POLICY STUDIES

# Electronic Bill Payment and Presentment: A Primer

**Ann H. Spiotto**
**Federal Reserve Bank of Chicago**

Emerging Payments Occasional Paper Series
December 2001 (EPS-2001-5)

FEDERAL RESERVE BANK
OF CHICAGO

FEDERAL RESERVE BANK
OF CHICAGO

# Electronic Bill Payment and Presentment: A Primer

Ann H. Spiotto

Ann H. Spiotto is senior research counsel with the Emerging Payments Studies Department of the Federal Reserve Bank of Chicago. She previously spent twenty-five years as an attorney for First Chicago Corporation working with its retail banking and credit card operations – during her last ten years at First Chicago she was responsible for the legal work performed for the credit card business. Special thanks to Brian Mantel for his support in reviewing and critiquing this article. 

The Occasional Paper Series is part of the Federal Reserve Bank of Chicago's Public Policy Studies series.

Address any correspondence about this paper to Ann H. Spiotto, Federal Reserve Bank of Chicago, 230 S. LaSalle Street, Chicago, Illinois 60604 or e-mail Ann at ann.spiotto@chi.frb.org.
Requests for additional copies should be directed to the Public Information Center, Federal Reserve Bank of Chicago, P.O. Box 834, Chicago, Illinois 60690-0834 or telephone (312) 322-5111. This paper is available at http://www.chicagofed.org/publications/publicpolicystudies. This paper first appeared in substantially similar form in the November 2001 edition of *The Business Lawyer*. [Ann H. Spiotto, *Electronic Bill Payment and Presentment: A Primer*, 57 BUS. LAW 447 (2001)]

## Executive Summary

Electronic bill payment and presentment (EBPP) services are a core component of many financial institutions' on-line banking offerings. This paper discusses the laws (state and federal), regulations, and regulatory guidance generally applicable to EBPP services offered through financial institutions. Particular emphasis is given to (i) the Electronic Fund Transfer Act and Regulation E (including provisions relevant to dispute resolution, liability for unauthorized transactions, and electronic disclosure) and (ii) regulatory guidance with respect to outsourcing arrangements in connection with the offering of EBPP services. The paper talks about and provides an overview of the law and regulatory guidance as it is today – it does not advocate or recommend any specific changes at this time.

## Table of Contents

Electronic bill payment and presentment (EBPP) services are a core component of many financial institutions' on-line banking offerings. This Article will describe the services and discuss the significant legal rules and regulatory guidance applicable to such services.

**DESCRIPTION OF EBPP SERVICES**

EBPP services involve the collection of information from billers about a consumer's bills and the payment of those bills. In its purest form EBPP is the process used by companies to present bills for payment via the Internet, direct-dial access, touch-tone phone system, wireless device, ATM, or other electronic device and the electronic payment of these bills by consumers through one of these technologies. However, in practice, the term EBPP covers several different variants or models.[1] The model discussed in this Article is provided for consumers under a financial institution's brand at the financial institution's Web site, with the operational and technical support provided by an outside vendor.[2]

---

[1] The various models of EBPP can be categorized broadly as "Biller Direct," "Third Party Consolidation/Aggregation," and "Customer Consolidation." Each model involves a unique set of end-to-end processes and participants in the enrollment, presentment and payment/remittance phases. *See* NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION'S (NACHA's) COUNCIL FOR ELECTRONIC BILLING AND PAYMENT, BILL PRESENTMENT, *at* http://www.ebilling.org/how/processes/bill-presentment/default.htm (describing the models of EBPP and diagramming their operations). *See also* NATIONAL AUTOMAATED CLEARING HOUSE ASSOCIATION'S COUNCIL FOR ELECTRONIC BILLING AND PAYMENT, ELECTRONIC BILL PRESENTMENT AND PAYMENT (EBPP) BUSINESS PRACTICES (Ed. 2.1 Draft for Public Comment) (May 9, 2000), *at* http://www.cebp.nacha.org/BPv2.1.pdf.

[2] At present, the leading EBPP provider is CheckFree Corporation. Its Web site (http://www.checkfree.com) indicates that it currently serves over five million U.S. consumers; that it is the EBPP provider for over 300 sites including those hosted by a number of major U.S. financial institutions including Bank One, Bank of America and First Union; that it is distributing more than six million bills a year; and that it has 245 live e-billers on the bill presentment side delivering bills electronically. Using the CheckFree service, a consumer can "pay everyone" he pays with checks via electronic payment and with respect to some of the companies the consumer can also begin receiving *and* paying the bill via his PC. *See generally* CHECKFREE CORP., ELECTRONIC BILLING AND

This is called the "consolidation/aggregation" model and the financial institution is considered to be "hosting" the EBPP consolidation site. Such services are generally provided to the consumer either for free or for a small monthly fee (generally between four dollars and thirteen dollars per month). For purposes of this Article, it is assumed that the EBPP service generally works as follows:[3]

- The consumer receives a bill from a biller either electronically or via traditional means.[4] If a bill is received at the EBPP Web site electronically, the consumer may be notified via e-mail.
- The consumer subsequently logs onto the Web site to review the bill. The consumer then electronically instructs the EBPP provider to pay the amount of the bill or a designated portion of it.
- Typically, the consumer can initiate payment via computer instructions to his EBPP provider regardless of whether the bill is delivered to the Web site.[5] Payments generally can be scheduled up to a year in advance; variable and recurring payments can also be scheduled. The consumer can generally review pending payments at the EBPP Web site and have access to payment history at that Web site.

