses in its aggregator role, which may differ from the types of information that the bank collects and discloses with respect to customers of its own banking products or services. Given that a bank that offers aggregation services may have access to a customer's entire financial portfolio, the bank may need separate notices for its aggregation customers in order to permit these customers to make an informed decision about the bank's privacy policies and practices. For instance, while the sample clauses in the appendix to the privacy regulations generally provide acceptable disclosures in connection with a credit relationship between a bank and a consumer, those examples may not adequately reflect the array of information in an aggregator's possession that may pertain to the customer's entire financial portfolio.

Banks also should be aware of the possible application of FCRA to the sharing of information collected through aggregation activities. Under FCRA, a bank may freely disclose to other parties its own transaction or experience information that bears on consumers' creditworthiness, personal characteristics, or mode of living. However, the sharing of information—to affiliates or other unrelated third parties—that does not relate to a bank's own transactions and experiences may trigger the requirements of FCRA.

Thus, if an aggregator discloses to nonaffiliated third parties consumer information it has compiled from other financial institutions, such as deposit account information, the aggregator could be considered a consumer reporting agency under certain circumstances, even if the aggregator has received a consumer's consent for such disclosures. Consumer reporting agencies are subject to a variety of requirements under FCRA. Additionally, aggregators that share such information with their affiliates could be considered consumer reporting agencies under certain circumstances, unless they comply with FCRA's notice and opt-out provisions.

Even if a bank determines that it may legally disclose customer information, because of the sensitive nature and amount of information that a bank collects on its customers in connection with aggregation, the bank should carefully consider the risks, such as reputation risk, of any disclosure of information beyond that which is necessary to provide the aggregation services. For instance, in addition to specific information about investments, insurance coverage, and credit account transactions, an aggregator will likely have its customers' passwords to these various accounts. Given that a bank's success in providing aggregation services depends in large part on maintaining a high level of trust by its customers, any disclosure of information to third parties that undermines that trust would not be consistent with safe and sound banking practices.

CONTROLS

Aggregator banks should establish appropriate risk management controls, including procedures to monitor developments and ensure they remain in compliance with legal and regulatory requirements. Bank management should apply the risk management process outlined in prior OCC guidance.[1]

[1]See OCC Bulletin 2001-08: Guidelines Establishing Standards for Safeguarding Customer Information (February 15, 2001), OCC Advisory Letter 2000-12: Risk Management of Outsourced Technology Services (November 28, 2000), OCC Bulletin 2000-25: Privacy Rules and Regulations (September 8, 2000), OCC Bulletin 2000-14:

Security. Security controls can mitigate reputation, transaction, and compliance risks. Management should safeguard its information systems as outlined in other OCC guidance and as part of this effort monitor and adopt appropriate industry standards and assess the sensitivity of information in making security decisions.

Authentication and Verification. Authentication and verification of bank customers are particularly important. Since aggregators typically offer their customers the equivalent of a single sign-on for many Web sites, the bank should employ authentication techniques, policies and practices that do not weaken the other Web sites' authentication mechanisms. Authentication of the aggregation service to other Web sites can enhance audit trails and improve the integrity of the information delivery mechanism. Bank management should consider using an authentication device that uniquely identifies the bank's service to the other Web sites. Additionally, management should consider the circumstances under which the bank verifies the customer's identity before initiating aggregation services or resetting the aggregation service's authentication mechanisms. Identification assists in protecting nonpublic personal information from disclosure to unauthorized parties.

Regulation E. Banks should be aware that for electronic fund transfers covered by Regulation E, consumers' liability for unauthorized transfers is generally quite limited. It is, therefore, imperative that banks design adequate security systems for access devices, and maintain the security of usernames and passwords used to access other Web sites, such as those of other financial institutions. This caution applies whenever usernames and passwords are stored, even when the aggregator does not use them to initiate transactions.

Record keeping. When expanding services from information gathering to the initiation of transactions, management should consider whether its aggregation processes are sufficiently robust to address issues relating to the validity of transactions, such as attribution and non-repudiation. Those processes go beyond security measures and encompass coordination of record keeping with other Web sites. That coordination should be sufficient to enable the tracing of a transaction from the customer through the bank to the other Web sites, with reasonable controls to protect against unauthorized changes to the transaction. Good records can improve a bank's position in the event of disputes. Record keeping requirements should be based upon the level of activity and risk.

