2001

If You Can't Beat Them, Join Them: Dara Aggregators and Financial Institutions

Kimberly L. Wierzel

Follow this and additional works at: http://scholarship.law.unc.edu/ncbi

Part of the Banking and Finance Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncbi/vol5/iss1/17

This Comments is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Banking Institute by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
If You Can’t Beat Them, Join Them: Data Aggregators and Financial Institutions

I. INTRODUCTION:

Data aggregation has been a hot topic in the financial industry since First Union’s December 1999 suit against Secure Commerce Services.¹ Data aggregation is the process of gathering information from multiple websites and delivering it to a consumer on a single website.² There are essentially two ways for an aggregator to gather information—direct feed and screen scraping.³ Both methods require a customer to create on-line account access with the institutions they want on their single website.⁴ The customer then turns over their account numbers, I.D. numbers and passwords to their selected aggregator.⁵

¹ First Union Alleges Online Payment Service Used Bank Customers’ Information Illegally, B.N.A., Feb. 1, 2000, at 2437 (citing First Union Corp v. Secure Com. Serv., Inc., No. 3:99CV519H (W.D.N.C. filed Dec. 30, 1999)). Secure Commerce Services, Inc., headquartered in Princeton, New Jersey, lets customers see their bank account information and pay their bills through its Paytrust website. Carol Power, First Union Confirms It Is Suing a ‘Screen Scraper,’ AM. BANKER, Jan. 19, 2000, at 5. The company gathers customers’ financial information directly from the websites of other companies at the request of its customers. Id.


³ Star Systems, Inc., Web Aggregation White Paper (Aug. 2000), at http://www.star-system.com/news-corpsearch.html, at 1 (last visited Feb. 20, 2001) [hereinafter Star Survey]. Star Systems, Inc. commissioned SWR Worldwide (SWR) to conduct a survey of online consumers to gauge knowledge and awareness of web aggregation services. Id. at 26. Between June 26 and July 17, 2000, SWR did an online survey of 705 consumers nationwide who had previously expressed an interest in online banking. Id. Respondents were invited by e-mail to visit the SWR web site to take the survey; each respondent was granted a one-time access to the survey. Id. The survey has an overall margin of error of 3.7% at a 95% confidence level. Id.

⁴ See Vartanian & Ledig, supra note 2.

⁵ See id.
Direct feed involves an agreement between the aggregator and the originating financial institution where the institution transmits the account information to the aggregator, who then makes the information available to the account holder on the aggregator’s web site. Unfortunately, direct data feed access by the aggregators places a huge demand on a financial institution’s computer system, which could have a harmful effect on the system’s speed and possibly cause a system to crash. On the positive side, direct data feeds involve an added level of security, such as authentication and data encryption, and so the feeds are less subject to fraud than screen scraping.

The second method, screen scraping, was the method that originally alarmed First Union. This method of aggregation does not require an agreement between the aggregator and the financial institution. Because the screen-scraping aggregator has all of the information an actual account holder would have, it gains access to the same screen of data that the true account holder would see and is electronically indistinguishable from the account holder. Other

---

6. Star Survey, supra note 3, at 4. Open Financial Exchange, based on the widely accepted computer standard XML (extensible markup language) is the most common communication protocol used by financial institutions and third party aggregators. Id. That standard may change. See infra notes 134–35 and accompanying text.

7. Star Survey, supra note 3, at 9; Lauren Bielski, Aggregators—AKA “Screenscrapers,” A.B.A. BANKING J., May 2000, at 47. Currently, the population of web aggregation at any given institution is not great enough for this to be a real concern. Star Survey, supra note 3, at 9. Additionally, many direct feeds are now done in batches overnight when demand on computer systems is relatively low. Id. at 9-10. Direct feeds done overnight, however, seem to have the same drawbacks involved with stale information a screen scraping method might have. See infra notes 138-143 and accompanying text. Nevertheless, as the number of aggregation customers grows into the millions and more customers require up to the minute account information, the demand that direct feeds place on financial institutions’ computer systems is expected to explode. Id. at 10.

8. See First Union Alleges Online Payment Service Used Bank Customers’ Information Illegally, supra note 1. Paradoxically, direct feeds may entail greater liability to participating financial institutions than does screen-scraping precisely because accessing data with direct feed requires their full knowledge and cooperation. Star Survey, supra note 3, at 10.


10. Star Survey, supra note 3, at 5.

11. Id. It is hard, if not impossible, to tell who is signed on—the customer, an aggregator, or a thief with the customer’s name and password. Miriam Leuchter, Aggregation Aggravation, U.S. BANKER, Oct. 2000, at 32.
risks associated with outside screen scraping include the potential security risk created when user names, account numbers and passwords are stored on the aggregator's servers. In addition, the screen scraping aggregator's visit to a bank's web site may overload the institution's hardware, leading to delays and performance issues. Problems also arise when a financial institution changes the design of its web site or screen. The design changes often make it difficult for the screen-scraping software to locate specific data—raising problems with inaccurate or incomplete data.

In First Union's December 1999 suit, the complaint alleged that Paytrust, a screen-scraping website, illegally lifted customer information off its website. First Union specifically alleged that Paytrust "secretly accessed the First Union Website... misrepresented its relationship with the bank, violated trademark and copyright law, and misled customers on the safety of their information, among other charges." The parties settled the suit in March 2000, but many of the security concerns involved in

---

12. Jerry Minkoff, Banking: Banks Face Loss of Customers to Account Aggregators, WEB FIN., Apr. 10, 2000, 2000 WL 4044340. When asked who the consumer thought would be responsible if someone gained unauthorized access to their information and omitted fraud, 75% said they thought the third-party Internet company offering the web aggregation service would be responsible. Star Survey, supra note 3.


14. Id. at 9. In many instances, aggregators collect account data once a day, meaning the information available at their web sites is updated only once every twenty-four hours. Id.

15. First Union Alleges Online Payment Service Used Bank Customers' Information Illegally, supra note 1, at 2437. In December 1999, First Union also announced requirements for aggregator companies in an effort to address customer and privacy concerns. First Union Announces Internet Requirements for Aggregator Companies in an Effort to Address Customer Service and Privacy Concerns, at http://personalfinance.firstunion.com/pf/press/item/0,2907,228,00.html (last visited Oct. 30, 2000). The requirements include: that First Union be able to identify and track aggregated transactions on its website; aggregators can only make inquiries, not initiate transactions on behalf of First Union customers; aggregators must sign a binding contractual agreement to consolidate the information in a way that protects its confidential nature; aggregators must provide end-to-end audit trails at the system and transactional level; and, aggregators must agree to adhere to privacy standards. Ross Snel, First Union Lays Down Guidelines for 'Screen Scrapers' Culling Its Site, AM. BANKER, Jan. 12, 2000, at 1.

aggregation still linger—especially regulatory oversight. According to Gayle Wellborn of First Union, "[n]on-financial companies don’t have the same regulatory oversight (as banks)."