---

PAYMENT, *at* http://www.checkfree.com/ebp. Among other vendors providing EBPP services for financial institutions are PayTrust, Inc., Metavante Corp., and Princeton eCom Corp.

[3] For a general description of the service, see CHECKFREE CORP., *supra* note 2.

[4] At this time, most of a consumer's bills are probably not available for presentment electronically at EBPP Web sites. Some vendors, such as PayTrust Inc., overcome this problem and enable consumers to view most of their bills at the site by using a combination of "scan and pay" and "screen scraping." See Andrew Roth, *Citigroup Uses Card Bills to Build EBPP Clientele*, AM. BANKER, Apr. 9, 2001, at 26 [hereinafter Roth, *Citigroup*]. With scan and pay, the consumer authorizes the biller to send his bills to the EBPP provider's address. The EBPP provider then scans the bills and delivers them to the consumer in electronic format. With screen scraping, the EBPP provider scrapes the biller's Web site for the consumer's bill, gaining access with consumer supplied user names and passwords. CheckFree has announced that it also plans to use screen scraping technology. See Andrew Roth, *CheckFree Says It Will Use Screen Scraping*, AM. BANKER, Mar. 22, 2001, at 10 [hereinafter Roth, *CheckFree*].

[5] In July 2000, the OCC summarized the results of responses to its Internet Banking Questionnaire. Of the responding national banks, 605 offered bill payment for retail customers whereas only 123 banks also offered bill presentment – thus roughly four times as many offered bill payment as offered bill presentment. Sixty-two percent of respondents had a Web site, but only thirty-two percent had transactional Web sites. OCC, SUMMARY RESULTS OF OCC'S INTERNET BANKING QUESTIONNAIRE (July 2000), *at* http://www.occ.treas.gov/ftp/release/2000-84a.pdf.

- The EBPP provider transfers money via the ACH or manual draft out of the consumer's checking or other asset account, credits the consumer's funds into the EBPP provider's own account, and then, if the biller accepts electronic payments, sends payment electronically.
- If the biller cannot be paid electronically, the EBPP provider pays the biller directly with its manual printed check. If a number of the EBPP provider's customers have payments due to such a biller on the same day, the EBPP provider may provide only one check together with a manual listing of the accounts being paid (the "check and list" approach).
- Alternatively, the EBPP provider may print up a draft against the consumer's asset account for the amount owed payable to the biller. That draft, sometimes called a "laser draft," is then mailed to the biller (without the biller provided payment stub) which processes it as any other payment check received unaccompanied by the payment stub.

EBPP has been viewed as a potential blockbuster product of the on-line financial services industry. It has been hyped as the "killer application" enabled by the Internet.[6] Some financial analysts have viewed the EBPP service as very important, since it helps define the customer relationship and because reviewing and paying bills is a time-consuming and hence 'sticky' activity, from the perspective of the Web. Whichever firm is the consumer's choice at which to view and pay bills, can target ads or cross-sell other products while the consumer is reviewing bills.[7]

---

[6] *See* A. Litan, *The Consumer E-Billing Hype Cycle,* GartnerGroup (Dec. 19, 2000), *at* http://gartner11.gartnerweb.com/public/static/hotc/hc00094769.html. *See also* PRICEWATERHOUSECOOPERS, ELECTRONIC BILL PRESENTMENT AND PAYMENT–EUROPAY (Oct. 29, 1999), *at* http://www.paynet.ch/paynet/pageshow/1,3069,291*2*25*8,00.html. Matthew Fassnacht & Raimundo Archibold, "*Architecting" the Open E-Finance Network: Built to Ride the Internet Wave* 32 (July 27, 2000) (Industry Analysis from J.P. Morgan Securities Inc.) (on file with *The Business Lawyer,* University of Maryland School of Law).

[7] Kenneth A. Posner & Athina L. Meetan, *The Internet Credit Card Report: A Primer on the Industry and Its Role in E-Commerce* 4-10 (July 20, 1999), at www.morganstanley.com/techresearch/netcard/info.html (Investment Report from Morgan Stanley Dean Witter).

Recent reviews, however, suggest less positive views of the growth of EBPP services than at earlier points in time. One June 2000 article in the popular press cited to a report from research company Forrester for the proposition that e-pay companies "will bleed money for the next two years and disappear entirely by 2002."[8] Other commentators have confirmed that despite the hype, both billers and consumers have been slow to use EBPP because neither has seen enough desire from the other party, creating a chicken-and-egg conundrum.[9] On-line payments are frequently described today as one of the great unfulfilled hopes of the Internet economy.[10] Presently, the process is perceived as too complicated and expensive for most people, and today the use of electronic bill payments is estimated at less than one percent of all the nation's bill payments.[11] Checks are still the predominant form of consumer bill payment.[12] According to a December 2000 GartnerGroup Research Note:

> Virtually all new technologies and applications go through a hype cycle . . . and consumer e-billing is no exception. Most, but not all, of the implemented consumer electronic bill presentment and payment (EBPP) applications have not addressed the strategic objectives of customer retention and acquisition and have failed to improve customer service in the physical world. Difficult customer enrollment procedures, high costs (averaging $6 a month) and a lack of financial incentives have kept consumers away. Less than 200,000 Americans use e-bill consolidator networks that have been

---

[8]Bill Wolfe, *Critics Say Few People Will Switch: Limited Appeal Seen in Online System,* CHICAGO SUN TIMES , June 4, 2000 at 45A.