Compliance. Banks that offer aggregation services should implement effective controls for managing the associated risks and complying with legal and policy requirements. Customer disclosures should be effective in averting potential customer confusion about the bank's roles and responsibilities and the nature of risks associated with the products or services offered.

Vendor Management. Most aggregation business models rely on vendors and subcontractors for the delivery of critical services. Vendor management controls can mitigate strategic, reputation, transaction, and compliance risks. Banks offering aggregation services through third-party service providers should evaluate security and business continuity issues from the point of

---

Infrastructure Threats-Intrusion Risks (May 15, 2000), OCC Bulletin 98-38: PC Banking (August 24, 1998), and OCC Bulletin 98-3: Technology Risk Management (February 4, 1998).

contact with the customer through the third-party service providers and the bank. The evaluations should address external and internal threats, controls that are critical to the overall security of the service, and necessary actions to correct weaknesses found in the evaluations. Management should ensure that the scope, content, and time period covered by the evaluations are sufficient to satisfy the bank's needs.

Data Gathering. Aggregators obtain information from restricted Web sites either by using the same method of requesting information employed by the customer, or by entering into direct data feed arrangements. Data feed arrangements frequently reduce transaction risk by implementing technologies that are more reliable and traceable than other data-gathering techniques. The OCC encourages the use of data feed arrangements where practical.

Contracts. Appropriate contracting can mitigate strategic, reputation, transaction, and compliance risks. Management should seek to control and manage these risks by structuring arrangements between the bank and the involved parties. Standardized contracts and the development and use of industry standards can facilitate those arrangements.

Contracting will primarily involve the bank, the bank's customer, and the aggregation technology provider. Customer agreements should specify the scope of the aggregating bank's authority to use the customers' passwords and other authenticators on their behalf. Moreover, customers should be advised of the degree of responsibility the bank assumes for the timeliness or accuracy of the information obtained from other Web sites.

The bank's contracts with technology providers should ensure the provided activities conform to applicable legal and policy standards, and should acknowledge the OCC's authority to examine and regulate the provided activities under 12 USC 1867(c). The contract should clearly disclose and authorize the roles and responsibilities of the bank and the technology provider. Contracts also should cover security requirements and reporting, performance reporting, data usage restrictions, indemnification arrangements, data retention policies, business continuation arrangements, and submission of financial statements.

To the extent that agreements with other Web sites are practical, those agreements should consider addressing: 1) system security applicable to the acquired data and authentication information; 2) the use of customer information; 3) the timing and method of data access; 4) the methods for verifying aggregator authority to access data on behalf of the consumer (including the authentication and authorization procedures used to verify the identity of account holders); 5) the need for transaction logs of specific consumer instructions for the aggregator; 6) the responsibility for the timeliness and accuracy of information to be provided; and 7) the responsibility for delivery of disclosures and consumer notifications.

Customer Education, Disclosures, and Service. Realistic customer expectations about such matters as data timeliness and completeness, support, and service levels can reduce reputation and transaction risk. Banks should use customer education and disclosures to manage those risks. For instance, transaction risks relating to data definitions and timing can be controlled by clearly disclosing when the aggregated information was obtained from the other Web sites, and any material changes in the definition of data elements. Banks should consider how best to direct

customers to those customer service areas, whether at the bank, technology provider, or operator of another Web site, that can most directly and effectively help resolve customer issues. Lack of a complaint mechanism or unclear directions to customers may precipitate customer dissatisfaction and increase reputation risk. Banks should also be aware that the Web sites from which information is aggregated may post disclosures that belong with the aggregated information. Management should consider whether and how to notify their customers of those disclosures.

RESPONSIBLE OFFICE

Questions regarding this banking issuance should be directed to Clifford A. Wilke, director, Bank Technology Division, (202) 874–5920 or via e-mail: clifford.wilke@occ.treas.gov.

_____
Clifford A. Wilke
Director
Bank Technology Division