Fordham Journal of Corporate & Financial Law

Volume 8 | Issue 2 Article 6

2003

Financial Account Aggregation: The Liability Perspective

Ann S. Spiotto

FINANCIAL ACCOUNT AGGREGATION: THE LIABILITY PERSPECTIVE

Ann H. Spiotto[*]

INTRODUCTION

When a consumer thinks about using a financial account aggregation site, one concern is whether or not such use is safe. A related question is *who* has responsibility for unauthorized transactions or other fraud-related problems occurring as a result of a consumer providing his account information, usernames, and personal identification numbers ("PINS") or other access codes to the aggregation site. An additional question is, *who* is responsible for costs and expenses incurred by the consumer as a result of actions he takes based upon inaccurate, incomplete or obsolete information (bad account data) provided at the site.

This Article explores the potential financial risks to the consumer and account holding financial institutions ("AHBanks") from aggregation. It also analyzes the current state of the law and

---

[*]Ms. Spiotto is senior research counsel with the Emerging Payments Studies Department at the Federal Reserve Bank of Chicago. She received a J.D. from the University of Chicago in 1972 and is a member of the Illinois Bar. The author would like to thank Patricia Allouise, Sujit Chakravorti, Sarah Jane Hughes, Leslie Mitchell, Sukhinder Singh, and David A. Stein for helpful comments on previous drafts. Special thanks to Brian Mantel for his support in reviewing and critiquing this Article. This Article reflects the author's preliminary views in connection with a developing business and technology product. Business, technology and laws are subject to changes in substance and interpretation. As the business and technology evolves, the legal analysis may also change and evolve. The views expressed in this Article are those of the author alone and do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Board of Governors of the Federal Reserve System. It does not provide legal advice to be relied upon by consumers, account holding financial institutions, or aggregators, each of whom should consult with their own attorney or legal advisor for advice on questions about liability issues in connection with aggregation.

contractual relationships relevant to such risks. It concludes that: (1) with respect to unauthorized transactions, parties other than the consumer appear to bear the ultimate liability for financial losses in most situations and parties other than the AHBank appear to bear the ultimate responsibility for financial losses in a number of situations, and (2) with respect to losses resulting from reliance upon bad account data, the consumer will probably have a more difficult time shifting losses to either the AHBank or another party.

The question of whether legislative or regulatory action is necessary at this time with respect to liability issues is then addressed, with the conclusion reached that at the current stage in the evolution of aggregation services such action appears to be premature.

The following framework is used in reaching these conclusions. First, the question "What is financial account aggregation?" is addressed in Part I. Part II identifies and discusses potential financial liabilities connected to aggregation, specifically those resulting from the display of inaccurate, incorrect, or incomplete information and those resulting from unauthorized transactions. Part III follows with an analysis of who has liability for unauthorized transactions, beginning with a discussion of the basic rules ("SIMPLE ANSWERS") governing liability in those simple situations where an unauthorized transaction occurs and the consumer has not used an aggregation site.

After conclusions are reached for the simple situations, Part IV continues the analysis by adding one additional factor to those situations already discussed: the consumer signs up for aggregation. It analyzes whether and how the previously defined SIMPLE ANSWERS change once the existence of the consumer's relationship with an aggregation site is added to the mix. After this discussion, the author concludes that significant concerns over consumer or AHBank liability for unauthorized transactions as a consequence of the consumer arranging for aggregation are premature at this time. Consequently, Part V offers some suggestions on why such concerns exist and why the evolution of aggregation over the past couple of years should have diminished those concerns.

This Article concludes that at this stage in the evolution of

aggregation services, legislative/regulatory action with respect to liability issues is premature and recommends that no such action be taken at this time. It points out that where theoretical problems are "solved" by new legislation/regulations before problems actually develop, the solutions may be unnecessary or result in unanticipated negative consequences. It recommends that (1) the financial services industry be allowed to exercise its judgment in developing the aggregation product under the existing regulatory framework and (2) regulators continue to monitor business practices and developments in connection with the aggregation product and take regulatory action only if the need is actually demonstrated.

I. WHAT IS FINANCIAL ACCOUNT AGGREGATION?

In order to answer the questions identified above, one must understand what aggregation is and who the participants are. Aggregation as discussed in this Article is relatively new, appearing on the landscape in 1999–2000. A Morgan Stanley Report estimates that there were just 10,000 aggregation users nationwide at the beginning of 2000; by September 2000, the number was estimated to be 500,000;[1] and at the beginning of 2002, the number of aggregation service users was estimated by various analysts at between 300,000 and one million U.S. consumers.[2]

---

1. *See* Henry H. McVey & Prem G. Kumar, *The Next Big Thing: Account Aggregation*, *in* 2000 MORGAN STANLEY DEAN WITTER INDUSTRY REP., at 4 (2000) (on file with the Federal Reserve Bank of Chicago) [hereinafter MORGAN STANLEY REPORT].

2. *See* Andrew Roth, *Aggregation's Advance Impeded By Data Issues*, AM. BANKER, July 26, 2001, at 1 (quoting BANKING INDUSTRY TECHNOLOGY SECRETARIAT ("BITS"), BITS VOLUNTARY GUIDELINES FOR AGGREGATION SERVICES (Apr. 2001), *available at* http://www.bitsinfo.org (last visited Apr. 2, 2003) [hereinafter BITS VOLUNTARY GUIDELINES]); *see also* Ray Graber, Comment, *Aggregation Providers Don't Yet Have It Together*, AM. BANKER, Aug. 14, 2001, at 10 ("The public's interest in aggregation far outweighs the propensity to sign up for it. Consumers like the concept, but balk at enrolling for it because of setup headaches . . . ."); Jack M. Pullara, *Aggregation's Risks, Costs Not Justified*, AM. BANKER, Nov. 16, 2001, at 8 (indicating that conservative estimates put the number close to 600,000 active users, i.e., customers who access the aggregation site at least once every thirty days). As of January 1, 2002, aggregation sites powered by Yodlee had over 2.2 million registered users; of

The following simple statement conveys the essence of aggregation:

> Web aggregation services are provided by companies—either financial institutions or third-party Internet companies—that [the consumer] can authorize to collect [his] account information so [he] can view it at a single place on the Internet. [The consumer gives] the Web aggregator [his] account information (which may include checking, savings, insurance, mortgage, credit card, investment and brokerage accounts), [his] ID codes and passwords. In turn, the Web aggregator collects [his] account information online and allows [him] to access it, with a password, on its Web site for "one stop" viewing.[3]

In other words, aggregation is the consolidation of on-line financial account information (*e.g.*, from banks, billers and brokerages) for on-line retrieval at one site. In a typical outsourcing arrangement, an intermediary (*e.g.*, a bank, brokerage firm or portal) agrees with a third party service provider to provide the service to consumers—the intermediary would then generally privately label the service and offer consumers access to it at the intermediary's website.[4] Alternatively, the two companies could

---

these, roughly 1.1 million had been active within the preceding ninety days. *See* Interview with Sukhinder Singh, Vice President of Yodlee (Jan. 18, 2002) [hereinafter Yodlee Interview]. By the end of third quarter 2002, published reports indicate that Yodlee had three million users (but that less than 50% of these are active). *See, e.g.*, Priya Malhotra, *Technology Market's Woes Aside, Yodlee Lands $2.4M*, AM. BANKER, Sept. 17, 2002, at 1; Lucas Mearian, *Online Aggregation Failing to Deliver ROI for Banks*, COMPUTERWORLD, July 8, 2002, at 7.

3. MORGAN STANLEY REPORT, *supra* note 1, at 21.

4. *See* Yodlee Interview, *supra* note 2; *see also, e.g.*, Thomas P. Vartanian, *Regulators Eye Electronic Banking Boundaries*, AM. BANKER, Sept. 21, 2001, at 20A; Megan J. Ptacek, *Aggregation Pits Banks Against Web Portals*, AM. BANKER, Dec. 8, 2000, at 1; Nicole Duran, *BITS Publishes Aggregation Guidelines*, AM. BANKER, Apr. 20, 2001, at 2; Larry Altman et al., *Run for the Money: The Battle for Online Aggregation Business*, BOOZ ALLEN HAMILTON, INC. ENEWS, Jan. 15, 2001, *available at* http://strategy-business.com/press/enewsarticle?art=15222&pg=0; Thomas P. Vartanian & Robert H. Ledig, *Scrape It Scrub It and Show It: The Battle over Data Aggregation* (2000), *available at*

co-brand the service and offer access to it through the intermediary's website[5] or the bank could provide an on-premises aggregation service solely in its own name based on technology/software that it either developed itself or licensed from a third party provider.[6] However, as the BITS Aggregation Services Working Group pointed out, "any company with any level of security can begin to offer aggregation services, potentially putting customers, financial institutions and even the aggregation model itself at risk."[7]

While several different models for aggregation services exist, the most prevalent method today is still "screen scraping," which involves the simulation of user behavior to access the financial account website and to scrape account summary information from the site.[8] With screen scraping, it is necessary for the consumer to disclose primary authentication credentials (i.e., the username and PINS) for the financial account's site to the aggregator in order for the aggregator to access the financial account.[9] This information is stored on the aggregator's servers to avoid having users re-enter it

---

http://www.ffhsj.com/bancmail/bmarts/aba_art.htm (last visited Apr. 2, 2003). BITS has recently pointed out that "the vast majority of aggregation services offered by [financial institutions] are outsourced to third-party vendors." BITS, BITS AGGREGATION SERVICES REQUEST FOR INFORMATION, May 2002, at 6, *available at* http://www.bitsinfo.org [hereinafter BITS RFI]; MORGAN STANLEY REPORT, *supra* note 1, at 14; BITS VOLUNTARY GUIDELINES, *supra* note 2 (defining the roles that various entities play in account aggregation.

5. *See* Yodlee Interview, *supra* note 2.

6. *See* Priya Malhotra, *UMonitor Mining Small-Bank Aggregation Market*, AM. BANKER, June 21, 2002, at 10.

7. BITS, PROPOSED BITS MINIMUM BUSINESS REQUIREMENTS, GUIDELINES AND RECOMMENDATIONS FOR AGGREGATION SERVICE PROVIDERS PHASE I (Nov. 8, 2000), *available at* http://www.bitsinfo.org [hereinafter BITS PROPOSED GUIDELINES].

8. *See, e.g.*, Raymond Graber, *Aggregation and the Limits of Screen Scraping*, AM. BANKER, Nov. 13, 2001, at 10A (indicating that "[a]ccording to TowerGroup estimates, 70% of account aggregation information is gathered through screen scraping."); Roth, *supra* note 2; Malhotra, *supra* note 6 (indicating that Yodlee now uses screen-scraping to collect 65% of the account data it presents, down from 100% initially, and that by contrast 90% of Teknowledge's data currently comes from screen-scraping).

9. *See* BITS RFI, *supra* note 4, at 3.

on each subsequent visit.[10] The aggregator issues the consumer a username and password for the aggregation site itself.[11] Where screen scraping is used, the aggregator may have no contractual relationship with the AHBank and that financial institution may assume no responsibility to make sure that the aggregator accurately reflects the scraped information.[12] Individual aggregators retain different amounts (*e.g.*, one month of historical data as compared to three months) and types (*e.g.*, summary credit card account balances as compared to individual transaction details) of account data for different periods of time.[13] Potential alternatives to screen scraping include transfer of data over the Internet based on agreement between the aggregator and the financial account provider.[14] Work is ongoing at this time in various industry groups to promote the data feed of financial account data to aggregators in a reliable manner.[15]

---

10. *See id.*; MORGAN STANLEY REPORT, *supra* note 1, at 14.

11. *See* MORGAN STANLEY REPORT, *supra* note 1, at 14; BITS VOLUNTARY GUIDELINES, *supra* note 4, at D17–18.

12. *See* BITS PROPOSED GUIDELINES, *supra* note 7, at J-1.

13. *See* MORGAN STANLEY REPORT, *supra* note 1, at 16.

14. *See* BITS RFI, *supra* note 4, at 5 (describing "screen scraping" as the most commonly used technology used in aggregation and indicates that the intent of the RFI is to "elicit feedback from the aggregator provider vendor community on potential solutions that address the problems faced with the current mechanisms, processes and technologies used in account aggregation.").