[9]Carrick Mollenkamp, *CheckFree to Buy TransPoint LLC in $1 Billion Deal,* WALL ST. J., Feb. 16, 2000 at B6.

[10] Carrick Mollenkamp, *Entrepreneur's Tough Sell: Pay Your Bills Online*, WALL ST. J., Feb. 18, 2000 at B1.

[11] *See id.*

[12] *See generally* PAUL H. GREEN, CHECKS AT THE END OF THE 20TH CENTURY AND BEYOND (1999). In 2001, it is estimated that over seventy billion checks will be issued in the United States. *Id at 128.* Americans write an average of twenty-five checks a month; ten to twelve of these are for bill paying. *Id at* 88. A recent *American Banker* article indicates that the TowerGroup estimates U.S. households paid 19 billion bills in 2000 and, of that amount, about seventy-five percent was paid by check and about seven percent by ACH debit. Peter Lucas, *Where Did the Bills Go?* AM. BANKER, Mar 2, 2001, at 30A.

> patched together during the past two years. Widespread market expectations that EBPP is the biggest "killer application" of them all have not materialized, and consumer adoption has been generally weak. *The market finds itself in a "trough of disillusionment.*" The downturn, however, is temporary and is expected to be followed by steadily increasing consumer adoption as enterprises learn what it takes to get consumers to view their bills on-line.[13]

Some commentators have concluded that the electronic presentment of bills will be a key driver leading to the electronic payment of bills. When consumer bills are presented electronically by the biller and the consumer initiates payment on-line, most such bills are paid electronically via the ACH. With today's technology, bills may be presented via the Internet, mobile phone, or personal digital assistant; however, most consumers still receive their bills via mail. Today, bill payment is frequently initiated electronically even though the bill is received by the consumer in paper form. Among the problems that have thus far prevented the widespread adoption of on-line bill payment are[14]:

- Many billers are not able to deliver their bills electronically (currently fewer than one percent of bills are distributed as well as paid electronically),[15] and it remains inconvenient for the consumer to have

---

[13] Litan, *supra* note 6 at 2 (emphasis added). According to Ms. Litan, GartnerGroup's hype cycle is designed to help enterprises make intelligent decisions about when to implement emerging technologies. It is said to be updated annually and to provide a scorecard to separate hype from reality. The "trough of disillusionment" is one of the five distinct phases in the hype cycle—in it "because the technology does not live up to its inflated expectations, it rapidly becomes unfashionable and the press either abandons the topic or touts its failure to meet expectations." *Id.* at 2.

[14] Mollenkamp, *supra* note 10.

[15] Andrew Roth, *Tech Dollars Going to EBPP*, AM. BANKER, May 22, 2001, at 17 (quoting information provided by Beth Robertson, a Senior Analyst at TowerGroup).

to key payment information into his PC. Some EBPP providers are addressing this problem by using the "scan and pay" or "screen scraping" approach.[16]

- EBPP services are perceived as expensive.
- Many companies are waiting for more on-line customers before spending money to upgrade technology to accept payments electronically and many consumers are waiting until more billers provide bills on-line—the so-called "chicken and egg" conundrum.
- Americans are reluctant to change their banking habits.
- Consumers have on-line security and privacy concerns.

## SIGNIFICANT LAWS APPLICABLE TO EBPP SERVICES

It should be kept in mind that the current financial institution legal and regulatory environment was generally designed for the paper world and brick/mortar branches. While new laws, regulations, and regulatory interpretations dealing with the on-line world have started to surface in the last couple of years, the regulatory and legal environment is obviously subject to additional change and differing interpretations. John E. Muller, writing in late 1998 concerning the state of cyberspace payment systems and the applicable legal principles, concluded that:

> While the emergence of new cyberspace payment systems is unsettled, the role of law and lawyers in the development of these systems is equally unsettled. There are few existing sources of public law which clearly apply to these new products, and legal issues

[16] *See* Roth, *CheckFree, supra* note 4.