Days before announcing it was dropping the suit, First Union announced: "We support aggregation. We want to be aggregators, but we want to be sure that we do it in a way that safeguards our customers." In the year following First Union’s suit much has changed in the industry. First Union plans to introduce an account aggregation service driven by Yodlee, Inc. in the second half of 2001.

First Union is not alone among financial institutions in its warming relationship with screen scraping. In July 2000, Citigroup, Inc. launched its aggregation site, myciti.com using Paytrust data aggregation technology. Customers and non-customers can view accounts they hold with any institution at myciti.com and can aggregate their e-mail and frequent flier miles at the site. In October 2000, Citibank also became one of the first

---

18. Id. (quoting Gayle F. Wellborn, director of customer advocacy with First Union).
19. Jessica Toonkel, First Union Yields to Screen Scraping, AM. BANKER, Apr. 13, 2000 (quoting Kellie Scott, First Union Senior Vice President and e-Channels Director).
20. Yodlee.com is a privately held technology company based in Sunnyvale, CA. Founded in 1999, it has already emerged as one of the biggest players in account aggregation. John Hackett, Domesticating Account Aggregators, BANK TECH. NEWS, Oct. 2000, at 1.
22. Carol Power, Citi Advances in Online Payments, Aggregation, AM. BANKER, Jul. 19, 2000 [hereinafter Power, Citi Advances]. As part of the online payment program, Citigroup pays AOL for every new customer it signs through AOL’s portal. Id. Myciti.com has already attracted fifty thousand customers, 11% of whom are new to Citigroup. Carol Power, Citi Deploys Its Web Troops Into Business Lines, AM. BANKER, Dec. 1, 2000, at 1 [hereinafter Power, Citi Deploys].
23. Power, Citi Advances, supra note 22; Power, Citi Deploys, supra note 22, at 1. As part of its cross-selling efforts, the site also offers one-stop shopping for Citigroup products, including Citibank banking, loans, mortgages, and credit cards; Salomon Smith Barney brokerage and investment products; and Travelers insurance products. Id. It also offers financial calculators and, among other things, enables customers to work out repayments on car loans. Id.
banking companies to offer online bill presentment. Chase Manhattan Bank has chosen an alternate route by only allowing Chase customers to access its aggregation site. Centura Banks, Inc. uses VerticalOne Corp to offer aggregation. Centura Snapshot offers to “bring together all of your accounts - including credit cards, investments, checking and savings, bills, travel rewards and email - together on one convenient, secure page with one security key to remember.”

The original data aggregation services provided by Internet companies like Yodlee or Corillian have mostly become the supporting technology for aggregators, whether those aggregators are banks, portals or investment firms. Moreover, in a sign that the industry is surely maturing, Yodlee and VerticalOne Corp, a subsidiary of rival S1 CORP, are merging. The merged entity will aggregate about 1.5 million accounts from 425,000 customers; it

---

24. Carol Power, Citi Jumps into Online Bill Presentment, AM. BANKER, Oct. 16, 2000 at 1. Many banks have Internet based programs that allow people to pay bills through the Internet, but few banks present bills this way. Id. The payment system is called C2it. Citi Deploys, supra note 22, at 1.


27. Id.

28. “A portal is a web site that mixes content and utilitarian features to attract users on a mass scale, which sets it apart from a specialized web site geared to a niche audience.” Julie Monahan, Portal Puzzle, BANKING STRATEGIES, Nov. 1999/Dec. 1999, at 148. Most of the major portal sites such as Yahoo! and AOL started as search engines. Id.

29. Star Survey, supra note 3, at 4. Yodlee offers a “consolidated, summarized view of a user's personal account information and enables users to view updated snapshots of all recent account activities in one place.” Yodlee for the Web, at http://www.yodlee.com/solutions/yodleeforweb.html (last visited Oct. 30, 2000). It has been suggested that financial advisors should be wary of aggregation. Frederick P. Gabriel, Jr., Online Account Aggregation Could Hurt Advisors, INV. NEWS, Oct. 2, 2000, at 1. If a client can aggregate a complete financial picture on his own, it could eliminate the role advisors play in assembling a complete picture of a client's financial well-being. Id. Citigroup, Chase, Merrill Lynch, and Morgan Stanley indicate that they intend to analyze clients' financial needs and suggest investments using data gathered through account aggregation. Winning Duo: Aggregation Plus Advice, AM. BANKER, Oct. 4, 2000, at 1 [hereinafter Winning Duo].

will have eighty-eight banking and other customers, including Yahoo!, AOL, Citigroup, Wells Fargo, Chase Manhattan and Morgan Stanley Dean Witter.\(^\text{31}\)

Despite the increasing use of screen scraping technology by financial institutions security concerns remain, and each institution has taken various approaches to privacy, security, and liability.\(^\text{32}\) Financial institutions used varying approaches for deciding whether or how to transfer or sell customer information to third parties so that those third parties could market products and services to the customer base.\(^\text{33}\) Pending guidelines on the Gramm-Leach-Bliley Act (GLBA) may lessen the variety of approaches.\(^\text{34}\)

How regulation will or should affect the development of online financial management and aggregation is still not very clear, even with the additional guidelines. This Note will begin with a discussion of why financial institutions became interested in offering account aggregation.\(^\text{35}\) Then, it will discuss the effect of privacy regulations on aggregating financial institutions and authority for those institutions to conduct such business.\(^\text{36}\) Next, it

---


32. Renee Boucher Ferguson, *Data Aggregation Poses Risks, EWEEK, Oct. 2, 2000, at 44.* Yahoo sets a $1000 limit on its liability; officials from Citigroup said the bank would cover money lost to an aggregator, although they did not say how much. *Id.* Wells Fargo promises 100% coverage for any funds improperly removed while they are handling the transaction, including online theft of account numbers or passwords and unauthorized removal of funds from the account. *Wells Fargo Online Banking Guarantee, at http://www.wellsfargo.com/per/services/security.html (last visited Feb. 21, 2001). In a typical user acceptance agreement, VerticalOne promises “not to sell, exchange, or release your Personal Information or your Login Information to a third party without your express permission, unless required by appropriate legal processes, such as a judicial or administrative order.” *Centura Snapshot Privacy Policy, at http://www.centura.com/whatsonline/snapshot.cfm? (last visited Oct. 30, 2000) (linking to VerticalOne privacy policy and User Acceptance Agreement). The agreement also states, “you expressly agree that under no circumstances shall VerticalOne’s total liability to you or any party claiming by, through or under you for any cause whatsoever, and regardless of the form of action, whether in contract or in tort, including negligence or strict liability, in the aggregate, exceed $1,000 (U.S.).” *Id.*


35. *See infra* notes 54 – 91 and accompanying text.