15. *See, e.g.*, BITS RFI, *supra* note 4 (indicating that BITS intends to use responses to the RFI to "help develop industry guidelines for authentication and data exchange models that support enhanced financial aggregation services."). In addition, BITS:

> [S]eeks to determine the best alternatives to improve financial service authentication and data exchange practices. More specifically, the RFI seeks to understand options for improving safety and soundness in aggregation services that eliminate the requirement to share customer credentials with external third parties not contractually responsible to the RFI .... Also, the RFI seeks to explore complementary data feed options which ... will provide efficient, auditable and non-reputable traceability of services initiated by the RFI's customer or designated authorized agent.

BITS RFI, *supra* note 4, at 8; *see also* Duran, *supra* note 4 (describing BITS's voluntary guidelines for aggregation and its ongoing work to "eliminate screen scraping."); Carol Power, *Will OFX Be the Online Data Exchange Standard?*, AM. BANKER, Sept. 8, 2000, at 10A. The Financial Services Technology Consortium ("FSTC") has undertaken an Aggregation Initiative to identify,

Predictions are that aggregation services will evolve to become part of financial institutions' overall online banking efforts, and that financial transactions (*e.g.*, the ability to initiate fund transfers between aggregated accounts and third parties) will likely be included as a basic part of aggregation service.[16] Additionally, the use of aggregation services by financial advisors and in connection with providing investment recommendations on-line to the "mass affluent" are being explored as potentially viable niche markets.[17]

Why would a consumer authorize aggregation? The primary reason suggested in the Morgan Stanley Report is:

> [S]imply because it will make managing their financial lives much easier. In our opinion remembering only one password for all your accounts, logging into those accounts with one click, and viewing consolidated financial data on one page really does make life easier. In the near future, however, we expect aggregation to become even more useful to consumers when new technologies like funds transfer, bill payment, online advice, and wireless aggregation are widely deployed.[18]

However, a number of commentators have questioned the value of aggregation services to consumers and suggested that what is available on aggregation sites is of limited interest to most consumers.[19] Contrary to the Morgan Stanley Report's

---

develop and pilot needed common protocols, connectivity and capabilities to eliminate the sharing of credentials and to eliminate the need to screen scrape financial data. *See* FSTC, Aggregation Initiative Design Phase Proposal, *available at* http://www.fstc.org/projects/fastaggregation.cfm.

16. *See* BITS RFI, *supra* note 4, at 3 (noting that "[a]dditional functionality, incorporating funds transfer transactions and other higher risk processes, is emerging in the second phase of product development."); Steve Bills, *Online Banking: B of A Makes Its Case—We're the Online Bank of America*, AM. BANKER, Apr. 11, 2002, at 1.

17. *See, e.g.*, Chris Costanzo, *Working Out the Kinks in Serving the Mass Affluent*, AM. BANKER, Aug. 20, 2002, at 4A; Dave Yonamine, *Is There Justification for Aggregation? The Value of Account Aggregation for the Affluent*, *in* ABA TRUSTS & INVESTMENTS, 33 (2002); Priya Malhotra, *CashEdge: Advisers the Best Aggregation Clients*, AM. BANKER, July 26, 2002, at 11.

18. MORGAN STANLEY REPORT, *supra* note 1, at 25.

19. *See, e.g.*, Yonamine, *supra* note 17; Lynn Cowan, *All in One—Account Aggregation Software May Work Better in Theory Than in Practice*, WALL ST. J., Oct. 29, 2001, at R17.

conclusions, a senior analyst with technology consulting firm Tower Group recently suggested that the adoption rates are low because of consumer's privacy, security and accountability concerns, indicating that "most consumers are waiting for additional value manifested in new services such as funds transfer and advice, before taking the plunge."[20] Similarly, the value of aggregation services to financial advisors has been the subject of some disagreement.[21]

Why would a financial institution offer aggregation services to its customers? The Morgan Stanley Report identified several benefits including customer retention, brand enhancement, and new sources of revenue.[22] However, the value of aggregation to

---

20. Graber, *supra* note 2; *see also* Roth, *supra* note 2 ("People in the high-net-worth-bracket are the most active users of aggregation and stand to benefit most from the next phase of its development."). The next phase apparently includes financial planning, portfolio analysis and investment planning plus the ability to transfer funds between accounts and to pay bills. It appears that this next phase will require a shifting away from screen scraping and toward direct data feeds from AHBanks. According to Jack Pullara, a senior manager at PricewaterhouseCoopers:

> What is keeping more customers from signing up? Apart from the security and privacy pitfalls that many customers express as serious concerns, there is the issue of functionality. What is the real benefit of being able to see account data from five or so different companies that I do business with, presented on the same Web site, if it means exposing myself to identity theft or other potential misuse of my very private financial data? . . . Aggregators and financial institutions must remember that the currently limited functionality does not justify the risks that consumers must assume.

Pullara, *supra* note 2.

21. *See, e.g.*, Costanzo, *supra* note 17; *Banks Pin Their Back-Office Hopes on Successors to Screen Scrapers*, U.S. BANKER, Aug. 2002, at 24 (noting that "[f]or all the hoopla about account aggregation and its benefits to financial advisers, there has not been much to show for it," suggesting that since: (a) the scraped data "is a snapshot and does not include a customer's investment history"; and (b) screen scraping can provide "an inaccurate picture of a customer's financial situation" given that "[w]eb sites update data at different times," it is difficult for financial advisors/representatives to provide timely and accurate advice based upon it). *Cf.* Malhotra, *supra* note 17.

22. MORGAN STANLEY REPORT, *supra* note 1, at 25. *But see* Jessica Toonkel, *As Aggregation Gains, Doubt on Cross-Selling*, AM. BANKER, Sept. 19, 2000, at 1 (reporting that early-on cross-selling was seen as a potential revenue source from aggregation but that customer surveys indicate that this may be counterproductive).

financial institutions has also been questioned. A summer 2001 report by Forrester Research is frequently quoted for questioning the value of aggregation and concluding that most firms should not bother with it today as "*[t]here's no [return on investment] ROI on aggregation.*"[23] The report observed that "[a] good number of banks say that the No. 1 reason they offer account aggregation is to increase customer retention, 'but that's bogus.' Bankers are abusing the retention benefit and are using it for every technology. That makes it almost impossible to measure a product's value."[24]

During periods of economic downturn, financial institutions carefully scrutinize all of their expenses and investments in technology; aggregation has gotten some negative attention in this context.[25] Thus, at this time, aggregation may be at a crossroads. It had a fairly dramatic and well-publicized early adoption by

---

23. Lauren Weber, *Aggregation Gaining Converts, If Not Fees*, AM. BANKER, Sept. 21, 2001, at 11A (quoting Catherine Graber, *Account Aggregation: The Elusive ROI*, *in* 2001 FORRESTER RESEARCH REP)) (emphasis added); Lauren Weber, *In Brief: Aggregation Merger: Adhesion and Ettache*, AM. BANKER, Aug. 17, 2001, at 13; Mark Bruno, *Questions About Aggregation*, U.S. BANKER, Oct. 2001, at 48; *see also* Megan J. Ptacek, *Aggregation Revenue-Drain Pegged at $28B for Banks*, AM. BANKER, Apr. 17, 2001, at 12 (citing consulting firm Novantas for the projection that banks offering aggregation stand to lose up to $28 billion of revenue to customers moving their money to accounts that earn more interest); Julie Monahan, *Banks Still Focusing on Yodlee's Potential*, AM. BANKER, Nov. 13, 2001, at 6A.

> Recent statistics seem to make one wonder why organizations are making the not-so-small investment in account aggregation. Companies who have signed up with aggregation service providers have discovered that the services certainly do not qualify as a cheap date; it costs roughly half a million dollars to implement Yodlee's account aggregation software on a company's Web site, and then there is the $8–$12 that Yodlee collects per user per year.

Pullara, *supra* note 2. *But see* Yodlee, *supra* note 2 (disagreeing with Ms. Graber's conclusion).

24. Bruno, *supra* note 23.

25. *See* Andrew Roth, *Slow Growth Expected in Bank Tech Spending*, AM. BANKER, Nov. 13, 2001 at 4A.

> Banks are rethinking their investments in technology now that the days of the 'blank check' are gone. As banks examine their IT budgets, peripheral technologies, those that lack a specific return on investment are being carefully scrutinized. The function that has been drawing perhaps the greatest attention is account aggregation, leaving many bankers and techies to ask whether the investment is worth it.

Bruno, *supra* note 23.

financial institutions in 2000 but its value from the customer retention and ROI standpoint still appears to be in question as of mid 2002.[26]

II. WHAT ARE THE POTENTIAL FINANCIAL LIABILITIES RESULTING FROM AGGREGATION?

According to the Morgan Stanley Report, aggregation involves a distinct set of risks for the companies that offer the service and for the consumers that use it.[27] The AHBanks' primary financial liability concerns with screen scraping-based aggregation involve the exposure of usernames and PINS to aggregators.[28] However, as

---

26. *See, e.g.*, Geoffrey Smith, *Account Aggregation Falls Apart; This Ballyhooed Online Service Has a Fatal Flaw: You Can See All Your Financial Data at One Site, But You Can't Manipulate It*, BUS. WEEK ONLINE, July 3, 2002; Jeremy Quittner, *Online Bill Payment Gains Popularity While Customers Eschew Aggregation*, AM. BANKER, July 23, 2002, at 6A; Marija Potkonjak, *Trendspotters See Advice Redefining Aggregation*, AM. BANKER, Aug. 20, 2002, at 8A; Amanda Fung, *Wary Bankers Tiptoe into Account Aggregation*, AM. BANKER, Apr. 10, 2002, at 12A; Nuala Moran, *Banks and Customers Take Time To Get It All Together: Account Aggregation*, FIN. TIMES (London), Sept. 4, 2002, at 6.

27. MORGAN STANLEY REPORT, *supra* note 1, at 28.

28. *See, e.g.*, OCC, BULLETIN ON BANK-PROVIDED ACCOUNT AGGREGATION SERVICES 2–6 (Feb. 28, 2001) (discussing potential risks from aggregation), *available at* http://www.*occ.treas.gov/occ_current.htm* [hereinafter OCC]; BITS RFI, *supra* note 4, at 6; MORGAN STANLEY REPORT, *supra* note 1, at 28–30. The Morgan Stanley Report concisely summarizes the basic risks of aggregation. With respect to the legal liability risk it notes:

> Liability. One largely unsettled issue concerning aggregation is the future of government regulation and legal liability. There are two principal pieces of legislation through which account aggregation will be regulated in the future . . . .
>
> The first is the Electronic Fund Transfer (EFT) Act of 1978 . . . Since many legal experts think that online banking and brokerage Web sites fall under the domain of electronic devices, liability for transactions processed through those Web sites still rests with the financial institution. Therefore, even if a transaction is initiated on an aggregated page (based on inaccurate data, potentially), liability for that transaction still appears to rest with the concerned financial institution.
>
> The banking industry is obviously not pleased with that interpretation of the Electronic Funds Transfer Act. As a result, the Federal Reserve is currently deciding whether Regulation E will also apply to aggregators, to ensure that liability for transactions rests with the party at which the transaction is initiated.

MORGAN STANLEY REPORT, *supra* note 1, at 28–30.

the possibility of aggregation services supporting funds transfers from one AHBank to another becomes a reality, concerns about data accuracy and credentials management (i.e., authentication of the identity of parties accessing data) are taking on added significance.[29] In the early days of aggregation, concerns also focused upon the basic inability of financial institutions to identify aggregators accessing a consumer's account.[30] In today's environment, AHBanks appear to be generally able to track whether or not a particular access to or transaction against a financial account was initiated by the consumer or was made by an aggregation site (and, if by an aggregator, the identity of the aggregator).[31]

Two primary ways in which use of aggregation sites by consumers might result in financial loss have been suggested in critiques of the service.[32] Generally, these are financial loss related to reliance upon bad account data and unauthorized transactions

---

29. *See* BITS RFI, *supra* note 4, at 5, 6–8.

30. *See* BITS PROPOSED GUIDELINES, *supra* note 7, at G-1.

31. *See* Yodlee, *supra* note 2 (indicating that an AHBank can review its server log to track the URL from which an inquiry or transaction is initiated and can identify an aggregation site from the URL).

32. Risks to consumers include:

> Security. Since aggregation requires that consumers sign over access to their accounts, it raises the risk that someone could gain unauthorized access to those accounts. If a hacker (or, potentially, even a criminally minded employee) were to crack into an aggregation data network, he would acquire a panoply of personal account information as well as the passwords to access those accounts. He could then use those passwords to transfer money out of certain accounts, or at least to wreak havoc by conducting unauthorized transactions. Although we are not aware of any such security breaches, the possibility does exist.
>
> * * * *
>
> Data accuracy. Given that many consumers will rely on the data on their aggregated pages to make financial decisions, aggregation also creates the risk that inaccurate or delayed data could lead users to make ill-informed financial decisions. For example, a consumer could check stock prices on his aggregated page and then decide to execute a transaction based on the data displayed there. If the data collected from his brokerage account had not been updated for a few hours, he could conceivably execute the transaction at a price different from the price displayed on his aggregated page. In the worst case, the customer might rely on inaccurate data on his aggregated page (since screen scraping is not 100% accurate) to make financial decisions.