> are only one (by no means the most important) of the possible sources of liability associated with the new payment systems, both for payments providers and for users .[17]

Generally, the laws and regulations applicable to a financial institution's products and services will be applicable to the EBPP service, as they are to other products and services offered through cyberbanking means. With cyberbanking, the delivery channel changes, but the laws and regulations generally do not.[18] One commentator has recently remarked that:

> For the most part, Internet banking is governed by the same set of regulations that applies to brick-and-mortar banking. Existing regulations have been adapted to the electronic world; it is up to the bank to make them work in that environment. For a compliance officer this imposes the uncertain responsibility of formulating what can be inferred from the regulations. The definitive source for answering many compliance questions [about Internet Banking] is the "Internet Guidelines" issued by the Federal Financial Institutions Examination Council . . . . As a general

[17] John D. Muller, *Selected Developments in the Law of Cyberspace Payments*, 54 BUS. LAW 403, 440 (1998). Mr. Mueller went on to state that:

> Ultimately, the new payment systems aspire to a state where, as with legal tender and credit cards, the rules are well-settled and essentially hidden in the system. . . . The credit card and ATM networks operate through system rules and private, usually standardized contracts, with an added layer of consumer protection law primarily at the federal level. . . .To reach that state, however, new payment systems will likely first pass through a stage of heavy uncertainty, as it may be unclear whether (i) existing regulatory law applies; (ii) policy makers and interest groups will become persuaded that new regulations need to be created if existing regulations do not apply; and (iii) standard agreements will be enforceable to the extent that a payments provider tries to establish an appropriate balance of competing interests through its agreements and/or private system rules.

*Id.* at 440-41.

[18] Letter from Carmen J. Sullivan, Director, FDIC, July 16, 1998, *at* http://www.fdic.gov/news/news/financial/1998/fil9879.html. This letter states that "[f]inancial institutions should understand that existing federal consumer laws and regulations generally apply to advertisements, transactions and other services conducted electronically." *See also* FED. FIN. INSTS. EXAMINATION COUNCIL, ELECTRONIC FINANCIAL SERVICES AND CONSUMER COMPLIANCE 2 (July 16, 1998), at http://www.fdic.gov/news/news/financial/1998/fil9879a.pdf [hereinafter FFIEC Financial Services Guidance].

> rule, the safest route to minimizing compliance violations is to keep the spirit and intent of existing regulations in mind when applying them in the e-world.[19]

Recently, the Federal Reserve Board (FRB) requested public comment on how its regulations may be adapted to on-line banking and lending.[20] The FRB noted that most of the "legislative and regulatory framework that governs banking was developed based on social, cultural and technological practices that existed before the advent of widespread computer based communications."[21] It indicated that it is trying to assess whether any FRB regulations should be amended in order to facilitate on-line banking. It invited "comment on how particular statutes, regulations, or supervisory policies specifically affect financial institutions and their customers' uses of new technologies."[22]

The legal analysis in this Article is based on the following assumptions: the EBPP service will be offered at a financial institution's home banking Web site, it will be provided under the financial institution's name, and operational support for the service will be outsourced to an EBPP vendor. Both

---

[19] Allie Buzzell, *Internet Compliance: Old Regulations, New Responsibilities*, ABA BANK COMPLIANCE, Nov/Dec. 2000, at 13-14. Another commentator has noted that:

> Though compliance requirements were premised on physical presence and proximity, cyberbanking is premised on remote access and the avoidance of that very physical presence and proximity . . . . There are no exceptions to the Truth in Lending Act, Truth in Savings Act or darn near Truth in Anything Act for electronic banking, and thus the disclosure content, format and timing rules apply in all their glory, as do the process oriented requirements of those laws.

Robert P. Chamness, *A Funny Thing Happened on the Way to the 21st Century*, ABA BANK COMPLIANCE, May/June 1998, at 34.

[20] Study of Banking Regulations Regarding the Online Delivery of Financial Services; Request for Comments, 66 Fed. Reg. 27912 (May 21, 2001) [hereinafter Study of Banking Regulations]. This request was made because the Gramm-Leach-Bliley Act requires federal banking regulators to conduct a study of existing regulations and to submit a report about adapting existing legislative or regulatory requirements to on-line banking. 15 U.S.C. §6808 (Supp. V 1999).

[21] Study of Banking Regulations, 66 Fed. Reg. at 27913.

[22] *Id.*

financial institutions and EBPP vendors are referred to in this Article as "EBPP providers." For purposes of this analysis, only EBPP services offered by regulated financial institutions located in the United States and transactions governed by U.S. laws or the laws of the fifty states will be considered. The conclusions expressed assume that the consumer has an established deposit account at a financial institution, that the EBPP service is provided by that financial institution, and that it is just one means of accessing funds on deposit in such account. Additional laws, regulations, and regulatory guidance are applicable to the basic deposit account relationship.[23]

## POWER AND AUTHORIZATION TO OFFER EBPP SERVICES

The threshold legal issue for a financial institution that proposes to offer EBPP services is whether it has the power and authority to do so. The National Banking Act empowers national banks to exercise "all such incidental powers as shall be necessary to carry on the business of banking."[24] In 1997, the Office of the Comptroller of the Currency (OCC) expressly authorized national banks, by regulatory interpretation, to engage in electronic banking stating that "a national bank may perform, provide, or deliver through electronic means and facilities any activity, function, product or service that it is