36. *See infra* notes 92 – 119 and accompanying text.
will discuss how third party aggregators may be regulated, including the application of Regulation E. Finally, this note will explore the issues financial institutions need to be concerned with when providing aggregation services: security, privacy, and fraud protection.37

II. FINANCIAL INSTITUTIONS’ INCREASED INTEREST IN PROVIDING DATA AGGREGATION:

Financial institutions became interested in offering data aggregation services because consumers wanted to aggregate their financial lives. According to a Star System survey, 65% of online consumers believe that they will make all or most of their financial transactions online five years from now.38 Prior studies estimated that between 400,000 to 800,000 people would be using aggregation services by the end of 2000.39 Long-term predictions have motivated financial institutions to move far more quickly than normal.40 U.S. Bankcorp Piper Jaffray, for example, predicts the number of aggregation users will hit 90 million over the next

37. See infra notes 120 – 150 and accompanying text.
38. Star Survey, supra note 3, at 6. Twenty-two percent believe they will make all of their financial transactions online, and 43% believe they will make most of their financial transactions online. Id.
39. There is no real consensus as to the number of people currently using aggregation; estimates range from 100,000 current users to over 1 million. See Jeremy Quittner, Consumers Show Interest in Aggregation, AM. BANKER, Sep. 27, 2000, at 8A (citing to U.S. Bankcorp Piper Jaffray) (with 1 million user estimate); Hackett, supra note 20, at 1 (estimating current usage at about half a million); Banks Look Forward to Becoming Aggregators, RETAIL DELIVERY NEWS, Apr. 26, 2000, at 9 (citing to a “Account Aggregators, Screen Scrapers and Online Financial Services” report from Celent Communications) (estimating in April 2000 that about 100,000 users made use of aggregation services); Megan J. Ptacek, Aggregation Pits Banks Against Web Portals, AM. BANKER, Dec. 8, 2000, at 1 (estimating 3.1 million users by 2003).

“With most banking technologies, it takes about four years to get a new technology into the market ... [i]t historically takes a year for most banks to figure it out, a year to try to stop it, a year to recognize they can’t stop it and a year to do it. With aggregation, many institutions have gone from recognizing what it is and what it can do for them to implementation in about four months[.]” Id. (quoting Mathew Cone, chief marketing officer for Corillian Corp).
five years. When asked if they would like to have online access to all of their financial accounts through a central web site, approximately half of the respondents to an American Banker/Gallup Consumer Survey responded positively. Of those who expressed an interest in online account aggregation, 43% said they would be more interested if their primary financial institution provided the service, and 52% said it would make no difference.

A trend is developing, as aggregation technology and use matures, of giving consumers the capability to transfer funds among accounts and to third parties. However, as aggregation moves toward offering real-time transactional capabilities, consumer protection issues such as privacy, security, accuracy, and fraud prevention will become increasingly important and complex. More and more types of accounts are being aggregated, with insurance and real estate information becoming available alongside data from banks, credit card companies, and brokerage houses. Soon, consumers will be able to receive financial advice based on aggregated account information, purchase financial products, and transfer money electronically between accounts and to third parties. Experts predict that future software will be able

41. Leuchter, supra note 11, at 29 (citing U.S. Bankcorp Piper Jaffray's senior eFinance analyst, Stephen Franco).
42. Quittner, supra note 39, at 8A. Twenty-one percent were “very” interested, and 28% were “somewhat” interested. Id. It should be noted that 49% were “not interested.” Id. Among those who own computers, the “very interested” numbers rose to 26%; for current online banking customers, those numbers rose to 35%. Id.
43. Id. Only 5% said they would be less interested if their bank provided the service. Id. A November 1999 survey by Gomez Advisors found that 45% of active web bankers who transact online at least once a month are not interested in consolidating their accounts with one financial services provider. It's Brand that Claims a Category, FUTURE BANKER, May 2000, at 25S. But the numbers vary. In a study done in June 2000, 89% of respondents ranked as important that the service be “provided or supported by [their] current financial institution.” Star Survey, supra note 3, at 40 (57% ranked it as “very important” and 32% ranked it as “somewhat important”). The same survey found that approximately two thirds believe that web aggregation services offered by a financial institution provided greater security (70%), privacy (69%), and fraud protection (65%) than similar services offered by third-party Internet providers. Id. at 60-61.
44. Winning Duo, supra note 29, at 1.
45. Star Survey, supra note 3, at 1.
46. Id. Myciti.com offers the ability to check e-mail, airline miles, and travel reservations. Myciti.com Home Page, at http://www.myciti.com (last visited Feb. 21, 2001).
47. Star Survey, supra note 3, at 7.
to evaluate customers’ aggregated account information and, based on their financial goals and risk tolerance, automatically reallocate assets as needed to maximize value and return.48

If consumers want to aggregate their financial lives onto one web site and their financial institution is not providing the service, the financial institution may be the one that loses. The financial institution’s brand name is less visible and fewer visits to the site mean fewer opportunities to cross-sell financial products to consumers.49 The longer a customer stays, the greater the cross-sell potential.50 The hosting bank can address concerns about exposing customers to competitors by establishing itself as a destination site where customers spend most of their time.51 Aggregation agreements may increase revenue, and the technology, perhaps in conjunction with electronic bill presentment and payment, could turn online banking into a ‘must-have’ service.52 Aggregation can

48. Id.

49. Minkoff, supra note 12 (citing to Celent Communications, Account Aggregators, Screen Scrapers and Online Financial Services report). Cross-selling need not be limited to financial products. Over the 2000 holiday season, several major banks, including Chase, Citigroup, Bank of America, and First Union, formed partnerships with Internet retailers and begun promoting the merchants’ goods on bank-sponsored web sites. Deborah Bach, Banks Putting Brands On the Line with E-Tail Pairings, AM. BANKER, Dec. 21, 2000, at 1. Chase said that it seeks to give customers a convenient shopping experience that will promote Chase credit cards as the payment instrument of choice. Id. Bank of America offers discounts for Bank of America cardholders and guarantees safety. Id. Citibank tied a holiday promotion to its new Click Citi credit card, which was designed expressly for online purchases. Id.

50. Minkoff, supra note 12. However, the cross-sell potential is not limitless. Jessica Toonkel, As Aggregation Gains, Doubt on Cross-Selling, AM. BANKER, Sep. 19, 2000, at 1. Consumers indicated that they do not want to use account aggregation if it will lead to a barrage of marketing messages about new products. Id. Focus groups found that customers were against banner ads, targeted ads, and opt-in marketing. Id.