MORGAN STANLEY REPORT, *supra* note 1, at 28.

or actions leading to loss.[33] While these issues of liability and financial loss come up frequently in articles and discussions, generally the discussions appear to be theoretical rather than based on practical problems that are actually being raised with AHBanks by customers.[34]

A. Display of Inaccurate, Incorrect or Incomplete Data

The first potential problem involves the display of bad account data at the aggregation site.[35] If a consumer thinks that he is viewing real-time information about his checking account and writes a check based on that information, the consumer could suffer embarrassment or financial loss if, in fact, the information is two days old and there are insufficient funds remaining in the account to cover the check.[36]

Screen scraping does not guarantee 100% accuracy in the data collected—changes in Web site layouts and the addition or removal of links to account information can result in the retrieval of

---

33. *See id; see also* BITS RFI, *supra* note 4, at 5, 6–8.

34. *See, e.g.*, Graber, *supra* note 2; Roth, *supra* note 2. The author has not found any *American Banker* articles reporting on situations where an AHBank or its customer has actually attempted to obtain reimbursement for a financial loss claimed to be attributable to the customer's participation in an aggregation site. Discussions with a smattering of knowledgeable bank lawyers, vendor representatives, and regulatory personnel at the end of 2001/beginning of 2002 did not uncover reported instances of such customer or AHBank loss.

35. With screen scraping, concerns have been expressed about the low quality of scraped data and completeness, and its use in transactions. For example:

> Account aggregation is useful because of customization—users' ability to tailor the service to their preferences.... This, however, is predicated on the assumption that the provider can deliver clean, accurate, and timely data. One financial institution offering aggregation is experiencing a 20% error rate in its overnight batch collection, mainly because of slip-ups that occur in data transportation, lack of familiarity with the aggregation provider, and customers changing their passwords without informing the aggregation provider.

Graber, *supra* note 2.

36. As summarized by the OCC, "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." OCC, *supra* note 28, at 3.

inaccurate information.[37] Inaccurate data can also result if the aggregator bypasses safeguards and data checks that the AHBank would otherwise have in place to detect or prevent errors.[38] Problems can be inherent in aggregation if the consumer does not understand the time lags and other constraints surrounding the display of data by the aggregator or the underlying AHBank site.[39]

---

37. For example:

> Current aggregation services rely on screen scraping as a primary data collection mechanism. As such, they are constantly struggling with changes in source data, website designs, data placements and formats. Additionally, since one of the major premises of account aggregation is to provide the end consumer with a consistent and integrated view, the ability to do so with data from a myriad of sources poses its own challenges. For example, one website might provide negative financial balances with a number preceded by a dash "-" while another might indicate the same through color or by position in a particular column.

BITS RFI, *supra* note 4, at 6.

38. *See, e.g.*, Graber, *supra* note 8 (detailing a discussion of the practical data accuracy/ timeliness problems with using screen scraping as a basis for aggregation). In late 2001, Mr. Graber estimated that "success rates for overnight batch-processing data-gathering are about 75%," and indicated that: "[S]creen scraping cannot guarantee the accuracy and timeliness of data that consumers expect from financial institutions. Inaccurate data will eventually undermine consumer confidence–and consumers will stop using aggregation services dependent on this technology." *Id.*

39. Generally screen scrapers utilize a time stamp mechanism which shows the time and date that data is updated by the screen scraper. *See* Yodlee, *supra* note 2. The primary questions that arise involve old data at the scraped site and whether the scraper is able to access a site to refresh information (*e.g.*, if the aggregator attempts to access a site when that site is being updated, the aggregator is unable to obtain access). Yodlee advises that, in reality, customers don't seem to have problems with confusion over old data—customers may be concerned that data is old, but, generally, they understand that it is old. *See id.*

> As important as the accurate and consistent interpretation of the data collected is the timeliness of its collection. Again, in the screen scraping model, financial institution websites might update daily account balances at various times during the day. Synchronizing such information without cooperation of the source data institution can be difficult and inconsistent.

BITS RFI, *supra* note 4, at 6

The lengthy, comprehensive disclaimer language used in the Terms and Conditions governing access to aggregation Web sites of such major financial institutions as Citibank and JP Morgan Chase are indicative that these institutions have a clear understanding of the limitations on the data provided at such sites. *See, e.g.*, Chase Online Plus Web, *at* http://www.chase.com (last visited

It should be pointed out that these same problems may well exist at a financial institution's on-line banking website today and that the data provided at such sites is not necessarily real time. Financial institutions differ on their own on-line banking websites as to the timeliness of data updates and disclosure of the limitations of displayed data.[40] With respect to who is responsible for financial losses caused by reliance on bad account data, no court decisions providing direct guidance on this issue appear to have been reported. This is not particularly surprising given the relative youth of aggregation services. Nor has the author found evidence in the trade press or in discussions with industry participants suggesting that consumers perceive themselves to be suffering any significant real dollar losses due to participation in aggregation.

1. Aggregator Liability

Whether or not an aggregator would have legal liability to the consumer for losses suffered as a result of reliance on bad account data displayed at the aggregation site is an open question.[41] The

---

Apr. 2, 2003); Myciti Web, *at* http://www.myciti.com/terms.html (last visited Apr. 2, 2003). The Chase Online Plus Terms and Conditions runs more than three pages—it contains numerous different lengthy disclaimers of liability, including: "Because of the possibility of human and mechanical error as well as other factors, the website (including all information and materials contained on the website) is provided 'as is' 'as available.' JPMorgan Chase and third party data providers are not providing any warranties and representations regarding the website." Chase Online Plus Web, *at* http://www.chase.com (last visited Apr. 2, 2003).

40. *See, e.g.*, BITS RFI, *supra* note 4, at 6; *see also* First USA Bank, N.A., which makes the following disclaimer with respect to data displayed on its Web site:

> We will use our best efforts to include accurate and up to date information on the Site, but we make no warranties or representations as to the accuracy of the information. You agree that all access and use of the Site and its contents is at your own risk. By using the Site, you acknowledge that we specifically disclaim any liability (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages arising out of or in any way connected with your access to or use of the Site . . . .

First USA Web site, Terms of Use, *at* http://cardmemberservices.firstusa.com/globals/terms.html (last visited Apr. 2, 2003).

41. *See, e.g.*, Roth, *supra* note 2, in which Mr. Roth stated:

consumer's argument in favor of aggregator liability might be that: (1) the aggregator was offering a service (particularly a fee-based service) based upon account data that it knew was so suspect and unreliable that its offering constituted negligence and (2) the presence of mice-type liability disclaimers and/or the wording used in such disclaimers was not adequate to inform the consumer of data limitations or that reliance upon information provided by the aggregation service might result in financial losses.[42]

The aggregator could probably limit, and even eliminate, any potential legal liability by appropriately advising the consumer in the aggregation site's "Terms and Conditions of Use" of known limitations on the accuracy, completeness or correctness of data using understandable language in a clear and readable format. However, whether inclusion of a disclaimer or whether the specific disclaimer language would be adequate to eliminate aggregator liability to the consumer in a given situation would generally be a question of fact.[43]

2. AHBank Liability

Despite the lack of reported precedent, logic suggests that a consumer should not be able to impose legal liability upon an

---

If the players fail to address the accuracy issue, it could be costly for all those involved: financial institutions, vendors and customers. What these parties don't sort out among themselves could be sorted out in the courts, because it is unclear where blame will fall if erroneous information results in financial loss.

"There is not a lot of law out there right now, no guidepost in terms of the court stepping in." said John Burke, counsel to BITS and an attorney at Foley Hoag LLP in Washington. "How you get information—what its currency is in terms of accuracy and who will be liable if consumers make a bad judgment based on data that is provided through an aggregation service—will only be resolved if there is litigation." he said. So far he has not heard of any such lawsuits.

"Screen scraping is a pretty clunky technology." Mr. Burke said. "Using consumers' access codes, you don't know when the Web site was modified or updated, or, frankly, what the accuracy of the data is."

Id.

42. *See generally* Roth, *supra* note 25, at 6A.

43. The author has been advised by Yodlee that aggregation sites generally attempt to limit their liability in the Terms and Conditions displayed at the site. *See, e.g.*, Chase Online Plus, *supra* note 39; Myciti Terms and Conditions, *at* http://www.myciti.com/terms.html (last visited Apr. 2, 2003).

AHBank in situations where the consumer's financial loss resulted from reliance on bad account data displayed at a third party aggregation site where the incorrect information has been screen scraped from the AHBank without its consent.[44] General principles of fairness and equity should not support imposition of such liability. The conclusion should not change where the AHBank is providing data to the aggregation site via a data feed arrangement at the specific request of the consumer; assuming, of course, that the data provided by the AHBank was accurate and was provided to the aggregator in accordance with agreed upon specifications.[45]

An AHBank could improve its already strong position by clearly stating in its account documentation that it has no responsibility and disclaims all liability for manipulation or display of account data by unrelated third parties, specifically including data provided to an aggregator at the consumer's request. Legal counsel could reasonably advise the AHBank to refuse to voluntarily assume responsibility for bad account data displayed at an unrelated aggregation site. These conclusions assume, naturally, that the information at the base AHBank website was accurate, appropriately displayed, and labeled at that site with whatever data limitations exist (*e.g.*, that the data displayed is as of midnight on the previous business day).

Of course, in special situations, the AHBank officer responsible for the customer relationship could make a voluntary concession and reimburse the customer for the loss. A concession

---

44. *See* Graber, *supra* note 2.

45. The conclusions expressed in this paragraph represent the author's views, based upon nearly thirty years of experience practicing law in the consumer financial services area, of what the results *should be* if litigation does arise. However, in the absence of controlling precedents, differing conclusions are certainly possible. "[C]larity, simplicity and uniformity have been in short supply in the consumer financial services arena in recent years." Lynn B. Barr et al., *Introduction to the 2001 Annual Survey of Consumer Financial Services Law*, 56 BUS. LAW. 1084, 1087 (2001). The authors' further point out that: "Clearly, this is a time of major and rapid changes in consumer financial services law, with long-standing and fundamental principles being constantly questioned and either defended or swept away, and new legal issues being asserted, confronted and resolved for the first time." *Id.*

might be made based upon account profitability, length of relationship or other factors (such as the negative impression given of the AHBank if it refuses to handle a complaint made by an 89 year old customer to her satisfaction). Additionally, the AHBank could contractually agree with its customer to assume liability for losses suffered due to bad data appearing on its home banking site.

B. Unauthorized Transactions or Unauthorized Actions

The second problem area involves unauthorized transactions or actions occurring as a result of information being provided to the aggregation site. While a number of potential scenarios could result in unauthorized transactions, they fall into two basic categories.

1. External Event or Act

The first type of scenario involves a hacker accessing the site, obtaining information and subsequently using it to perpetrate an unauthorized transaction or to undertake other fraudulent activity. The BITS Working Group, in attempting to define minimum security requirements for "trusted" aggregation services, has articulated that the general framework for implementation should be designed to protect the most sensitive information from direct Internet access (i.e., to reduce impacts from a single compromise of a server).[46] The Morgan Stanley Report made the following observation about the dangers of aggregation: simply put, an aggregation site is a hacker's dream. The wealth of passwords, personal data, and access to financial accounts that aggregation sites contain could make breaking into one aggregation site more worthwhile than breaking into hundreds of individual sites.[47]

2. Internal Event or Act

The second type of scenario involves the use of information obtained from a site to make an unauthorized transaction by those

46. *See* BITS PROPOSED GUIDELINES, *supra* note 7, at F-1.
47. *See* MORGAN STANLEY REPORT, *supra* note 1, at 9.

providing the site, or their agents or employees. The BITS Working Group has noted that "although focus is often placed on the Internet and the hacker, reality is that 75% to 85% of all compromises occur from within a corporation."[48] By mid-2002, no reported court decisions have been identified providing direct guidance on the issue of who is responsible for financial losses caused by participation in an aggregation service. Nor has the author identified anything suggesting that significant problems are being reported by consumers. However, in discussing liability issues, clearly the conclusions depend on many factors and will differ depending upon specific fact situations. The answer to the question of *who* has liability depends on the particular problem encountered by the consumer and is discussed in detail in Parts III and IV below.