---

[23] For example, the Truth in Savings Act of 1991, 12 U.S.C. § 4301 (1994), and Regulation DD, 12 C.F.R. § 230 (2001), require depository institutions to provide disclosures so that consumers can make meaningful comparisons among depository institutions. The Expedited Funds Availability Act, 12 U.S.C. § 4002 (1994), and Regulation CC, 12 C.F.R. § 229 (2001), require depository institutions to comply with certain requirements with respect to the availability of funds and to make specific disclosures regarding their policies. Various sections of the Federal Reserve Act, 12 U.S.C. §§248 (1994 & Supp. V 1999), 461(a)-(c) (1994), 465 (1994), 466 (1994), 601(1994), 615 (Supp.V 1999), and Regulation D, 12 C.F.R. § 204 (2001), impose reserve requirements on asset accounts maintained at a depository institution. Provisions of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1994 & Supp. V 1999), may be applicable with respect to the obtaining and providing of information regarding the deposit account. Provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §6801-6809 (Supp. V 1999) and Regulation P, 12 C.F.R. § 216 (2001) are applicable with respect to an institution's privacy policies concerning customer information, disclosure of such policies and the sharing of information with respect to customers. Regulation J, 12 C.F.R. § 210 (2001), specifies the rules applicable to the collection of checks and other cash and noncash items and the handling of returned checks by Federal Reserve banks.

[24] 12 U.S.C. § 24(Seventh) (1994).

otherwise authorized to perform, provide or deliver."[25] A number of OCC approvals indicate that the OCC has been very supportive of national banks providing EBPP services and has had little problem determining that bill payment services are within the permissible realm of the business of banking.[26]

For state financial institutions, power to undertake specific activities generally comes from state laws and the statutes of the state chartering authorities. This power is subject to the restraints that can be imposed by federal law.[27] Federal law currently permits state-chartered financial institutions to engage in any activity that is permissible for national banks as principal. Consequently, "OCC precedents on bank permissible activities generally define the parameters of permissible state bank activities."[28] Additionally, while the statutory scheme pursuant to which the Federal Reserve system operates generally does not provide enabling powers to the financial institutions it regulates, the Federal Reserve has approved electronic banking activities for financial institutions which "precedents provide comfort that the performance of traditional banking activities through electronic means is permissible."[29] In order to determine whether a particular state-chartered financial institution is constrained in the offering of EBPP services, the specific state laws applicable to that institution would need to be reviewed. It is likely that

---

[25] 12 C.F.R. § 7.1019 (2001).

[26] *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, CONDITIONAL APPROVAL #221 (Dec. 4, 1996), at http://www.occ.tras.gov/interp/dec/conda221.pdf (giving approval for a group of financial institutions to form Integrion LLC to develop and operate a platform for home banking services over the Internet including bill payment); OFFICE OF THE COMPTROLLER OF THE CURRENCY, CONDITIONAL APPROVAL # 289 (Oct. 2, 1998) *at* http://www.occ.treas.gov/interp/nov98/ca289.pdf (giving approval for the same consortium to enter into an agreement with CheckFree and acquire warrants in it); OFFICE OF THE COMPTROLLER OF THE CURRENCY, CONDITIONAL APPROVAL #304 (Mar. 5, 1999) *at* http://www.occ.treas.gov/interp/apr99/ca304.pdf (giving approval for Citibank to invest in TransPoint to provide bill payment services).

[27] *See generally* John L. Douglas, *Cyberbanking: Legal and Regulatory Considerations for Banking Organizations*, 4 N.C.BANKING INST. Apr. 2000, at 57, 62 (Apr. 2000).

[28] *Id.*; *see* 12 U.S.C. § 1831a(a), (i) (1994).

[29] Douglas, *supra* note 27 at 62.

EBPP activities would be permissible unless the applicable state statutory scheme contains a specific prohibition.

Generally, none of the federal banking agencies require prior approval for an existing financial institution to offer EBPP services; however, prior notice is apparently required by the Office of Thrift Supervision before a savings and loan association begins offering such services.[30]

### STATE LAW APPLICABLE TO THE EBPP PROVIDER'S RELATIONSHIP WITH ITS CONSUMER CUSTOMER

The question of which state's or country's laws control an Internet relationship is still developing. The financial institution's agreement with its customer should clearly specify the state whose laws it determines to be applicable. If a consumer has a deposit account at a brick and mortar financial institution in his state of residence, arranges for EBPP services through that financial institution, and is subject to a customer agreement providing that the laws of the state where the financial institution branch at which the consumer banks is the applicable law, the law of the state specified in the agreement would probably be applicable. Beyond that simple conclusion for a simple fact situation, the answer as to the applicable law may depend on the state in which litigation occurs, the specific laws at issue, and the facts in each particular situation. It is possible that the laws of the consumer's state of residence would control certain aspects of the EBPP service irrespective of the contractual choice of law provision.[31]

As in any situation where a vendor is involved that is providing retail services to consumers in multiple states, the financial institution's counsel should verify that the processes, procedures, and documentation set up by the vendor for the financial institution's customers are in compliance with the

[30] *Id.* at 63. 12 C.F.R. § 555.300(b) (2001).

[31] *See* Jeffrey I. Langer, *The Scope of Exportation: Some Unresolved Issues After* Smiley v. Citibank, 52 BUS. LAW 1065, 1071 (1997).

appropriate state laws. Simply because the vendor is located in one state is not determinative and is probably not particularly relevant to the issue of whether that state's laws are applicable to the relationship.