52. John R. Engen, Financial Funnel, BANKING STRATEGIES, Nov. 2000/Dec. 2000, at 64. “Ultimately, this is a chance for Internet banking to finally boost the bottom line....” Id. (quoting Octavio Marenzi, president of Celent Communications). Internet-only banks may reap the greatest benefit from aggregation services. Jessica Toonkel, Banks Stop Whining, Learn to Love Aggregation, AM. BANKER, Sep. 8, 2000, at 3A [hereinafter Toonkel, Banks Stop Whining]. Consumers who want to maintain a relationship with a traditional bank often question if they can get all of their services from Internet-only banks. Id. “Aggregation is a way we can allow them to maintain those relationships easily while growing our own relationships.” Id. (quoting D.R. Grimes, chief executive officer and vice chairman of Atlanta-based NetBank).
also make a financial institution’s web site “sticky,” because once customers take the time to set up aggregation of their accounts, they are not likely to go through the process again on another site.  

III. EFFECT OF PRIVACY REGULATIONS ON AGGREGATING FINANCIAL INSTITUTIONS  

Among other things, the Gramm-Leach-Bliley Act (GLBA) establishes a minimum federal standard of financial privacy, requiring written privacy policies and their disclosure to customers, as well as providing an opportunity for consumers to opt out of information sharing with a non-affiliate. Title V of GLBA was enacted to provide a mechanism to protect the confidentiality of a consumer’s personal financial information and give a consumer some power to choose how financial institutions use that information, without undermining the benefits that will result from enhanced affiliations and competition. Congress believed the development of new technologies that facilitate consumers’ access to the broad range of products and services

53. Toonkel, Banks Stop Whining, supra note 52, at 3A.
55. KENNETH R. BENSON, ET. AL, FINANCIAL SERVICES MODERNIZATION: GRAMM-LEACH-BLILEY ACT OF 1999, LAW AND EXPLANATION (1999), at 3. GLBA permits the creation of new financial services holding companies that can offer a full range of financial products under a strong regulatory-based regime. Id. It eliminates legal barriers to affiliations among banks and securities firms, insurance companies, and other financial services companies. Id. GLBA also provides financial organizations with flexibility in structuring these new financial affiliations through a holding company structure or a financial subsidiary with appropriate safeguards. Id. Under GLBA, the Federal Reserve Board remains the umbrella supervisor for holding companies and incorporates a system of functional regulation designed to utilize the strengths of the various federal and state regulators. Id. It also creates a system of coordination between the Federal Reserve Board and the Secretary of the Treasury for the approval of new financial activities for holding companies and national bank financial subsidiaries. Id.
56. Gramm-Leach-Bliley §§ 501-527 (codified as amended in scattered sections of 15 U.S.C.); BENSON, supra note 55, at 3. Title V requires financial institutions to develop practices to protect customers’ information from unauthorized access, to disclose to them in a clear, timely manner their policies for sharing information with unaffiliated third parties, and to inform them of their right to refuse permission for dissemination of certain types of data. 15 U.S.C. §6801-03 (Supp. V 1999). It also forbids financial institutions from disclosing customers’ account numbers to third parties for marketing purposes. 15 U.S.C. § 6802 (Supp. V 1999).
available through online media should be encouraged, provided such technologies continue to incorporate safeguards for consumer privacy.\textsuperscript{57}

The aggregation companies may not have seen themselves as falling under government oversight, but they seem to be coming around.\textsuperscript{58} GLBA defines "financial institution" to mean any institution engaged in financial activities as described in Section 4(k) of the Bank Holding Act of 1956.\textsuperscript{59} Those "financial activities" include not only a number of traditional financial activities specified in section 4(k) itself, but also those activities the Federal Reserve Board (Fed) has found to be either closely related to banking or usually in connection with the transaction of banking or other financial operations abroad, by regulation (or order or interpretation) "in effect on the date of the enactment of the [GLBA]."\textsuperscript{60} Expressly included in certain circumstances is:

\textsuperscript{57} BENSON, supra note 55, at 99. Congress' belief seems to assume a certain level of self-regulation. \textit{Id.} While responsible aggregators are currently doing an admirable job of this, there is no guarantee that they will continue to do so, or that some rogue aggregator will not break the rules. \textit{Id.}

\textsuperscript{58} Hackett, supra note 20, at 1. "It was a real wake-up call for some of these technology providers when they first got involved with regulators and banks. The aggregators discovered that they're treading in an area where we're going to be looking at them." \textit{Id.} (quoting Jennifer Dickerson, director, technology risk management, at the Office of Thrift Supervision).


[T]he following activities shall be considered to be financial in nature:

(A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities.

(B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State.

(C) Providing financial, investment, or economic advisory services, including advising an investment company (as defined in section 3 of the Investment Company Act of 1941).

(D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.

(E) Underwriting, dealing in, or making a market for securities.


\textsuperscript{60} Id. The Fed's list of such activities is found in 12 C.F.R. § 225.28 and 12 C.F.R. § 225.86(a) (2000). The FTC interprets GLBA to refer to those activities in section 4(k) that are described as financial in nature at present, and not automatically to include those activated that the Federal Reserve Board later determines are
“providing financial data processing and transmission services, facilities (including hardware, software, documentation, or operating personnel), data bases, advice, or access to these by technological means.” Thus, it appears that financial institutions and their aggregators fall under GLBA.

GLBA lists the various categories of “financial institutions and other persons” subject to Title V and specifies their respective regulators. After detailing the respective regulators for brokers, insurance companies, and various categories of banks, section 505 assigns responsibility for “any other financial institution or other person” to the Federal Trade Commission. The Office of Thrift Supervision (OTS) has taken the position that aggregation technology companies providing services to institutions fall within the agency’s jurisdiction. “The concept of ‘financial institution’ is a very significant concept and may be interpreted somewhat differently depending on which regulatory agency you’re dealing with." The Fed is responsible for Regulation E, the regulation that governs electronic fund transfers. It has not formally weighed in on whether or not aggregators would be considered financial institutions, but as the discussion later in this paper indicates, it is possible that the Fed could construe the regulation that way. However, commentators on the Privacy of Consumer Financial Information rules set forth by the Federal Trade Commission (FTC) requested clarification concerning whether certain Internet industries are affected by the rule. In its final rule, the FTC noted that institutions operating on-line, like those operating off-line, must evaluate whether they are engaged in a

---

incidental or complementary to financial activities. Id.