III. SIMPLE ANSWERS—AS TO WHO HAS LIABILITY FOR UNAUTHORIZED TRANSACTIONS

If an unauthorized transaction is made from a consumer's financial account, the simple answer as to who bears the financial loss under the law as of the middle of 2002 is that the responsibility varies depending on the type of unauthorized transaction and/or the account from which the unauthorized transaction is made.[49] Also, lawyers may argue and disagree as to the simple answer and what the law is based on the parsing of words and differing conceptualizations of fact situations.

A fairly simplistic view of current laws and regulations suggests that generally the consumer is required to be protected and to be made whole, and initial responsibility to make the consumer whole will be borne by an AHBank.[50] However,

48. *See* BITS PROPOSED GUIDELINES, *supra* note 7, at F-4.

49. *See* Monahan, *supra* note 23; *see also* Thomas Vartanian, *Regulators Eye Electronic Banking Boundaries*, AM. BANKER, Sept. 21, 2001, at 20A.

50. At a September 11–12, 2000 Conference on Account Aggregation sponsored by Thomson Financial Media, a panel of lawyers discussing "Aggregation—Legal and Public Policy Issues" expressed the general views that: (1) the consumer is not at risk of loss for unauthorized transactions if the aggregation business is to survive; and (2) if the consumer suffers a loss because of the aggregator's negligence or misfeasance and the aggregator is not able to pay, the consumer will get reimbursement for his loss from the bank. *See* Sarah

notwithstanding the current laws and regulations, generally: (1) due to various payment processing associations' contractual agreements and the charge-back rules between financial institutions, the ultimate responsibility for absorbing the financial loss in a number of the fact situations described in this Part III may well rest with a financial institution other than the AHBank, (2) due to various private contractual arrangements between financial institutions and their corporate or business customers, responsibility for loss may shift to that corporate orbusiness customer, and (3) due to industry cooperative practices, an AHBank may be able to obtain reimbursement (based upon appropriate indemnification or legal protection by the AHBank) from another financial institution that would then look to its customer for reimbursement.

The following fact situations can arguably give rise to the following simple legal answers—these answers assume that *no* aggregation site has been used by the consumer. Part IV, "EXCEPTIONS TO 'SIMPLE ANSWERS' (where the consumer has arranged for aggregation)," will examine if and how the SIMPLE ANSWERS change as a result of the consumer having authorized aggregation by a third party.

A. Unauthorized ACH Debit Drawn on Checking Account

If the unauthorized transaction is caused by an Automated Clearing House ("ACH") debit drawn against a checking account, the AHBank is required to reimburse the consumer under the Electronic Fund Transfer Act ("EFTA") and Regulation E ("Reg

---

Jane Hughes, *Promoting the Use of Electronic Payments: What Role Will/Can Consumer Protection Play?*, Oct. 11, 2000, at 5 (paper presented at the Federal Reserve Bank of Chicago Workshop on promoting the use of electronic payments) (on file with the Federal Reserve Bank of Chicago). Banks and legal commentators have expressed the generalized concern that:

> Unlike vendors that the bank may supervise directly or commission to create a product for the bank, third-party aggregators have no contractual relationships or other allegiance to the bank and they cannot be required to warrant their work or procure insurance, or to hold the bank harmless in case of error. *For this reason, I have a recurring nightmare that banks may keep the risk of liability despite the inability to control this non-bank intermediary in any way . . .*

Id. (emphasis added).

E").[51] This liability is subject to the AHBank's right to impose limited liability upon the consumer depending upon the time frames within which the consumer notifies it of the unauthorized transaction or the loss or theft of the access device.[52]

Further, the AHBank would have rights under the rules and regulations governing the ACH Network ("ACH Rules") to transmit an adjustment entry for the unauthorized debit to the bank of first deposit ("ODFI"), again assuming that timing and other technical requirements could be satisfied.[53] The ODFI probably would have contractual rights to charge-back the unauthorized transaction to its customer.

B. Unauthorized Purchase on Credit Card Account

If the unauthorized transaction involves an unauthorized merchandise purchase charged to a credit card account, the card issuing financial institution is responsible for the loss under the Truth in Lending Act ("TILA") and Regulation Z ("Reg Z").[54]

---

51. *See* 15 U.S.C. § 1693g (1994); 12 C.F.R. § 205.6 (2001).

52. *See* 15 U.S.C. § 1693g; 12 C.F.R. § 205.6 (limiting the consumer's liability for an unauthorized EFT to $50 if the consumer notifies the financial institution within two business days of learning of the loss or theft of the access device). The amount is limited to $500 if the consumer doesn't notify the AHBank within two business days. *See* 15 U.S.C. § 1693g; 12 C.F.R. § 205.6. If a consumer fails to report unauthorized EFTs that appear on a periodic statement, he can be held liable for all unauthorized EFTs that occur more than sixty days after the transmittal of the first statement reflecting the unauthorized EFTs. *See* 15 U.S.C. § 1693g; 12 C.F.R. § 205.6. However, both Visa U.S.A. and MasterCard International have adopted "zero liability" policies for debit card transactions processed over their networks—online or off—whereby the consumer is not to be held liable for any part of an unauthorized transaction. *See* Visa U.S.A., Inc., *Zero Liability*, at http://www.usa.visa.com/personal/secure_with_visa/zero_liability.html (last visited Apr. 2, 2003); http://www.mastercardintl.com/about/press/pressreleases.cgi?id=303.

53. *See* National Automated Clearing House Association (NACHA), 2001 ACH Operating Rules § 7.7.1. The adjustment entry must be made no later than the opening of business on the banking day following the sixtieth calendar day following the settlement date of the original entry.

54. *See* 15 U.S.C. §§ 1643, 1666; 12 C.F.R. §§ 226.12, 226.13 (authorizing the financial institution to hold the consumer responsible for the first $50 in

However, that financial institution would frequently have rights under the Visa and MasterCard charge-back rules to charge-back the unauthorized transaction to the bank (merchant acquiring bank) that acquired the transaction from its merchant customer, again assuming that timing and other technical requirements had been satisfied.[55] The merchant acquiring bank probably would have a contract with its merchant customer (merchant) giving it the contractual right to charge-back the transaction to the merchant.[56]

---

unauthorized transactions provided that certain procedural requirements are complied with). Here again, both Visa U.S.A., Inc., and MasterCard International have adopted "zero liability" policies whereby the consumer is not to be held liable for the first dollar of unauthorized transactions. *See supra* note 52 and accompanying text.

55. *See generally* Visa U.S.A., Inc., *Chargeback Management Guide for Visa Merchants* (2002), *available at* http://www.usa.visa.com/media/business/chargeback_mgt.pdf. This Guide explains the chargeback process and suggests preventive measures for merchants to take to minimize their recurrence. *Id.* Chapter Seven deals with Potential Fraud Chargebacks and Chapter Ten contains a summary description of the chargeback process and a diagram illustrating that process. *Id.*

56. The terms of the merchant's relationship with its acquiring bank (including the conditions under which the acquiring bank can chargeback a transaction to the merchant) are typically spelled out in a processing contract (the "merchant agreement"). Visa U.S.A., Inc. in an online communication addressed to potential Visa merchants includes a list of questions the merchant should ask before signing a processing contract. *See* Visa U.S.A., Inc., *Merchants—Accepting Visa—Get an Account, at* http://www.usa.visa.com/business/merchants/get_an_account_questions.html (last visited Apr. 2, 2003). Among the questions is whether it will be required to have a certain percentage of its sales dollars or specific dollar amounts held by the acquirer for chargebacks—this obviously assumes that the acquiring bank will specify in the processing contract the conditions under which chargebacks will be made. *Id.* Paymentech, L.P., a major merchant transaction processor, discusses chargebacks at its Web site. *See* Paymentech Web site, *available at* http://www.paymentech.net (last visited Apr. 2, 2003). The site includes an "Operating Guide for Mail Order/Telephone Order/Internet Transactions." *Id.* Section Five defines chargebacks as "the debiting of your Account or withholding of settlement funds for all or part of the amount of a particular sale as permitted by the Merchant Agreement." *Id.* Obviously, this also assumes that a processing agreement spelling out chargeback rights will be in place between the merchant and its acquiring bank.

C. Forged Drawer Signature on Check

If the unauthorized transaction is caused by a forged drawer signature or a counterfeit check drawn on a checking or open end credit account, the AHBank that pays the check is responsible for reimbursing the customer under the Uniform Commercial Code ("UCC").[57] Additionally, if the check is drawn against an open end credit account (*e.g.*, a cash advance check charged against a credit card account), the billing error provisions of TILA and Reg Z would require the AHBank to reimburse the consumer.[58] Further, if the check had been converted to an electronic form of payment, it would generally be considered an electronic funds transfer ("EFT") and the AHBank would be responsible for reimbursing the customer under EFTA and Reg E.[59]

While there is no general legal right for the AHBank to reverse the transaction under the processing rules for paper checks, it is always possible for a financial institution to attempt a consensual return to the depositary bank (a return without entry). Thus, if funds remain on deposit in the original account into which the forged or counterfeit check was deposited, the depositary bank might be persuaded (with appropriate indemnification or other protection such as a court order) to reverse the transaction and recredit the payor bank. Additionally, if the check had been converted to an electronic form of payment, the AHBank would have the right to transmit the check back to the ODFI for reimbursement under the ACH Rules, assuming that timing and other technical requirements could be satisfied.[60]

---

57. *See* U.C.C. §§ 3-401, 3-403 (1996); *see also* HENRY J. BAILEY & RICHARD B. HAGEDORN, BRADY ON BANK CHECKS: THE LAW OF BANK CHECKS ch. 28 (rev. ed. 1997).

58. *See* 15 U.S.C. § 1666; 12 C.F.R. § 226.13.

59. 15 U.S.C. §§ 1693f, 1693g; 12 C.F.R. §§ 205.6, 205.11; Official Staff Interpretations to Electronic Fund Transfer (Regulation E), 12 C.F.R. pt. 205, Supp. I, § 205.3(b)1.v.

60. *See, e.g.*, National Automated Clearing House Association (NACHA), 2001 ACH Operating Rules § 7.7.1 (concerning PPD Accounts Receivable Truncated Check Debit Entries). The ODFI warrants that "all signatures on the item to which the PPD debit entry relates are authentic and authorized." *See* ACH Rule, § 2.9.3.4. If this warranty is breached, the ODFI indemnifies the RDFI against all liability and expense "resulting directly or indirectly from the

D. Identity Theft—Credit Account

If a financial institution suffers losses due to opening a credit account for the perpetrator of an identity theft, that financial institution would take the loss when charges are made against the credit account and payments for those charges are not received. The consumer whose name is stolen and used should generally have no financial responsibility.[61] However, despite having said that, the consumer may well experience practical difficulties in persuading the credit account issuing bank that identity theft was involved in the opening of the account and in clearing his credit report of information resulting from the identity theft.

E. Identity Theft—Asset Account

If a checking or other deposit account is opened for the perpetrator of an identity theft, the financial institution that opens the account generally takes any resulting losses (*e.g.*, if deposits into that account are returned unpaid and no funds remain on deposit in the account to offset against).[62] Again the consumer

---

breach . . . ." ACH Rule, § 2.9.3.11. The RDFI has the right to transmit an adjustment entry to the ODFI providing that technical requirements are met not later than the opening of business on the banking day following the sixtieth calendar day following the Settlement Date of the Debit Entry. *See* ACH Rule, § 7.7.13(2). If an electronified check were presented under the POP (point-of-purchase) program, general ACH Rules would provide for similar adjustment entries in the event of an unauthorized transaction. *See* ACH Rule § 7.7.1.

61. Though this issue has not been settled, the federal government and many states are considering bills to explicitly hold financial institutions liable to consumers for losses suffered from identity theft. *See Security: The Politics of Identity Are Stirring*, FUTURE BANKER, Oct. 2001, at 10. This type of protection can be observed in the protection provided to a consumer when an imposter succeeds in validating an unsolicited access device to a financial institutions failure to correctly verify the consumer's identity. *See* Official Staff Interpretations to Electronic Fund Transfer (Regulation E), 12 C.F.R. pt. 205, Supplement I, § 205.5(b)4.

62. The most likely scenario here would probably be the deposit into an account opened by the thief of stolen checks payable to a real consumer bearing an endorsement made by the thief. Under the UCC, a bank which accepts a check for deposit warrants that all signatures on the item are authentic and authorized. *See* U.C.C. § 4-207 (1996). If this warranty is breached, the

whose name is stolen and used should generally have no financial responsibility; however, he may experience practical difficulties in clearing his credit records and dealing with the financial institution. Table 1 below summarizes the SIMPLE ANSWERS described in this Part.