In its May 2001 Request for Comments, among the questions that the FRB asked financial institutions to comment on was whether particular aspects of conducting on-line banking activities could benefit from a single set of legal standards that can be applied uniformly nationwide. It also asked whether there are any inconsistencies between federal and state laws that impede the electronic provision or use of financial products of services.[32]

LAWS REGULATING THE PROTECTION OF CONSUMERS

Consumers using EBPP systems as described above are protected in various ways and to various extents by the federal Electronic Fund Transfer Act (EFTA) and Regulation E (Reg E),[33] and by state electronic fund transfer laws and regulations (State Laws). The EFTA provides the "basic framework establishing the rights, liabilities and responsibilities of participants in electronic fund transfer systems."[34] EBPP providers are also covered by various statutory prohibitions against unfair or deceptive practices.[35] The Truth in Lending Act (TILA) and Regulation Z (Reg Z) are not generally applicable to EBPP

---

[32]*See* Study of Banking Regulations, s*upra* note 20.

[33]Electronic Fund Transfer Act, 15 U.S.C. §§ 1693-1693r (1994 & Supp. V 1999); FRB Regulation E, 12 C.F.R. § 205 (2001).

[34] 15 U.S.C. § 1693(b) (1994 & Supp. V 1999).

[35] *See, e.g.,* Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. ANN. 505/1 (West 1999 & West Supp. 2001).

services such as those described in this article; certain provisions would apply if the consumer was permitted to use a credit card account as the account from which bill payments would be made.[36]

### *EFTA, Reg E and the Official Staff Commentary on Reg E.*

The EFTA establishes the basic rights, liabilities and responsibilities of consumers who use electronic fund transfer (EFT) services and of financial institutions that offer those services. The primary objective of the EFTA and Reg E is the protection of individual consumers engaged in EFTs.[37] The requirements of EFTA and Reg E are generally applicable to financial institutions which offer EBPP services to their deposit account customers by virtue of the definition of "electronic fund transfer" to mean "any transfer of funds that is initiated through a[] . . . computer . . . for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account."[38] A recent comment added to the Reg E Official Staff Commentary (Commentary) provides explicit guidance on this point stating that, generally, the definition of electronic fund transfer in Reg E covers bill payment services.[39]

[36] Truth in Lending Act, 15 U.S.C.A. §§ 1601-1666j (1994); FRB Regulation Z, 12 C.F.R. § 226 (2001). If the financial institution permitted its EBPP customers to pay bills through charges to a credit card account, a payment charged to that account would be subject to Reg Z rather than Reg E since Reg E only applies to EFTs if an "account" is involved. 12 C.F.R. § 205.3(a) (2001). The term account is defined in Reg E as an "asset account." 12 C.F.R. § 205.2(b)(1) (2001). Consequently, since credit card transactions do not involve asset accounts, Reg E does not apply to them. There are no federal requirements comparable to those of Reg E that apply specifically to EFTs where a credit account is charged. A disputed bill payment charged to a credit card account would be covered by Reg Z §§ 226.12(c) or 226.13. No additional requirements are triggered under Reg Z simply because the transaction is electronically initiated rather than initiated with a paper sales draft--thus, the normal Reg Z rules would most likely apply to such a transaction and it would simply be one among many transactions charged to the credit card account and subject to the same Reg Z requirements. If a financial institution offers the credit card payment option, then it must make sure that its EBPP contract does not create the impression that Reg E (e.g. the error resolution requirements) applies to bill payments charged to a credit card account.

[37] 12 C.F.R. § 205.1(b) (2001).

[38] *Id.* § 205.3(b) (2001).

[39] Amendments to Official Staff Commentary to Regulation E, 66 Fed. Reg. 15187, 15193 (Mar. 16, 2001) (to be codified at 12 C.F.R. pt. 205, Supp. 1). Comment 3(b)-1.vi reads as follows:

> *Fund transfers covered.* The term "electronic fund transfer" includes:
> * * *

The EFTA and Reg E require that consumers receive initial disclosure statements[40] and periodic disclosure statements.[41] They also contain consumer protections limiting the liability of the consumer for unauthorized transactions[42] and requiring financial institutions to investigate and resolve errors.[43] Further requirements are imposed with respect to notification of specified changes in terms and an error resolution notice that must be provided at least annually.[44]

*Dispute Resolution and Liability for Unauthorized Transactions*. One of the questions that may be asked by a consumer who is thinking about enrolling for EBPP services is what are the real live risks

---

> A payment made by a bill payer under a bill-payment service available to a consumer via computer or other electronic means, unless the terms of the bill-payment service explicitly state that all payments, or all payments to a particular payee or payees, will be solely by check, draft, or similar paper instrument drawn on the consumer's account, and the payee or payees that will be paid in this manner are identified to the consumer.

*Id.*

[40] 15 U.S.C. § 1693c(a) (1994) and 12 C.F.R. § 205.7(b) (2001) specify the initial disclosures that must be made when the consumer contracts for an EFT service.