64. Hackett, supra note 20, at 1. The ruling by OTS is narrower than it first appears; aggregators working independently of any financial institutions may or may not be subject to regulation when offering their services directly to the public. Id.
65. Id. (quoting John Burke, outside counsel for BITS, the technology arm of the Financial Services Technology Consortium).
66. Id.
67. The Fed will likely consider Internet aggregators to fall under federal regulations. See infra notes 69-119 and accompanying text.
financial activity, and if so, whether they have consumers or customers that trigger the disclosure or other requirements of the Act.\textsuperscript{[69]} The FTC specifically noted that the language of proposed Regulation E brings into the definition of ‘financial institution’ “an Internet company that compiles, or aggregates, an individual’s online accounts ... at that company’s web site as a service to the individual, who then may access all of its account information through that Internet site.”\textsuperscript{[70]}

As for the relationship between aggregating companies working for financial institutions, bankers should tread carefully, since creating a principal-agent relationship between an aggregator and a financial institution presents an opportunity for liability. Commentators to privacy regulations proposed by the various agencies agreed with the principle that an individual should not be considered a consumer of an entity acting as agent for a financial institution.\textsuperscript{[71]} Financial institutions should note that the financial institution that hires the agent is responsible for that agent’s conduct in carrying out the agency activities; therefore, the financial institution fulfills any obligations regarding the agent’s handling of consumer information that otherwise would fall on the agents.\textsuperscript{[72]} This concept is critical to banks entering the data aggregation business. Banks could face possible liability through a principal-agent relationship for any mishaps that occur through the aggregator’s fault.\textsuperscript{[73]} Further, whenever a third party contracts with a depository institution to provide technology or services that enable the institution to offer web aggregation, the law seems to expect the third party to uphold specified safety and soundness standards to protect the depository institution and its customers.\textsuperscript{[74]}

\textsuperscript{69} Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646, 33,655 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313). The FTC also notes that financial software and hardware manufacturers, as described, are financial institutions but will have no disclosure obligations if they sell only to businesses. \textit{Id}.

\textsuperscript{70} \textit{Id}. at 33,655.

\textsuperscript{71} \textit{Id}. at 33,651.

\textsuperscript{72} \textit{Id}. It is possible for two institutions to provide a financial service to the consumer as part of the same transaction, such as a loan broker that locates a creditor who makes a loan to the individual; in those situations, the consumer will have a customer relationship with both financial institutions. \textit{Id}.

\textsuperscript{73} \textit{See id}.
Financial institutions should also exercise care with respect to the labyrinth of federal privacy safeguards. Privacy provisions do not apply to all consumer information; they apply only to so-called 'non-public personal information.' GLBA defines nonpublic personal information to mean "personally identifiable financial information—(i) provided by a consumer to a financial institution; [or] (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) [information] otherwise obtained by the financial institution. The final Office of the Comptroller of the Currency, Fed, OTS and Federal Deposit Insurance Corporation (FDIC) rule states that: "information will be deemed to be 'publicly available' and therefore excluded from the definition of 'nonpublic personal information' if a financial institution has a reasonable basis to believe that the information is lawfully made available to the general public from one of the three categories of sources listed in the rule." The joint final rule treats any information as personally identifiable financial information if the consumer provides information in order to obtain a financial product or service, or the bank otherwise obtains the information in connection with

---


Banks must understand how absolutely vital it is to choose a reputable source for aggregation technology or services...[j]ust as no bank would ever make a loan unless it had a loan officer that understood credit risk, banks also must be sure that they have the internal expertise necessary to evaluate and select reputable and credible vendors. This is critical to their reputation and responsibility to account holders.


76. Id.


providing a financial product or service to the consumer. Further, information obtained over the Internet will be considered publicly available if it is lawfully made available on a site that is accessible to the public on an unrestricted basis. The FTC’s final rule considers information to be publicly available if a bank has a reasonable basis to believe that the information is lawfully made available to the general public from government records, widely distributed media, or disclosures required by law.

The full range of federal privacy safeguards does not apply to information shared by financial institutions with either affiliates or third-party providers and servicers of the institution. A consumer has no right to opt out of disclosure, but the bank must satisfy certain requirements in order to qualify for the exception. First, before the bank shares the information, it must disclose to the consumer that it will provide this information to the nonaffiliated third party. Second, the bank must enter into a

79. Id. at 35,171.
80. Id. at 35,172. A web site is not restricted merely because an Internet service provider or a web site operator requires a fee or a password, so long as access is available to the general public. Id. A site such as a ‘look up’ service, that makes available personal information (that may combine publicly available and confidential information on a particular individual) compiled in response to a specific request, is not available to the general public on an unrestricted basis. Id.

81. Privacy of Consumer Financial Information, 65 Fed. Reg. 33,645, 33,657 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313). A bank may not assume that a consumer’s information is publicly available but must determine that the information is of the type that is available to the general public and whether an individual can direct that the information not be publicly available (for example, an unlisted telephone number). Id. If an individual can take steps to prevent information from being made publicly available, a bank must determine whether the consumer has done so. Id.

83. Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162; Privacy of Consumer Financial Information, 65 Fed. Reg. 33,645, 33,657. Proposed Fair Credit Reporting Act regulations would require financial institutions to send “opt-out” forms to customers. Michele Heller, In Brief: Roundtable Knocks Privacy Opt-Out Plan, AM. BANKER, Nov. 17, 2000, at 4. The fair credit proposal would require a notice that details what information is being released, what kind of companies will have access to the information, the customer’s right to refuse to share the information, and how someone would actually execute an opt-out. Id. The proposal does not seem to distinguish between data sharing within the ‘corporate family.’ Id. GLBA requires all customers be notified of a financial institution’s privacy policies and those that share data outside the corporate family must give customers an opportunity to opt out of the information sharing. Id. (emphasis added).

84. Heller, supra note 83.
contract with the third party that requires the third party to maintain the confidentiality of the information.\textsuperscript{85} The final rule requires that the contract generally prohibit the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.\textsuperscript{86} The final rule imposes no additional conditions for the availability of this exception beyond those indicated in the statute.\textsuperscript{87} If nonpublic personal information is received under one of the above exceptions, its use is also restricted.\textsuperscript{88} The information can be shared with affiliates of the financial institution from which the information was obtained.\textsuperscript{89} It can also be disclosed to the receiving institution’s affiliates, but those affiliates can only use the information to the extent that the receiving institution has disclosed or used the information.\textsuperscript{90} The information can also be disclosed in the ordinary course of business of carrying out the activity covered by the exception under which the receiving institution received the information.\textsuperscript{91}

IV. REGULATING THIRD PARTY AGGREGATORS

Although consumers may not have specific knowledge about all of the federal and state imposed controls placed on depository institutions, these safeguards contribute to subtle perceptions about the ‘safeness’ of these institutions and instill

\textsuperscript{85} Id.
\textsuperscript{86} Id.
\textsuperscript{87} Id.
\textsuperscript{88} 16 CFR §313.11(a)(1)(2000) (FTC regulations).
\textsuperscript{89} Id.

Except as otherwise provided in this subtitle, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

\textsuperscript{90} Id.
\textsuperscript{91} Id.
confidence in the services the financial institutions provide. Ninety-two percent of Star survey respondents believe that all web aggregators—third-party Internet providers as well as financial institutions that offer web aggregation—"should be required to comply with federal banking regulations." Significantly, 51% of respondents assumed that third-party Internet companies "are required to comply with federal banking regulations." An overwhelming majority also say they would be less likely to use third-party providers if they knew that those providers "were not required to comply with federal banking regulations."