An additional issue is whether reimbursement to the innocent consumer will include reimbursement of fees imposed by the AHBank (*e.g.*, Non-Sufficient Funds ("NSF") check fees in connection with legitimate checks bounced as a result of unauthorized transactions drawing down the funds in a checking account). Reasonable business practices as well as regulatory requirements should cause this to happen.[63] Less clear is whether the AHBank will reimburse the consumer for charges imposed by other third parties as a result of problems created by erroneous or unauthorized transactions (*e.g.*, bounced check fees imposed by a retailer on a check returned because an account was drained of funds by unauthorized transactions).[64]

---

depository bank is responsible for reimbursing the payor bank (and any other collecting banks) based upon the breach of its warranty. *Id.*

63. Under both Regulation E and Regulation Z, the consumer alleging an unauthorized transaction would be entitled to be credited for interest and fees imposed by the AHBank. *See* Official Staff Interpretations to Electronic Fund Transfers (Regulation E), 12 C.F.R. pt. 205, Supp.I, § 205.11(c)6; Reg Z, 12 C.F.R. § 226.13(e)1 (2001). However, the AHBank is apparently not able to charge-back the amount of such finance charges or fees to the ODFI or merchant-acquiring bank under existing ACH or credit card charge-back rules.

64. Under U.C.C. § 4-402 (1996), a payor bank that wrongfully dishonors a check is liable to its customer for damages "proximately caused" by dishonor of the check. *Id.* With respect to unauthorized EFTs, reimbursement is not required by the error resolution requirements of Regulation E and is arguably not required under the billing error resolution requirements of Regulation Z. *See* Official Staff Commentary to Regulation E, 12 C.F.R. pt. 205, Supp. I, §205.11(c)6; Reg Z, 12 C.F.R. § 226.13(e)1. However, an individual AHBank may consider such reimbursement prudent as a relatively small concession to terminate contentious discussions with aggrieved consumers; it may consider such reimbursement required by the U.C.C. if the unauthorized transaction (either EFT or forged check) caused the wrongful dishonor (bouncing) of a legitimate check and the fee is connected to that wrongful dishonor.

Table 1: Summary of Simple Answers As to liability for Unauthorized Transactions Where a Customer Has No Aggregation Arrangement

Type of Transaction	Is the AHBank responsible for loss under the law?	Does the AHBank have any contractual/legal charge-back rights?	Does the consumer have responsibility under the law for any financial loss?
A. Unauthorized ACH debit drawn on checking account*	Yes	Yes—to bank of first deposit	Maybe—up to limited amounts
B. Unauthorized purchase on credit card amount**	Yes	Yes—to merchant acquiring bank	Maybe—up to limited amounts
C. Forged drawer signature on check***	Yes	No—not unless the check has been converted to an electronic form of payment	No
D. Identity theft—credit card account	Yes	No	No
E. Identity theft—asset account	Yes	No	No

Notes to Table 1:

*Under the EFTA and Reg E, the AHBank is generally liable for an unauthorized ACH debit drawn on a checking account; subject, however, to certain limited liability that can be shifted to the consumer. Consumer liability is limited to $50 if the consumer notifies the AHBank within two business days of learning of the loss or theft of an access device. It is limited to $500 if the consumer doesn't notify the AHBank within two business days. If a consumer fails to report unauthorized EFTs that appear on a periodic statement, he can be held liable for all unauthorized EFTs that occur more than 60 days after the transmittal of the first statement reflecting an unauthorized EFT. *See* 15 U.S.C. § 1693g; 12 C.F.R. § 205.6. However, both Visa U.S.A. and MasterCard International have adopted "zero liability" policies for debit card transactions processed over their networks—under these policies the consumer is not to be held liable for the first dollar of unauthorized transactions. *See* http://www.usa.visa.com/personal/secure_with_visa/zero_liability.html (last visited Apr. 2, 2003); http://www.mastercardintl.com/about/press/pressreleases.cgi?id=303.

**TILA and Reg Z generally put liability for unauthorized credit card transactions upon the AHBank. However, the AHBank is authorized to hold the consumer responsible for the first $50 provided that certain procedural requirements are complied with. 15 U.S.C. sections 1643 and 1666; 12 C.F.R. sections 226.12 and 226.13. Again, both Visa U.S.A. and MasterCard International have adopted "zero liability" policies for unauthorized credit card transactions.

***The AHB bank which pays a forged drawer check is responsible for reimbursing the customer under the UCC sections 3-401 and 3-403. Additionally, if the check is drawn against an open end credit account, the billing error provisions of TILA and Reg Z require the AHBank to reimburse the consumer. *See* 15 U.S.C. § 1666; 12 C.F.R. § 226.13. Further if the check was converted to an electronic form of payment, it would generally be considered an EFT and the AHBank would be responsible for reimbursing the customer under the EFTA and Regulation E. *See* 15 U.S.C. §§ 1693f, 1693g; 12 C.F.R. §§ 205.6, 205.11; Official Staff Commentary to Regulation E, 12 C.F.R. pt. 205, Supp. 1, § 205.3(b)1.v. If the unauthorized check was converted to an electronic form of payment, it could be transmitted back to the originating bank for reimbursement under the ACH rules, assuming that timing and other technical requirements could be satisfied. *See, e.g.*, National Automated Clearing House Association (NACHA), 2001 ACH Operating Rules (ACH Rules) (concerning PPD Accounts Receivable Truncated Check Debit Entries and the POP Point-of-Purchase program).

IV. EXCEPTIONS TO SIMPLE ANSWERS WHERE THE CONSUMER HAS ARRANGED FOR AGGREGATION

The following must be remembered when analyzing whether the presence of an aggregation relationship changes the SIMPLE ANSWERS: *simply because a consumer has signed up for aggregation and suffers some type of unauthorized transaction against a financial account does not mean that the cause of the unauthorized transaction was the consumer's involvement with, or providing information to, an aggregation site.* For example, fraud on credit card accounts has been around since the inception of credit card lending—dumpster divers, bad merchants, bad credit card issuer's employees, fraud rings hacking into merchant databases, and other bad actors have all been involved in obtaining information about consumer's credit card accounts and using that information to conduct fraudulent transactions on those accounts. Simply because aggregation has appeared on the landscape does not mean that all credit card fraud is now attributable to the consumer's having arranged for account aggregation. Fraud in connection with consumer financial accounts is quite large[65]—reported fraud in connection with enrollment in aggregation sites has thus far been virtually nonexistent.[66]

For aggregation to be relevant in determining who has liability for an unauthorized transaction, the AHBank must realize that the consumer has arranged for aggregation and then be able to prove that aggregation has some relevant connection to the fraud. With aggregation in its infancy and having relatively few users, it will probably not be a factor in the near future for most claims that a transaction is unauthorized. However, if at some future point aggregation is implicated frequently when unauthorized transactions appear, then utilization of an aggregation service might start appearing on an AHBank's checklist of facts to look for when a fraudulent transaction occurs.

According to the SIMPLE ANSWERS: (1) the customer generally

---

65. For example, Visa and MasterCard reported $576.3 million in fraud losses as of 1/1/98. CARD INDUSTRY DIRECTORY 15 (Faulkner & Gray, Inc. 2000).

66. The author has been advised by a representative of Yodlee that to his knowledge such fraud has been nonexistent. *See* Yodlee Interview, *supra* note 2.

has rights under existing laws/regulations to reimbursement when an unauthorized transaction is made against his financial account; (2) the AHBank will generally be the party initially responsible for reimbursement under the existing laws/regulations; (3) the AHBank may have contractual rights under ACH Rules or payment processing association rules to charge-back this loss to another financial institution; and (4) that financial institution may have contractual rights to reimbursement from its customer. Assuming that aggregation evolves in such a way that aggregation sites become the sources of information used to commit some unauthorized transactions, this Part will address whether the SIMPLE ANSWERS change where an AHBank believes that the source of the information used in the unauthorized transaction was an aggregation site. Table 2, below, sets forth simple conclusions as to whether the SIMPLE ANSWERS change when an aggregation relationship is implicated in connection with an unauthorized transaction.

Table 2: Exceptions to Simple Answers Where the Consumer Has Arranged for Aggregation

Type of transaction	Does the SIMPLE ANSWER change if the consumer has arranged for aggregation?
A. Unauthorized ACH debit drawn on checking account	Maybe (See Tables 3 & 4 below)
B. Unauthorized purchase on credit card account	Maybe (See Tables 3 & 4 below)
C. Forged drawer signature on check	No
D. Identity theft—credit card account	No
E. Identity theft—asset account	No

A. "Worst Case" Scenario

The worst case scenario from both the AHBank's and its

customer's perspective is if the customer's user ID or password is used to enter the AHBank's online banking site and initiate the unauthorized transaction, transferring money from the customer's account at the AHBank to another bank (a "credit push" transaction). As a practical matter, SIMPLE ANSWERS A and B may both change in terms of whether the customer is protected and who is ultimately liable.

In this situation, appropriate resolution is confusing and uncertain at best.[67] The basic problem is that many factual issues must be resolved prior to the AHBank reaching a conclusion as to its legal responsibilities. The conclusion will be largely dependent on the facts in each case. The AHBank will have no rights of charge-back under ACH or credit card association rules.[68] The

---

67. The difficulty in appropriately assessing liability is captured in this excerpt from a question and answer session at the Federal Reserve Bank of Chicago Workshop on Promoting the Use of Electronic Payments, at 140 (Oct. 11, 2000) (transcript on file with the Federal Reserve Bank of Chicago):

> Audience Member: You mentioned in your paper that the bank could be found liable for account aggregation even though the customer provides the information, the number, PIN, et cetera, and the bank does not even know they have done that and yet could be held liable. I have heard that a number of times. I wonder how that is the case.
>
> Sarah Jane Hughes (Professor Indiana University School of Law): I do not think there is a law on that subject .... I think it is a question of proof and whose fault it is. On one level it is the customer's fault for disclosing information that should be guarded. But we never know whether it is a participant failure, participant error, system issue, electrical outage. And we have had examples over the last 15 years of payment issue problems that are related to electrical outages. We do not know whether there is a hacker. We just have a lot of difficulty proving fraud.
>
> From the consumer's perspective it is incredibly difficult to show where an error occurred. It is comparable to one of us looking at a car that has many embedded computers in it and pointing to the one that is not working correctly ... and from the consumer's perspective the cost of finding someone to help penetrate this problem is enormous. I think we have to consider the prospect that a jury is going to be deciding this, and that the jury is highly likely to assume that the error is not the consumer's error but somebody else's in the system. And we also have the tendency to look for the deepest pocket to assign the loss to .... So it suggests to us that we need to consider how we are going to insure ourselves ....

Id.

68. The AHBank in this scenario is acting upon what it believes to be its consumer customer's instruction in initiating the transaction. Its role is that of transaction originator (comparable to the originator in the ACH system and the

AHBank's right of reimbursement from the aggregator or aggregation technology provider ("ATP") will be matters for negotiation and fact dependent. In such a heavily fact dependent scenario, it is impossible to conclude with any certainty what a specific AHBank, aggregator or ATP would do vis-à-vis assuming liability—the parties could spend many hours arguing over (1) whether the transaction was unauthorized or whether the customer was involved (i.e., a "friendly fraud"), (2) if unauthorized, who the fraudster was, and (3) what the source of the information used to make the unauthorized transaction was. However, the basic laws, regulations and common law may already provide the basis for liability determinations in most cases—the specific facts determine what result is reached in applying those laws, regulations and common law principles. The following paragraphs will detail how an AHBank might approach such a complaint by its customer and illustrate the complex factual issues facing the parties.

The AHBank's first reaction may be that, since the customer's password and/or user ID was used to initiate the transaction, the customer or someone that he authorized must have initiated the transaction. One might assume that the customer had simply forgotten that he had initiated the transaction and there would probably be an attempt to get the customer to remember it. The customer might be asked who else has access to the account that might have initiated the transaction. He would be asked how someone else might have obtained his secret information: did he write it down somewhere (and, if so, where); does a relative or friend know the information; does he use the same password or user ID for other applications; has he provided the secret information to a financial advisor; or, perhaps, has he provided it to an aggregation site. The AHBank might attempt to determine a connection between the customer and the recipient of the funds. In this murky fact situation, the AHBank might reach a conclusion based on sketchy and imperfect information as to how the transaction occurred; the inclination, even after a lengthy

---

merchant in the credit card system) vis-a-vis either the ACH or the credit card processing systems. The processing systems' rules generally provide for chargebacks against the originator or the merchant, not for chargebacks by either of them.

investigation, might still be to conclude that the AHBank considered the transaction authorized and to advise the customer that it was resolving the issue against him.[69] Alternatively, the AHBank might determine that the transaction was unauthorized and that (1) the most probable source of the fraud is information provided to the aggregation site, (2) there was another identifiable source of the information, or (3) it has no idea whatsoever as to the source of the fraud or information.