[41] 15 U.S.C. § 1693d(c) (1994) and 12 C.F.R. § 205.9(b) (2001) require that periodic statements must be provided for an account to or from which EFTs can be made. This applies to a financial institution that permits its asset accounts to be affected by ACH debits. Such periodic statement must be sent for each monthly cycle in which an EFT has occurred, and at least quarterly if no transfer has occurred. Designated information is required to be provided on each such statement. 15 U.S.C. § 1693d(a) (1994) and 12 C.F.R. § 205.9(a) (2001) require that consumers must be provided with receipts at electronic terminals. Reg E section 205.2(h) comment 1.ii, however, clarifies that a terminal receipt need not be provided when "[a] consumer initiates a transfer by a means analogous in function to a telephone, such as by home banking equipment. . . ."

[42] 15 U.S.C. §1693g(a) (1994); 12 C.F.R. § 205.6 (2001). Three possible tiers of liability are specified. A consumer may be liable for (i) up to $50 (if notification is given to the financial institution within two business days after learning of the loss or theft of the access device); (ii) up to $500 (if the financial institution is not notified within two business days); or (iii) an unlimited amount depending on when the unauthorized EFT occurs (i.e. if the consumer does not notify the financial institution within sixty days after receiving a periodic statement showing an unauthorized transaction and unauthorized transactions occur subsequent to the sixty day period that could have been avoided with appropriate notification). 12 C.F.R. §205.6(b) (2001). A consumer can be held liable for unauthorized EFTs that do not involve an access device, but than only the third tier of consumer responsibility is applicable. *Id.* If state law imposes lesser liability, then the state law provisions control.

[43] 15 U.S.C. § 1693f (1994); 12 C.F.R. § 205.11 (2001).

[44] 15 U.S.C. §§ 1693c(a)(7), (b) (1994); 12 C.F.R. § 205.8 (2001).

in using the service. A simple answer is that the consumer is probably safe from liability for unauthorized transactions; additionally transaction errors should be corrected. The consumer, however, will not necessarily avoid short-term inconvenience in connection with his financial or bill payment accounts. To date,

> [M]ost "live" problems with EBPP have apparently involved errors in executing transactions rather than fraudulent transactions. With respect to these, the financial institution must resolve such problems in accordance with the error resolution requirements of the EFTA and Reg E. Generally, the inconvenience of having one's checking account or relationships with billers disturbed for a period of time due to an error may be a more realistic problem than concerns about its ultimate resolution.[45]

Federal examiners look at how financial institutions handle customer complaints about EFT errors.[46] The financial institution is required to investigate any alleged error or unauthorized transaction and report back to the consumer within ten business days; the financial institution may take up to forty-five days if it provisionally recredits the consumer's account while it continues to investigate.[47] These requirements only apply if the consumer's notification involves a defined "error." In connection with the EBPP product these would generally include: an unauthorized bill payment; an incorrect bill payment;

---

[45] Ann Spiotto & Brian Mantel, *Rethinking Business: Electronic Bill Payment and Presentment and Aggregation,* ABA BANK COMPLIANCE, May/June 2001, at 18, 20. Industry sources indicate that one common error alleged by consumers involves late payment of a bill and the consequent late fees imposed by the biller. CheckFree guarantees its customers that it will bear the responsibility for any late-payment-related charges (up to $50) should a "payment arrive after its due date as long as you scheduled the transaction in accordance with the service's terms and conditions." *See* CHECKFREE CORP., *supra* note 2. This guarantee contractually commits CheckFree to reimburse consumers. Whether or not it obtains reimbursement from billers for any refunded late fees depends upon voluntary action by the biller. Billers may be unwilling to reimburse customers for late payment fees resulting from the involvement of an EBPP service not authorized or agreed upon by the biller--apparently some number of such payments result from the additional time involved in the manual handling of payments necessitated when the biller-provided billing stub does not accompany either a laser draft or a "check and list" payment.

[46] Lucy Griffin, Calvin R. Higgins, & Gary Louis, *Eliminating Mistakes by Taking Note of Them: Common Exam Violations and How to Avoid Them,* ABA BANK COMPLIANCE, Jan./Feb. 2001, at 30.

[47] 12 C.F.R. § 205.11(c) (2001).

omission of a bill payment from the periodic statement; a computational or bookkeeping error in connection with a bill payment; the incorrect identification of a bill payment; and a request for documentation or additional information with respect to a specific bill payment transaction.[48] The error resolution requirements appear to apply to a bill payment transaction where the consumer is signed up for the bill payment service and initiates the transaction via the computer, even if the bill is paid with a check sent by the EBPP provider to the biller.[49]

One issue frequently raised in connection with the use of "screen scraper" technology is whether the consumer is liable for transactions that are made possible because the screen scraper was given account information (including the consumer's ID and account password) in connection with the sign up for the service. The EBPP model under discussion in this Article renders the question moot since it involves a financial institution offering the EBPP product under its own name at its on-line banking Web site and charging the consumer's asset account at the same financial institution for the EFT transactions. To the extent that unauthorized transactions occur because the consumer provided his password to the EBPP site, the consumer has provided the "secret" information to his own financial institution or its agent. Consequently, the financial institution should obviously be precluded by general principles of estoppel or contributory negligence from asserting against the consumer that he had "authorized" the screen scraper and its or the financial institution's employees to act.[50]

---

[48] *Id.* § 205.11(a).