Amid the current regulatory uncertainties, the leading third-party aggregators realize that ensuring consumer privacy and security is vital, and many have instituted robust, comprehensive security technologies and procedures. Aggregators have been

92. Star Survey, supra note 3, at 15. These safeguards include capital and reserve requirements, review of board and senior management qualifications, deposit insurance and regular governmental examinations. Id.

93. Id.

94. Id.

95. Id. Eighty-nine percent said they would be less likely to use third-party providers if not regulated by federal banking regulations. Id.

96. Id. Typical of the high level of security, Yodlee employs the following security measures for its liaison with myciti.com: Twenty-four hour monitoring of the physical site with access to servers requiring multiple levels of authentication, including biometric (hand print scan); and, network infrastructure including firewalls, intrusion detection, private addressing, sanitized systems, and Secure Socket Layer, which creates an encrypted connection between the users browser and the MyAccounts Web servers. Citigroup, Privacy / Security Policy, at https://myaccounts.myciti.com/help/privacy.html (last visited Feb. 27, 2001). MyCiti.com also employs regular audits and inspections by Ernst & Young (audits network and policy security) and Security (audits network and Internet application security). Id. Citigroup and Yodlee employ a fairly typical privacy statement, promising that they will ensure the confidentiality of customer financial information by the following pledges:

- We will not sell or share your data with any third parties.
- We will not contact you or allow others to contact you without your explicit permission (via opt-in on site), unless required for customer service.
- We cannot view your usernames, passwords or any of your data collected from other sites – this information is kept encrypted at all times.

Id. The site also states that it will not share personal data with third parties "unless it is required to be disclosed by law under a subpoena." Id. Some third-party aggregators are members of the TRUSTe Program, an independent, nonprofit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent. Star Survey, supra note
working hard to convince institutions and consumers that their systems are safe and secure. Best practices for aggregators have emerged, which include third-party audits, identification and authentication systems, access-control procedures and incident protection procedures. However, these safeguards are privately enacted. Traditionally defined financial institutions are subject to enforcement by traditional banking regulators, who examine them on a regular, proactive basis. If an independent aggregator falls within the updated definition of ‘financial institution’ under GLBA, it would appear that the aggregator is subject to FTC enforcement. Once the FTC is involved, it moves swiftly, aggressively, and publicly to investigate and penalize an offender. However, the FTC does not proactively audit or seek out offenders as would traditional banking regulators.

What happens when aggregators move away from offering just account viewing and move into providing bill-paying or money-transferring services? One potential way to regulate third party aggregators that offer bill-paying services is through the Electronic Fund Transfer Act (EFTA). Enacted in 1978, EFTA

3, at 21. However, the TRUSTe program is not perfect. In July, 2000, Columbus, Ohio based Interhack Corp., a security firm that does risk assessment for Internet retailers, reported that at least two websites that carried the TRUSTe privacy seal, Lucy.com and Fusion.com, were sending personal information to the marketing company Coremetrics. Rebecca Lynch, Analysis: E-Privacy Debates Faces Long Road Ahead, at http://www.cnn.com/TECH/10/04/privacy.fuss.idgl/index.html (last visited Nov. 7, 2000). ToySmart, the mostly Disney-owned online toy retailer based in Waltham, Massachusetts, filed for bankruptcy protection and then tried to sell its customer lists (complete with member's children's names, ages and e-mail addresses), even after their TRUSTe blessed site promised it would never share that information with a third party. Id. It is reassuring to note that TRUSTe is the entity that first alerted the FTC to the bankrupt e-tailer's intent to sell its confidential customer data. Id. As of October 4, 2000, the FTC has agreed to settle the suit filed against ToySmart. Id.

98. Id.
101. Star Survey, supra note 3, at 19. This was demonstrated in July 2000 when the FTC sued to prevent the bankrupt Internet toy seller ToySmart from selling its confidential customer data. See supra note 96 and accompanying text.
102. Star Survey, supra note 3, at 19.
provides a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer (EFT) systems. The EFTA is implemented by the Fed's Regulation E, and includes language specifying which regulator has authority over each category of institution and stating that any category not expressly listed falls under FTC jurisdiction.

Appendix B of Regulation E uses the same explanations of responsibility, concluding "all others not covered above" fall under the jurisdiction of the FTC.

No definitive ruling has been issued on how Regulation E will apply to third party Internet aggregators when aggregation evolves to incorporate EFT capabilities. The Fed has taken the general position that an aggregator would be a financial institution for purposes of Regulation E. In an effort to determine the

104. 15 U.S.C. § 1693 (1994). As of now, data aggregation sites provide only information; they have not yet jumped onto the transaction bandwagon, but pundits indicate that it is a natural next step. See Leuchter, supra note 11, at 28.

105. 12 C.F.R. pt. 205 (2000). Types of transfers covered by EFTA and Regulation E include transfers initiated through an ATM, point-of-sale terminal, automated clearinghouse, telephone bill-payment plan, or remote banking program. Electronic Funds Transfer, 65 Fed. Reg. 40,061 (June 29, 2000). The Act and regulation require disclosure of terms and conditions of an EFT service; documentation of electronic transfers by means of terminal receipts and periodic account statements; limitations on consumer liability for unauthorized transfers; procedures for error resolution; and certain rights related to preauthorized electronic transfers. Id. The Act and regulation also prescribe restrictions on the unsolicited issuance of ATM cards and other access devices. Id.


108. Star Survey, supra note 3, at 20. Most commentators believe that any aggregator through which a consumer can initiate an EFT would likely be subject to Regulation E. Id. Even before aggregation evolves to incorporate EFT capabilities, a serious question exists regarding where liability will fall if fraudulent transactions occur because of account access information provided by the consumer to the aggregator. Id. Among other possibilities, the Federal Reserve suggests that, depending on the exact circumstances surrounding a specific unauthorized EFT, liability might be found to lie with the financial institution, with the third party aggregator, or with the consumer who had given the aggregator access to the consumer's account. Id.

109. Electronic Funds Transfer, 65 Fed. Reg. 40,061. Typically, only one access device is contemplated to initiate an EFT to or from a consumer's account. Star
applicability of Regulation E, the Federal Reserve issued a request for comment on "the implications of a determination that aggregators are or are not financial institutions for purposes of Regulation E. . . ." The Board has specifically requested comments on the following:

- Are aggregators providing or planning to provide bill-payment or other EFT services (in addition to information services)?
- To what extent do agreements exist between aggregators and account-holding institutions, governing matters such as procedures for access to information and for electronic transfers?
- Additionally, what are the implications of a determination that aggregators are or are not financial institutions for purposes of Regulation E generally or under §205.14.