If the AHBank concluded that the unauthorized transaction was connected to an aggregation site, it may try to judge how the secret information had been obtained from the aggregation site—whether by a hacker, by a dishonest employee of the aggregator or the ATP, or by the aggregator itself. In the simple situation where a dishonest aggregator was the fraudster, SIMPLE ANSWER A might change as the AHBank would have a basis under Reg E for refusing to reimburse the customer.[70] The basis for shifting liability to the customer is created by language in Reg E which indicates that where a customer furnishes his access device (*e.g.*, the username and PIN) to a third party (*e.g.*, the aggregator), the customer is fully liable for transfers made by the third party unless he has notified the AHBank that transfers by the third party are no longer permitted.[71] Informal comments from Federal Reserve Board of Governors ("FRB") staff indicate that this argument would be correct only if the customer had originally authorized the aggregator to perform EFT transactions. If the aggregator was not originally authorized to do EFT transactions, even this very limited

69. Both Regulation E and Regulation Z require an AHBank to "investigate" an alleged unauthorized transaction. *See* 12 C.F.R. §§ 205.11(c), 226.13(f) (2001). They do not require the AHBank to always believe the allegation nor do they define in detail what is or is not adequate proof that a transaction is unauthorized. *See id.* § 205.11(c), 226.13(f). This remains a fact question for determination by the AHBank. *See id.* §§ 205.11(c)–(d), 226.12(b), 226.13(f). Having said this, in making the factual determination, the AHBank must remember that both the EFTA and TILA place the burden of proof on the AHBank to show that the EFT or credit card transaction was authorized. *See* 15 U.S.C. §§ 1693g(b), 1643(b) (1994).

70. *See* 12 C.F.R. § 205.2(m)(1); Official Staff Interpretations to Regulation E, 12 C.F.R. pt. 205, Supp. I, § 205.2(m)(2).

71. *See* 12 C.F.R. § 205.2(m)(1); Official Staff Interpretations to Regulation E, 12 C.F.R. pt. 205, Supp. I, § 205.2(m)(2).

basis for refusing to reimburse the customer should be eliminated.

What does it mean to say that the aggregator was the fraudster? If the AHBank refused reimbursement under the aggregator-as-fraudster scenario, it is inevitable that the question would come up as to *who* is the aggregator—specifically, how far can Reg E be stretched to provide a basis for the AHBank to refuse to reimburse the customer if the actual fraudster was a high level employee of the aggregator, a low level employee, the ATP, or one of the ATP's employees? Who among these would be considered the "aggregator" whom the customer authorized to make EFT transactions when he signed up for the aggregation service? While the AHBank might argue that each of these parties should be considered the "aggregator," its right to refuse reimbursement on this basis is less than clear under Reg E and would be a matter of dispute.[72]

If the account accessed is a credit account, SIMPLE ANSWER B does not change vis-à-vis liability to the customer: the AHBank does not have a legitimate argument under specific language of Reg Z for refusing reimbursement simply because the aggregator or one of its employees/agents was the fraudster.[73]

If the fraudster was a hacker, it is hard to find a basis for the AHBank to refuse reimbursement under either Reg E or Reg Z.[74]

This "worst case" scenario would not be relevant or applicable in the situations described in SIMPLE ANSWERS C, D, or E.

If the AHBank reimburses its customer in a situation involving a credit push, it has no rights of charge-back under the ACH rules

72. *See* Official Staff Interpretations to Regulation E, 12 C.F.R. pt. 205, Supp. I, § 205.2(m)(1). A consumer has no liability for erroneous or fraudulent transfers initiated by an employee of a financial institution. *Id.* The consumer might attempt to use these words against the aggregator (or perhaps even its AHBank) should an aggregator fit within the Regulation E definition of a "financial institution" and the fraudster be the aggregator's employee. It is unlikely that the comment was originally written to be applied in this manner against an AHBank. Nonetheless, the words are arguably broad enough to be so applied, and neither the words of Regulation E, nor the Commentary attempt to allocate liability between the AHBank and the Aggregator in this situation.

73. *See* 12 C.F.R. §§ 226.12, 226.13.

74. *See* Official Staff Interpretations to Regulation E, 12 C.F.R. pt. 205, Supp. I, § 205.6(b)(2) (clarifying that consumer negligence does not provide a basis for refusing reimbursement).

or the card processing association rules because the AHBank itself was the party taking instructions from a fraudster.[75] However, the AHBank may obtain reimbursement from (1) the recipient financial institution if it will voluntarily cooperate in removing funds from the fraudster's account (should any remain on deposit) on the basis of indemnification or other protection, (2) the fraudster through litigation or other means, or (3) the aggregator or the ATP.

Theories on which to base a claim for reimbursement from the aggregator or ATP would include reimbursement based on contractual rights if the AHBank had an agreement with either one for reimbursement (*e.g.*, in a data feed or aggregation site agreement) should losses be attributable to an AHBank customer having provided information to the aggregation site. The problem that the AHBank still faces is providing "proof" that the aggregation site was the source of the information used in making the fraudulent transaction. The aggregator or ATP might require more in the way of "proof" than the AHBank had been willing to request from its good customer.

Alternatively, if no contractual relationship existed, the AHBank could attempt to obtain reimbursement based on alleged negligence. In a given situation, the aggregator or ATP might find it advantageous to reimburse the AHBank in order to avoid (1) the time and money involved in litigation, (2) creating bad precedent in an unfavorable fact situation, or (3) negative press as to the safety and security of the aggregation service.

While the above described "worst case" scenario does not give rise to clear or simple answers,[76] it is hard to identify any benefit

---

75. *See supra* note 64 and accompanying text.

76. *See, e.g.*, OCC, *supra* note 28 (describing the potential exposure to liability under Regulation E when AHBanks provide their customers with usernames and passwords for electronic banking). 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 transaction. *Id.* at 4. The OCC also provided the following caution when a national bank is acting as aggregator:

In aggregating customer information, banks should closely monitor regulatory

from or need for the enactment of additional laws, regulations or interpretations at this time. Specifically, such identification is difficult given the fact intensive nature of any dispute under this scenario and the absence of a real life factual basis for concluding that existing law is not sufficient to handle most problems that may arise. Table 3 attempts to set forth the author's conclusions as to who is responsible for absorbing the financial loss in several possible fact situations. It must be emphasized that without a real life fact pattern significant ambiguities exist in the examples given and parties may differ as to the outcomes.[77]

---

changes in the application of Regulation E. Currently Regulation E . . . does not specifically address the responsibilities of aggregators . . . . 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 . . . .

Id. at 4; *see also* Ronald Congemi, *Regulation of Aggregators Needs More Uniformity*, AM. BANKER, Oct. 13, 2000, at 17; John Jin Lee, *Lee: Repair Inadequate Aggregation Regs*, AM. BANKER, Sept. 8, 2000, at 14A.

77. As artfully stated by Star Systems, Inc. in its August 2000 report on aggregation in a section entitled *Consumer Protection: The Legal and Regulatory Landscape:*

> It comes as no surprise that even the Internet-savvy consumers surveyed for STAR are confused about the regulatory implications of Web aggregation. It is such a new and dynamic area that definitions of law and delineations of responsibility are continually evolving, and new questions arise as quickly as others are answered. What is true today is likely to be vastly out-of-date by year's end. The best anyone can do at this point is to paint as complete a picture as possible of the current, hazy landscape and to make an educated prediction of what lies ahead.

Letter from Paul Schmelzer, Executive Vice President Star Systems, Inc. to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Sept. 5, 2000) (on file with the FRB) [hereinafter

Table 3: Worst Case Scenario—"Credit Push" Transaction Where the Customer Has Arranged for Aggregation*

Fact situation: Consumer's user ID/password is used to enter the AHBank's online banking site and initiate the unauthorized transaction, transferring money from his account at the AHBank to another bank.

Type of Transaction	Is the AHBank responsible for loss under the Law?	Does the AHBank have any contractual charge back rights?	Does the consumer have responsibility under the law for any financial loss?
A. Unauthorized ACH debit drawn	Appropriate resolution is confusing and uncertain—conclusion will be on checking accountlargely dependent on the facts in each case.		
A.1 Aggregator was the fraudster, AND Customer has authorized aggregator to perform EFT transactions	In A.1 the "SIMPLE ANSWERS" change as follows: No	N.A.	Consumer must look to aggregator for reimburse-ment
A.2 Aggregator was the fraudster, AND Customer has NOT authorized the Aggregator to perform EFT transactions	The "SIMPLE ANSWER" does not change in A.2 as to who is liable as between the AHBank and the customer; it does change with respect to whether the AHBank has any charge-back rights Yes	No+	Maybe—up to limited amounts (See* at Table 1)
A.3 Aggregator employee, ATP, or ATP employee was the fraudster, AND Customer has authorized the aggregator to perform EFT transactions	Unclear in A.3 whether the "SIMPLE ANSWERS" change—the AHBank might argue that the parties listed should be considered the "aggregator;" its right to refuse reimbursement on this basis is less than clear under EFTA and would be a matter of dispute		
A.4 Aggregator employee, ATP, or ATP employee was the fraudster, AND the customer has not authorized the aggregator to perform EFT transactions	The "SIMPLE ANSWER" does not change in A.4 as to who is liable as between the AHBank and the consumer; it does change with respect to whether the AHBank has any charge-back rights Yes	No+	Maybe—up to limited amounts (See * at Table 1)
A.5 The fraudster was a hacker	The "SIMPLE ANSWER" does not change in A.5 as to who is liable as between the AHBank and the consumer; it does change with respect to whether the AHBank has any charge-back rights Yes	No+	Maybe—up to limited amounts (See * at Table I)
B. Unauthorized transaction on credit card account	The "SIMPLE ANSWER" does not change in this fact situation as to who is liable as between the AHBank and the consumer; it does change with respect to whether the AHBank has any charge-back rights Yes	No+	Maybe—up to limited amounts (see**at Table 1)

*DISCLAIMER: This Table reflects the author's preliminary views in connection with a developing business and technology product. Business, technology and laws are subject to changes in substance and interpretation. As the business and technology evolves, the legal analysis may also change and evolve.

Schmelzer letter] (enclosing Star Systems, Inc. report titled *WEB AGGREGATION, A SNAPSHOT*).

B. Debit Transactions

With "debit" transactions, the unauthorized transaction would be initiated through a financial institution or retail merchant and would take the form of either an ACH debit, or a debit card/credit card charge (debit) against the customer's account. Examples of this situation might occur if a bad aggregator or hacker accessed an aggregation site and obtained the customer's credit card or debit card account information together with other personal information. The bad aggregator/hacker might create a counterfeit card using the information and use it at a retail merchant to consummate a fraudulent transaction. Alternatively, the information might be used without creating a card to do a telephone order with a merchant or a transaction over the Internet. The threshold issue with any such transaction, again, is how to identify and prove that the unauthorized transaction had any relationship to the customer's involvement with an aggregation site.

1. Unauthorized Transactions Initiated By a Bad Aggregator

Such a scenario might involve the bad aggregator (or its merchant partner) having a retail business unrelated to the aggregation site, through which the aggregator could submit sales drafts or ACH authorizations for retail purchases. Should this scenario surface and the consumer complain to his AHBank, the standard ACH or credit card or debit card contractual charge-back mechanisms should work to place liability upon the ODFI/merchant acquiring bank which acquired the transaction from the aggregator (or his merchant partner); typically, the ODFI/merchant acquiring bank would then have the contractual right to charge-back to its merchant customer, i.e., here the bad aggregator (or its merchant partner). If for some reason the normal charge-back mechanisms did not work, the specific type of fraudulent transaction involved determines whether arguments can be successfully raised by the AHBank that it should not be liable to the customer.