The Credit Union National Association, Inc.'s (CUNA) comment letter on Regulation E was typical of comments received and stressed three key points. First, the letter urged the Fed to consider financial aggregators to be financial institutions subject to Regulation E. CUNA's letter also expressed concern about credit union members giving their Personal Identification Survey, supra note 3, at 20. Nevertheless, if a consumer enters a security code issued by the aggregator to access information on the aggregator's web site and the consumer initiates an EFT using a security code provided by the account-holding institution, the security code issued by the aggregator arguably meets the definition of an "access device." Id. The Fed has also said that if a consumer gives the aggregator access to his or her financial information and the aggregator is not a financial institution, and a transaction takes place, the consumer's account may assume liability for the transfer. Id. Independent Community of Bankers Association President Thomas J. Sheehan takes the position that aggregators "indirectly hold consumer accounts by virtue of being entrusted by the consumer with access codes to the consumer's account." Id.

110. Electronic Funds Transfer, 65 Fed. Reg. 40,061. The request was sent June 23, 2000 and comments were due August 31, 2000. A final ruling is due by the end of 2001. Id.
111. Id.
113. Id.
Numbers to financial aggregators and the potential for abuse.\textsuperscript{114} Finally, the letter urged the Fed to propose “rigorous encryption, network security, and fraud detection system guidelines for screen scrapers.”\textsuperscript{115}

In discussing possible avenues of regulation for aggregators, one cannot ignore the possibility of state level regulation. States presently license a wider array of financial service providers than does the federal government.\textsuperscript{116} Aggregators are not yet licensed under existing state laws, but other financial service providers that provide very similar services are subject to state licensing in connection with those activities.\textsuperscript{117} Some states could interpret current money transmitter laws to include those who receive payment instructions that result in the transmission of money, and not just those who actually receive money.\textsuperscript{118} If states get into the act, aggregators could find themselves subject to license fees, background investigations, surety bonds, minimum net worth requirements, annual record keeping and reporting requirements, periodic examinations by state regulators, fee limitations and criminal and civil penalties for noncompliance.\textsuperscript{119}

V. AGGREGATING FINANCIAL INSTITUTION CONCERNS

Consumer fears concerning the inappropriate use of personal information could quickly turn into distrust of the financial institution itself.\textsuperscript{120} In a survey of consumer attitudes

\textsuperscript{114} Id.

\textsuperscript{115} Id. (quoting the comment letter from CUNA). It also urged that guidance by the board should also protect the account holding institution form liability resulting from an aggregator’s activities. Id.

\textsuperscript{116} Mugavero & Negoroni, supra note 97.

\textsuperscript{117} Id. For example, several states regulate companies engaged in money transmission. Id. At the simplest level, money transmitters receive money from one party to pay another party. Id. Aggregators are distinguishable from money transmitters because rather than receiving funds, they receive instructions from a customer and then instruct the customer’s bank to transfer funds. Id. Aggregators have the ability to make traditional money transmitters obsolete, and states may not allow a regulated industry to be displaced by an unregulated one. Id.

\textsuperscript{118} Id.

\textsuperscript{119} Id.

\textsuperscript{120} Vartanian & Ledig, supra note 2.
about Internet privacy, respondents who were asked specifically about their online privacy said they were most worried about web sites providing their personal information to others and collecting information about them without their knowledge. Seventy-one percent of those surveyed said it is absolutely essential that companies ask consumers' permission before using their personal information for any purpose other than the one originally given. Ninety-one percent of those polled trust companies somewhat or completely to follow their posted privacy policies. Consumers are most worried about the security of their financial information online, with 53% afraid their financial or other sensitive information may be stolen during transmission to a web site. Seventy-four percent thought the protection of financial asset information was most important. To create a higher level of consumer confidence, financial institutions and aggregators need to address security, privacy, and fraud protection. An aggregator's need to store customer authentication information within its computer system is one of

121. To measure consumer attitudes about Internet privacy, security and children's online safety, the National Consumers League, with the support of Dell, commissioned a survey that was conducted by Harris Interactive in August 2000. Press Release, National Consumers League, Online Americans More Concerned about Privacy Than Health Care, Crime, and Taxes (Oct. 2000) (available at http://www.natlconsumersleague.org/news2000.htm#October) (last visited Feb. 23, 2001) (linked directly to Harris Poll). Harris Poll Online conducted the survey within the United States, from August 30-31, 2000, and surveyed 2,810 adults. Id. The national sample was designed to be representative of adults over eighteen who are online. Id. The survey weighted figures for age within gender, race, education, region, and income where necessary to bring them in line with their actual proportions in the population. Id.

122. Id. Sixty-four percent were 'very concerned' about web sites providing information to other organizations without the consumer's knowledge, and 59% were 'very concerned' that web sites would collect information about them without their knowledge.

123. Id.

124. Id. Ninety-nine percent of respondents had seen a privacy notice or other explanation of how personal information collected by that site would be used, but only 20% always read the information in the privacy notice and 49% read it sometimes. Id. Forty-eight percent wanted web sites to explain exactly how their sensitive information is secured in transmission and storage. Id.

125. Id. Thirty-five percent of the respondents were very concerned that someone could get into the company database and steal customer information, while 47% were very concerned about receiving a virus. Id.

126. Id.

127. Star Survey, supra note 3, at 8.
the biggest concerns to financial institutions. Even the most powerful security precautions can be subject to foul play. In February 2000, federal and industry security teams warned that malicious codes embedded in Internet links and e-mails could allow hackers to capture any information entered by the user. In June 2000, America Online faced the possibility that hackers had penetrated the company security system and obtained subscribers' credit card numbers. If a hacker successfully breached a web aggregator's security, "consumers could face losses far greater than a single credit card number and expiration date." Additionally, financial institutions and third-party aggregators have not agreed on a common set of control points to form a dependable audit trail, which would help track a fraudulent transaction.

128. *Id.*; Renee Boucher Ferguson, *Data Aggregation Poses Risks*, *E*WEEK, Oct. 2, 2000, at 44.

129. Star Survey, *supra* note 3, at 21. Catherine Allen, chief executive officer of BITS, says that "if a master computer hacker, working either within a third-party aggregator or alone, wanted to badly enough, he or she could conceivably gain access to account and authentication information, log directly on to financial institutions' web sites, and make off with funds from a multitude of accounts. And because there currently is no audit trail, it would be difficult, if not impossible, to trace such transactions." *Id.*


132. Star Survey, *supra* note 3, at 8. The methods currently available to aggregators for authenticating customers' identities is also a concern. *Id.* Financial institutions must use multiple authentication processes and tools when opening a new account for a new customer; web aggregators, however, currently base authentication decisions exclusively on information provided to them online by their presumptive customers. *Id.*