As previously described in the "worst case" scenario, a regulatory basis for insisting that the customer should bear

financial responsibility vis-à-vis the AHBank only exists with respect to unauthorized EFT transactions drawn on an asset account by a bad aggregator.[78] Thus, SIMPLE ANSWER A may change. It should be noted that raising this issue in the first instance, prior to attempting charge-back/reversal, may generally complicate rather than simplify the situation from both the customer's and the AHBank's perspectives. Both may be more assured of reimbursement if the AHBank simply recredits the customer's account and charges-back the unauthorized debit; this should also reduce customer dissatisfaction with the AHBank and leave the customer with only a relatively small risk of ultimately bearing the loss. Only if this reimbursement and charge-back/reversal fails may it make much practical sense for the AHBank to deny compensation to the consumer, forcing the consumer to deal with the aggregator. One should keep in mind that this "bad aggregator" fact scenario becomes less likely the more often that the entities providing aggregation sites are financial institutions or other established businesses.

In the case of unauthorized credit card transactions, the customer should not bear financial losses and no such successful arguments by the AHBank to the contrary appear likely. Thus SIMPLE ANSWER B would not change. The debit transaction fact situation described in this Part is not relevant in connection with transactions resulting from counterfeit/forged checks or the opening of accounts based upon identity theft. Thus SIMPLE ANSWERS C, D, and E would not change.[79]

---

78. *See* 12 C.F.R. § 205.2(m)(1); Official Staff Interpretations to Regulation E 12, C.F.R. pt. 205, Supp. I, § 205.2(m)(2).

79. TILA and Regulation Z require the AHBank to reimburse the consumer for unauthorized transactions—no exceptions are made for transactions enabled by the negligence of the consumer. *See* 15 U.S.C. §§ 1643, 1666 (1994); 12 C.F.R. §§ 226.12, 226.13. With respect to identity fraud, litigation against the real consumer based upon the theory that he enabled the fraud by negligent disclosure of information to the aggregator would need to be proved—this is a non-starter with no realistic possibility of success. With respect to counterfeit checks drawn against a real deposit account in the name of the real consumer, it is possible that the AHBank could refuse to reimburse the consumer based on some very tortured negligence theory (*e.g.*, that the consumer had enabled the fraudulent transaction by negligently providing private information to the aggregator). However, given the liability for consequential damages which an

2. Unauthorized Transactions Initiated By a Hacker or Other Third Party

If losses involving debit pull transactions were due to unauthorized transactions by a hacker who accessed information at the aggregation site, the customer should be made whole by his AHBank. The customer has not authorized the hacker to use the information; any alleged negligence by the customer in disclosing his secret information to the aggregation site should not be relevant to the liability determination under either Reg E or Reg Z.[80]

If it were possible to tie the losses to negligent practices at the aggregation site, it might be possible for the AHBank, the merchant acquiring bank, or the ODFI that processed the transaction for the hacker (or for the merchant that accepted the transaction from the hacker) to attempt to impose some sort of liability on the aggregator. However, unless significant dollars are involved this would appear quite unlikely given the difficulties in proving the source of the information used in the fraud or such negligence. Additionally, if flaws (negligence) could be found in the practices of the financial institution that had either entered into a contractual arrangement with the hacker or that had opened an account for the hacker based on identity fraud, it is somewhat unlikely that those institutions would want to expose their own weak or flawed processes in attempting to recover from the

---

AHBank has for wrongful dishonor of the real customer's checks and for conversion, the considerable time and effort that would be required to proceed with such flimsy theories, and that the probability of success is remote, this would not appear to be an intelligent or cost effective approach.

80. *See* Official Staff Interpretations to Regulation E, 12 C.F.R. pt. 205, Supp I, § 205.6(b)(2).

> Has the aggregator been hacked and somebody was able to pull up the PIN and the account number and use it? If so, I think the law is quite clear, the customer is not responsible. The customer can write the PIN on the back of their ATM card and leave it on the bus and they are still not responsible. We are very protective of the consumer. I think a different question is whether the aggregator itself exceeded its authority to use the data.

David Teitelbaum, Remarks at the Workshop on Promoting the Use of Electronic Payments 141 (Oct. 11, 2000) (transcript on file with the Federal Reserve Bank of Chicago).

aggregator.

Table 4 attempts to set forth the author's conclusions as to who is responsible for absorbing the financial loss in connection with debit transactions where an aggregation site has been utilized at some point by the customer and is implicated in the transaction. Again, it must be emphasized that without a real life fact pattern significant ambiguities exist in the examples given and parties may differ as to the outcomes.

Table 4: Unauthorized Debit Transactions Where the Customer Has Arranged for Aggregation

Fact Situation: An unauthorized transaction is initiated through a financial institution or retail merchant and takes the form of either an ACH debit or a debit card/credit card charge (a "debit" transaction). For example, a bad aggregator or hacker accesses an aggregation site and obtains the customer's credit card or debit card account information together with other personal information and uses that information to do a transaction at a merchant site.

Type of Transaction	Is the AHBank responsible for loss under the law?	Does the AHBank have any contractual charge back rights?	Consumer responsibility for any financial loss?
A. Unauthorized ACH debit drawn on checking account	Appropriate resolution is largely dependent on the facts in each case.		
A.1 Aggregator was the fraudster AND Customer has authorized aggregator to perform EFT transactions*	In A.1 the "SIMPLE ANSWERS" change as follows: No	N.A.	Consumer must look to aggregator for reimbursement
[*As a practical matter, if the AHBank chooses to ignore its "legal rights" and assist the consumer, it would probably be able to charge back the transaction to the bank of first deposit which would then probably obtain reimbursement from its depositor—the AHBank's customer would be made whole and loss would probably fall upon the aggregator or the party processing the transaction for the aggregator]			
A.2 The fraudster was a hacker or other third party	The "SIMPLE ANSWERS" do not change Yes	Yes—to the bank of first deposit	Maybe—up to limited amounts (See * at Table 1)
B. Unauthorized purchase on credit card account	The "SIMPLE ANSWERS" do not change Yes	Yes—to merchant acquiring bank	Maybe—up to limited amount (See ** on Table I)

C. Practical Considerations

One very important practical consideration to keep in mind is that the answers outlined above and the legal rights provided by the various applicable laws, regulations, and contractual arrangements, do not necessarily mean that the consumer will be made whole. Of primary importance is whether the customer is credible when he claims that the transaction is unauthorized. If not, the AHBank will determine that no unauthorized transaction occurred and probably will not reimburse him voluntarily. Additionally, the customer's reimbursement also will depend on whether the AHBank knows the law and whether its counsel interprets existing consumer protection laws conservatively or aggressively.

Since neither statutory or regulatory language nor the interpretation of facts are ever 100% clear, an aggressive attorney

might well parse words or interpret facts differently and reach different conclusions than those outlined in this Article. However, assuming that the AHBank and its counsel take a conservative approach, just as important is whether the customer service staff understands what the law requires. If the customer service staff does not understand that claims of unauthorized transactions must be resolved as required by law and that procedures are specified for their resolution under both Reg E and Reg Z, then a claim may not be investigated or resolved.[81]

Given the endless permutations that can be thought up when dealing with hypothetical situations (which is the only approach available unless an AHBank has real life experience with or actual knowledge of reality and common factual situations), arriving at the correct answers for who has liability when an unauthorized transaction is related to the provision of information to an aggregation site is a very complex issue.[82] Consequently, reasonable business people might conclude, based upon a cost-benefit analysis, that it is simply not worth attempting to determine the appropriate resolution of all conceivable fact situations or to train the customer service staff in all possible nuances. Rather a more practical approach might be to simply establish thresholds (i.e., the lesser of X dollars or Y claims). As long as the thresholds are not exceeded, customer claims of unauthorized transactions would result in customer reimbursement and be handled under standard charge-back, reversal, or write-off policies irrespective of

---

81. *See* 12 C.F.R. §§ 205.6, 226.13.

82. The authors of a recent BUSINESS LAWYER article on developments in cyberbanking discussed liability issues concerning aggregation in the following terms:

> As aggregation services have increased in popularity, questions have arisen under Regulation E, which implements the Electronic fund Transfer Act, and Regulation Z, which implements the Truth in Lending Act, as to whether the consumer, the aggregator, or the account holding financial institution would be liable for fraudulent transfers initiated by either an employee of an aggregator or by a hacker who gains access to the aggregator's Web site. More specifically, a key unresolved issue is whether fraudulent transfers are unauthorized transfers when, for example, the consumer has furnished the aggregator with a PIN or access code, and therefore, it is not clear which party should bear the loss for such transfers.

Lee S. Adams & David J. Martz, *Developments in Cyberbanking*, 57 BUS. LAW 1257, 1265 (2002).

whether information had been provided by the customer to an aggregation site. If the threshold were reached, it might begin to make economic sense to devote the time and energy to figuring out technical rights based upon experience with real life situations. If problems arise infrequently and involve relatively small amounts of money, the cost of analysis and training may far exceed the costs of any write-offs.

Additional factual considerations, such as the amount of the potential loss, may be determinative of whether the customer is reimbursed. If a small amount is involved, a concession and reimbursement may be quickly made without much thought by either the AHBank or the aggregator, both of whom may have a policy of reimbursing small losses irrespective of technical responsibility in order to limit expenses for staff time (or to limit the size of a class in a potential class action lawsuit). If large amounts are involved, there would tend to be a more careful examination of statutory/regulatory provisions and technical defenses.

Further, if funds cannot be recovered through charge-back or reversal mechanisms, losses may simply be absorbed by various financial institutions as a cost of doing business. Procedures may develop to limit the possibilities of such fraud (*e.g.*, by refusing to participate in data feed arrangements and getting aggressive in limiting screen-scraping activities) or the increased costs of fraud resulting from the concentration of information at aggregation sites may simply be priced into the amounts charged to consumers for general banking services (or priced into those services for the customers who choose to use aggregation). Alternatively, a financial institution or other data site might decide to enter into a data feed arrangement if it were possible to negotiate an assumption of responsibility by the aggregator for fraud transactions tied to information provided to the aggregator.

Whether litigation will develop to shift responsibility for fraud losses to aggregators depends on whether significant dollars can be identified and proven lost due to the negligence of the aggregator.[83]

---

83. While Regulation E in some fact situations might be read to place responsibility on an aggregator to resolve an alleged error raised by a consumer, Regulation E does not generally provide a clear roadmap as to how liability is to

To the extent that the aggregation site has followed procedures common in the industry and the industry is largely populated by large financial institutions or other large corporate entities, proving negligence may be difficult. If litigation develops, it is not possible to predict the outcome with certainty. Given the costs of litigation, the possibility of using it to resolve aggregator liability issues appears unlikely in the absence of a significant level of loss. Additionally, the AHBank seeking to shift liability to an aggregator may also operate an aggregation site—it may be that it would prefer to absorb a significant loss rather than to create precedent that others might use to attempt to shift liability to it in another situation where it is acting as aggregator rather than AHBank.

The evolution of aggregation may also work to reduce the number of situations where aggregators are a significant concern to AHBanks. Consider the case of a bank holding company's branded/sponsored aggregation site. If a customer signs up for aggregation at that site, he may have six accounts that are designated for aggregation. It is certainly possible that one or more of these six accounts (*e.g.*, the checking account, a money market account, and a couple of credit card accounts) may be with the bank holding company's subsidiaries. To the extent that an aggregator and an AHBank are members of the same financial family (*e.g.*, within the same bank holding company), any arguments that the AHBank might otherwise use under Reg E to avoid liability to the customer for an unauthorized transaction should evaporate, as a practical matter. While the various subsidiary entities might argue among themselves as to which is to write-off a loss from an unauthorized transaction, the customer should be taken care of. The emergence of large financial institutions with many customer accounts in the aggregation space should lessen the frequency with which unrelated small entities are aggregating information from such banks' customers' accounts.

Other relevant practical considerations are which persons or groups within the AHBank are making decisions on the issue and

---

be allocated between an aggregator and an AHBank in situations where a consumer is alleging that an unauthorized transaction has occurred. *See generally* 12 C.F.R. pt. 205 (2001).

how much thought is going into those decisions. Additionally, what is the "climate" or philosophy within the institution at the time the issue arises? At various times, the relevant philosophy within an institution differs—it is determined by the specific people involved in decision making on a specific issue together with the general financial conditions within the economy and the institution. It may range between always "taking care of the customer" and "the customer is always right" to parsing words so as to do only what is unarguably technically required. If significant losses tied to aggregation by consumers occur, the philosophy may shift to one of aggressively pursuing aggregators on negligence or other theories.

V. WHAT HAS CAUSED THE CONCERN WITH ACCOUNT AGGREGATION?

Given the state of aggregation at the middle of 2002, one might well ask why there has been such a vocal concern with aggregation and the prospective allocation or definition of liabilities. The answer may lie in the historical development of the aggregation product. In late 1999 through early 2000, a number of small entities suddenly emerged offering screen-scraping-based account aggregation.[84] These entities were generally newly formed, and in many cases had few assets. Additionally, these early aggregation services received significant attention in the trade press as perhaps forming the basis for the next "killer" application in consumer financial services.[85]

AHBanks were concerned that these small screen-scraping-based entities would create customer service problems in the financial institution's relationships with its customers; specifically, that account information was being reflected inaccurately or without adequate disclosure of limitations on the accuracy of such information.[86] Of significant concern was whether consumers

84. *See* W.A. Lee, *Yodlee Takes Lead in Aggregation World*, AM. BANKER, Sept. 8, 2000, at 4A.

85. *See, e.g.*, Bill Currie & Janet Rodger, *Aggregation Is Banks' Last Chance to Win Back Disaffected Customers*, AM. BANKER, Mar. 9, 2001, at 14; *see also* Lee, *supra* note 84, at 4A.

86. *See, e.g.*, Schmelzer Letter, *supra* note 77 (noting that the accompanying report, entitled *WEB AGGREGATION, A SNAPSHOT*, summarizes issues of concern to financial institutions).

might take action in reliance on bad account data and then look to the financial institutions to solve their resulting problems.[87] Financial institutions were also concerned that inadequate security procedures used by the unknown aggregators would result in a significant increase in unauthorized transactions for which the financial institutions might bear financial responsibility.[88] The basic concern was that the AHBanks had no way to protect themselves—and no way to prevent or quantify the risk of loss.[89] To summarize: (1) the degree of concern with the introduction of financial account aggregation apparently resulted from the potential of "screen scraping" to dramatically increase the amount of financial data available at small, unknown, non-financial institution aggregation sites, and (2) the large amount of "hype" that the aggregation services were receiving further heightened the financial institutions' concerns.

The evolution of aggregation appears to have significantly diminished these initial concerns. The most common approach to offering aggregation services has changed from portals or small, non-bank aggregators competing with the financial institutions to financial institutions entering into partnerships with the early aggregators, with those entities now providing technical/operational services on the financial institutions' behalf.[90]

---

87. *See, e.g.*, BITS PROPOSED GUIDELINES, *supra* note 7, at E-2.

88. *See, e.g.*, Letter from Morrison & Foerster LLP, writing on behalf of Star Systems, Inc., to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Aug. 31, 2000) (on file with the FRB).

89. *See, e.g.*, Letter from Paula Holstein, Vice President First Union Corp., to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Aug. 31, 2000) (on file with the FRB); Rob Blackwell, *Banks Urge Fed: Extend Reg E to Cover Aggregators*, AM. BANKER, Sept. 6, 2000, at 4; Jessica Toonkel, *Banks Stop Whining, Learn to Love Aggregation*, AM. BANKER, Sept. 8, 2000, at 3A. These issues are reflected in the decision by First Union Corp. to sue PayTrust in late 1999. *See* First Union Corp. v. Secure Commerce Services, Inc., No. 3:99CV-519-P, (W.D.N.C. 1999).

90. *See, e.g.*, Michelle Heller, *Aggregators Playing By the Rules Get Nod in Poll*, AM. BANKER, Aug. 17, 2000, at 4 (discussing the overwhelming view of consumers as reflected in a 2000 survey by Star Systems that aggregation services should be provided or supported by their financial institutions); Megan J. Ptacek, *Online Banking: Aggregator-Blocking Service May Be Blocked by Bad Timing*,

With financial institutions or larger brand names such as Yahoo, Inc., America Online, and Microsoft now standing behind many aggregation sites,[91] the concern that massive unresolved problems will result from aggregation by small providers with limited capitalization appears to have significantly diminished. This greater confidence in aggregation providers is reinforced by the reality that, to date, none of the anticipated financial liability issues has cost financial institutions any significant real life dollars.

At this point in time, new concerns may be arising and new challenges are appearing in the aggregation arena with respect to dealing with third party service providers and the outsourcing of services.[92] Additionally, privacy concerns are being raised concerning the uses that may be made of aggregated data. Both subjects are beyond the scope of this Article.[93]

CONCLUSION

It seems too early in the development of aggregation services for any regulatory or legislative action to be appropriate or necessary. It appears prudent to let the business develop before considering action to allocate liability given (1) the absence of any significant dollar losses clearly tied to aggregation services and (2)

AM. BANKER, Feb. 16, 2001, at 1; *Comment: Account Aggregation Brings Both Opportunities and Risks*, AM. BANKER, June 13, 2001, at 17; Miriam Leuchter, *Aggregation Aggravation*, US BANKER, Oct. 2000, at 28; Kimberly L. Wierzel, *Technology If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions*, 5 N.C. BANKING INST. 457, 458–62 (2001).

91. *See, e.g.*, Megan J. Ptacek, *Aggregation Just One Dish on B of A Web Menu for '01*, AM. BANKER, Oct. 17, 2000, at 14.

92. For a general discussion on outsourcing and privacy issues in connection with aggregation, see Julie L. Williams, *The Impact of Aggregation on the Financial Services Industry, Remarks before the American Banker's 2nd Account Aggregation Conference* (Apr. 23, 2001), *available at* http://www.occ.treas.gov/ftp/release/2001%2D39.txt (last visited Apr. 2, 2003); *see also* Megan J. Ptacek, *OCC Counsel Urges Banks to Monitor Aggregators*, AM. BANKER, Apr. 24, 2001, at 18; OCC, *supra* note 28, at 3; Wierzel, *supra* note 90, at 467.

93. For general background on privacy initiatives and developments impacting online financial services, see, e.g., Michael A. Benoit and Nicole F. Munro, *Recent Federal Privacy Initiatives Affecting the Electronic Delivery of Financial Services*, 56 BUS. LAW. 1143 (2001); Stephen F. Ambrose, Jr. & Joseph W. Gelb, *Consumer Privacy Regulation and Litigation*, 56 BUS. LAW. 1157 (2001).

the current relatively small number of consumers using aggregation.[94] While theoretical problem areas have been identified, reports of actual financial losses as a result of aggregation have not risen to the public consciousness or to the problem level. In fact, it is possible that so far they are virtually nonexistent. If aggregation services are provided by financial institutions or other large fiscally responsible corporate entities, the possibility exists that most concerns can be handled without additional legislation or regulation.[95] If merchant acquiring banks or ODFIs are suffering losses based upon transactions tied to the fraudulent use of information originally provided to an aggregation site, the solution may start with their duty to carefully screen and know their own customers.

In response to a June 23, 2000 Request for Comments,[96] the FRB received a wide range of responses from interested parties concerning risks to AHBanks and consumers from aggregation and the proposed solutions to those perceived risks.[97] The problems

---

94. *See, e.g.*, Letter from Patrick M. Frawley, Senior Vice President Bank of America Corporation, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Aug. 31, 2000) (on file with the FRB) (indicating that "[w]e applaud the Board's approach of foregoing any premature attempt at regulation in favor of first gathering information to learn more about aggregation.").

95. *See, e.g.*, Hughes, *supra* note 50 (discussing the view that system rules might be preferable to state or federal regulations).

96. *See* Federal Resolution Board, Request for Comments on Proposed Changes to the Official Staff Commentary on Regulation E [Docket No. R-1074] (June 23, 2000) (requesting information on how aggregation services worked and the potential coverage of Regulation E to such services), *available at* http://www.federalreserve.gov/boarddocs/press/boardacts/2000/20000623/attachment.p. The Federal Resolution Board has not yet formally addressed these issues. *See* Federal Resolution Board, Final Rule Revising the Official Staff Commentary to Regulation E (March 13, 2001), *available at* http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010313/attachment.pd.

97. *See, e.g.*, Adam Wasch, *Electronic Commerce: 'Screen-Scrapers' Should Be Regulated, Banks Tell Fed in Regulation E Comments*, *in* BNA ELECTRONIC COM. & LAW REP., Sept. 13, 2000, Vol. 5 No. 35, at 911; Letter from Hogan & Hartson LLP, on behalf of VerticalOne Corporation, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Aug. 31, 2000) (on file with the FRB); Letter from Morrison & Foerster LLP,

identified at that time were, perhaps, quite different from those which would be identified today. The concern was focused on unregulated non-financial institution aggregation providers and the problems that they might create. Now, as was described earlier in this Article, a number of major financial institutions have entered the aggregation space and concerns appear to be becoming more focused on (1) the profitability of aggregation, (2) how to obtain more robust data that can be used as a basis for transactions and analysis, (3) the risks of outsourcing, and (4) privacy issues.

In August 2001, the FRB received comments in connection with a more general review of banking regulations governing the online delivery of financial services.[98] A number of respondents indicated that, generally, they did not want the FRB to take action in anticipation of a need but rather that the FRB should wait until a real need for change is shown.[99] Significantly, some argued that

---

writing on behalf of Star Systems, Inc., to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Aug. 31, 2000) (on file with the FRB); Letter from Lloyd G. Harris, Vice President & Assistant General Counsel, Chase Manhattan Bank, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re Docket R-1074 (Aug. 31, 2000) (on file with the FRB) (raising issues such as whether aggregators should be defined as "financial institutions" under Regulation E); Holstein, *supra* note 89. One might ask what good it does to simply define an aggregator as a "financial institution" for Regulation E purposes? Mere revision of this definition may not establish the aggregator's liability to the consumer for an unauthorized EFT conducted by a rogue employee or hacker.

The responses indicate that financial institutions are uncomfortable with being held responsible for unauthorized EFTs connected to information being provided voluntarily to an aggregator by the consumer. If the goal is to establish that an AHBank does not have responsibility for such unauthorized EFTs, a clear statutory statement that the AHBank shall have no responsibility for losses suffered by the consumer that can be proved to have resulted from the consumer providing financial account information/access devices to the aggregator would be more straightforward.

98. *See* Federal Resolution Board, Request for Comments on Banking Regulations with Respect to the Online Delivery of Financial Services [Docket No. R-1105] (May 16, 2001), *available at* http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010516/default.htm.

99. Letter from Jennifer L. Jones, Vice President and Assistant General Counsel, J.P. Morgan Chase & Co., to Jennifer J. Johnson, Secretary, Board of

premature regulation might unintentionally deter private sector providers from pioneering more creative and efficient solutions potentially beneficial to consumers. Given developments in aggregation services since the June 23, 2000 Request for Comments (in particular the accelerated entry of major financial institutions into the aggregation space as aggregators), it continues to appear that a hands-off approach to the regulation of aggregation is warranted.

Existing laws and regulations generally require that the consumer participating in aggregation be held harmless from the unauthorized actions of hackers and other third parties with respect to financial accounts. If consumers were ever realistically being left unprotected (i.e., if consumers suffer significant losses that are not protected under existing laws or regulations), that would be the time to consider stronger enforcement of existing consumer protection laws or additional legislative or regulatory action. Laws and regulations should not be added or revised until it has been demonstrated that existing ones are not adequate to handle a new service. To the extent that theoretical problems are

---

Governors of the Federal Reserve System Re Docket R-1105 (Aug. 17, 2001) (on file with the FRB). This view was articulated in this letter, specifically stating that:

> While Congress and the Agencies should work toward removing existing barriers to electronic commerce, we ask them also to be cautious that their efforts do not result in inadvertently creating new barriers in the process. We believe caution is particularly advisable in areas where the Agencies might anticipate a potential need or concerns to consumers which has not yet in fact arisen. We are concerned with attempts by the Agencies to address these perceived needs by the implementation of prophylactic rules which can create barriers and huge, unanticipated burdens to financial institutions without providing a commensurate benefit to consumers.

Id; *see also* Letters addressed to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re: Docket R-1105 (on file with the FRB) (articulating similar views); Letter from James D. McLaughlin, Director Regulatory and Trust Affairs, American Bankers Association, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System (Aug. 20, 2001) (on file with the FRB); Letter from Phillip A. Wertz, Counsel, Bank of America, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System (Aug. 20, 2001) (on file with the FRB); Letter from Charlotte M. Bahin, Director of Regulatory Affairs and Senior Regulatory Counsel, America's Community Bankers, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System (Aug. 20, 2001) (on file with the FRB).

"solved" by new legislation/regulations before problems actually develop, the solutions may be irrelevant, unnecessary or produce unanticipated negative consequences. At this time it appears sensible for banking regulators to: (1) allow the financial services industry to exercise its judgment in developing aggregation under the existing regulatory framework, (2) continue monitoring business practices and developments in connection with aggregation, and (3) take regulatory action only if the need is demonstrated.