133. *Id.* Financial institutions provide personal I.D. numbers (PINs) to their customers so that those consumers can access their accounts online. Vartanian & Ledig, *supra* note 2. It is clear enough that the information belongs to the customer, but is the PIN a blanket authority for the consumer to access (and allow others to access) their account information, or may the provider impose terms and conditions limiting the purposes for which the PIN may be used and the parties who may use it? *Id.* Mr. Vartanian and Mr. Ledig of Fried, Frank, Harris, Shriver, & Jacobson cite America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d. 244 (E.D. Va. 1998) for the possibility that the PINs can be limited in this way. *Id.* America Online filed suit against a company sending unwanted e-mail to its members in violation of the conditions of use of the service. *Id.* The Court found this breach was a violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (Supp. IV 1998). *Id.*
Direct data feed access by the aggregators challenges a financial institution’s computer system because it places a huge demand on that system, which can have a detrimental effect on the system’s speed and could even cause a system to crash.\(^{134}\) Directly feeding data from a financial institution to an aggregator is less subject to fraud than screen scraping because it has an added level of security.\(^{135}\) There is an impetus to create a common language for direct feed. In January 2001, a group of technology companies led by IBM introduced an Internet standard that gives companies a common platform for exchanging information about customers.\(^{136}\) Companies that join the Customer Profile Exchange Network (CPExchange) will be able to swap customer names, addresses, phone numbers, and ages, plus harder-to-track data like transaction information and purchases.\(^{137}\)

As discussed earlier in this Note,\(^{138}\) a financial institution that changes the design of its web site or screen can create problems with inaccurate or incomplete data collected by screen scraping aggregators.\(^{139}\) Exacerbating problems with accuracy, many aggregators collect account data once a day, which means that the information available at their web sites is updated only once every twenty-four hours.\(^{140}\) Although some institutions aim to

\(^{134}\) Star Survey, \textit{supra} note 3, at 9. Bielski, \textit{supra} note 7, at 47. Currently, the population of web aggregation at any given institution is not great enough for this to be a real concern. \textit{Id.} Moreover, the aggregators and banks accomplish direct feeds overnight in batches, when demand on computer systems is relatively low. \textit{Id.} at 9-10. It is not clear what will happen as the number of aggregation customers grows into the millions. \textit{Id.} at 10.

\(^{135}\) See \textit{supra} notes 6-8 and accompanying text. Because direct feed access requires a financial institutions’ full knowledge and cooperation, this method actually may expose participating financial institutions to greater liability than screen-scraping. Star Survey, \textit{supra} note 3, at 10.


\(^{137}\) Star Survey, \textit{supra} note 3. The exchange is in the experimentation and demonstration phase, and its organizers have not said when they expect to have it fully up and running. \textit{Id.} First Union is involved in the development of CPExchange, and some have questioned whether bank involvement violates GLBA. Sen. Shelby Questions First Union’s Involvement in Data-Sharing, B.N.A. BANKING DAILY, Dec. 11, 2000.

\(^{138}\) See \textit{supra} notes 9-14 and accompanying text.

\(^{139}\) Star Survey, \textit{supra} note 3, at 9.

\(^{140}\) \textit{Id.}
impede screen scrapers by reconfiguring their web sites, most changes are made simply to accommodate more information or otherwise enhance customer convenience. Regardless of the motivation for change, the aggregator’s site is inaccurate.

In addition to technological concerns and worries about third parties, financial institutions need to worry about data aggregator behavior and the taint of misbehavior by other financial institutions. Potential aggregator misconduct is reflected in reports that a senior executive at Wells Fargo was warned by several screen scrapers that if the bank failed to cooperate, the aggregators “would be happy to introduce shared customers to banks that would.” Financial institutions will have to vigorously condemn the mere appearance that it improperly shared customer information. FleetBoston Financial Corporation is under fire from Minnesota Attorney General Mike Hatch for allegedly sharing its customers’ home mortgage account numbers, contact numbers, and other personal information with telemarketing companies.

With public awareness of privacy issues and the foibles of its human operators at an all time high, a financial institution may react with guarantees of maximum protection on its website. However, at least one writer for the magazine Web Finance thinks that would be an overreaction. Celia Santander argues that the worst possible approach is to promise too much and deliver too

141. Bielski, supra note 7, at 47. There is some interesting software by Vyou, Inc. that allegedly “foil[s] account aggregators by prohibiting them from taking customer information from bank [w]eb sites . . . .” Megan Ptacek, Aggregator-Blocking Service May be Blocked by Bad Timing, AM. BANKER, Feb. 16, 2001, at 1. Since banks seem to be adopting aggregation services and accepting screen-scraping as a fact of life, Vyou’s success may hinge on how much anti-aggregation sentiment banks are still harboring; alternatively, financial institutions may be able to find a profitable use for the technology by keeping illegitimate screen-scrapers away from a bank’s web site. Id.


143. Id.


little by making promises in a privacy policy that are logistically or technically impossible to keep. In the recent Toysmart.com case, the FTC filed suit against Toysmart.com for violating its own website privacy policy, which stated that personally identifiable information would ‘never’ be sold to a third party. Toysmart’s attempted sale was in the context of bankruptcy and demonstrated how far the FTC would go to enforce the terms of a consumer website privacy policy. Regulatory enforcement aside, any commerce site subscribing to seal organizations such as TRUSTe can be open to breach of contract claims under the terms of such programs.

VI. CONCLUSION:

Customers want aggregation so long as concerns about security, fraud, and privacy are appropriately addressed. Financial institutions are in a good position to address those concerns while providing a service under rising demand. If financial institutions decide to continue fighting the aggregation trend, others organizations will provide the service—and keep the customers. As enhancements such as investment advice, portfolio management, and cross-selling are added to aggregation service, the opportunities for increased revenues from aggregation are likely to increase as well.

If a financial institution decides to become an aggregator, it must consider and evaluate the risks and methods. The decision-makers must evaluate the technological demands on their system, as well as what kind of aggregator it wants to be—direct feed only or primarily screen scraping. As a financial institution, banks must examine regulations as they apply to banks, and must also take

147. Id.
148. Id. Commissioner Orson Swindle explained simply that “never really means never”—a warning to website privacy policy drafters to say exactly what you mean. Id.
150. Santander, supra note 146.
appropriate measures to assure themselves that the aggregation service provider follows applicable regulations. It appears that aggregators, whether independent or working with a financial institution, will fall under some federal regulations such as GLBA. It does not appear as if the financial institution will have to look only to the contract to enforce those regulations; they will be able to ask for FTC enforcement.

This Note does not propose that federal regulatory oversight of aggregators to the same degree of federal regulatory oversight of financial institutions is in the best interests of financial institutions or their customers. First, the enforceability of such oversight would be catch-as-catch-can at best. Second, the expense of enforcement would be horrendous. Finally, such regulation could have a chilling effect on competition and the development of new technologies that may help banks work better, faster, and cheaper. Requiring the same kind of auditing banks must endure does not seem to meet the same level of cost-benefit. Enacting more regulations for aggregators, only leads to further regulation of the banking industry. The FTC umbrella for enforcement would seem the most cost-efficient manner of enforcement. It is a proven system that relies on consumer and banker vigilance. Requiring aggregators to abide by privacy regulations should not dampen innovation and should lead to greater customer confidence and satisfaction.

Kimberly L. Wierzel