[49] Recent Commentary revisions clarify that computer-initiated payments are covered by the regulation unless the service agreement explicitly states that all payments (or all payments to identified payees) will be made solely by check, draft or similar paper instrument drawn on the consumer's account. Amendments to Official Staff Commentary to Regulation E, 66 Fed. Reg. 15187, 15193 (Mar. 16, 2001) (to be codified at 12 C.F.R. Pt. 205.3(b), Supp.1, cmt. 3(b)-1.vi). Presumably since computer initiated payments are covered by the regulation, such payments (even if made by paper instrument) are protected by the error resolution requirements of section 205.11

[50] Concern has been expressed in the trade press recently about the dangers of information aggregation. Two primary categories of unauthorized transactions could potentially result from "secret" information being provided to an EBPP site:

- Those resulting from a hacker accessing the [EBPP] site and using information from it.

With respect to more generic unauthorized transactions made through an EBPP site that are unrelated to the fact that the consumer disclosed his "secret" information,[51] the financial institution hosting the site (which for purposes of this discussion is also the account holding financial institution) has responsibility to reimburse the consumer. This is, of course, subject to the consumer's responsibility for certain amounts based upon the date notification is given by the consumer. Although the financial institution has legal responsibility to the consumer for unauthorized transactions, *after taking care of the consumer,* that financial institution may be able to shift the ultimate liability to the outsourcing vendor based upon contractual provisions allocating responsibility.[52]

> Simple answers, however, do not necessarily mean that the customer is always made whole – of crucial importance is whether the consumer's claim that a transaction is unauthorized is believed. If the financial institution does not believe that the transaction is unauthorized (and instead concludes that it is "attempted customer fraud" or that it was authorized) it will not reimburse the consumer voluntarily and litigation may be necessary to resolve the factual issue. Additionally,

---

- Those resulting from the use of information by those providing the site, their agents or employees.

Spiotto et al., *supra* note 45, at 20, 22. The consumer has liability for "authorized" transactions – he has very limited liability for "unauthorized" transactions. *Id.* at 19. The determination of liability depends on the specific facts. If the facts involved an EBPP service provided by a portal the issue becomes potentially more problematic for the consumer. *Id.* at 19-20. Should the non-financial institution EBPP provider or one of its employees make EFTs in a manner different than that originally authorized by the consumer, it is not entirely clear whether the account holding financial institution rather than the consumer would bear the financial loss resulting from such transfers. Under current laws and regulations responsibility may vary depending upon the type of challenged transaction and/or the account from which the transaction is made. Generally, the consumer has rights to be made whole by the financial institution holding the account on which the challenged transaction occurs and, generally, a financial institution (but not necessarily the account holding financial institution) will be the party ultimately responsible. A discussion of various fact scenarios and the possible outcomes with respect to allocation of liability appears in a recent ABA BANK COMPLIANCE article. *See id.*

[51] This might occur, for example, if the consumer left the password/user ID information for the EBPP site on a piece of paper next to his computer at work and an unauthorized person found that information and used it to sign on and to direct payment of the crook's own credit card bills.

[52] Spiotto et al., *supra* note 45, at 22.

reimbursement may turn on whether the financial institution knows the law and, perhaps more important, whether its customer service staff understands what is legally required.[53]

*Electronic Disclosure*. Recent amendments have been made to Reg E and the Commentary to establish uniform standards for the electronic delivery of Reg E disclosures. These amendments were styled as "Interim Final Rules" and the FRB requested comment from the public (with the comment period ending June 1, 2001).[54]

The amendments set forth the general rule that financial institutions subject to Reg E may provide disclosures electronically provided that they comply with both the requirements set forth in Reg E and the consumer consent requirements of the Electronic Signatures in Global and National Commerce Act (E-SIGN).[55] E-SIGN requires the financial institution to disclose the requirements for accessing and retaining disclosures in electronic format--the consumer must affirmatively consent electronically to electronic delivery (in a manner that demonstrates the ability to access the information electronically). Prior to consenting to the electronic delivery, the consumer must also be presented with a number of "clear and conspicuous" disclosures about the electronic delivery process itself.[56]

---

[53] *Id.* The financial institution might try to argue that the consumer was negligent in leaving his user ID and password next to the computer and thus that the financial institution has no liability. Reg E, however, *expressly provides* that the consumer's liability for unauthorized use is limited (based upon the timing of notification). The Commentary clarifies that

> Negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E. *Thus, consumer behavior that may constitute negligence under state law, such as writing the PIN on a debit card or on a piece of paper kept with the card, does not affect the consumer's liability for unauthorized transfers.*

12 C.F.R. pt. 205, Supp. 1 at 205.6(b)2 (2001) (emphasis added).

[54] Regulation E Interim Rule (for electronic delivery of disclosures), 66 Fed. Reg. 17,786, 17,793 (Apr. 4, 2001) (to be codified at 12 C.F.R. §205.17).

[55] *Id.*

[56]Pub. L. No. 106-229, Tit. I, § 101, 114 Stat. 464 (2000 (to be codified at 15 U.S.C. § 7001(c)(1). The consumer must be informed of his right to have the disclosures on paper and to withdraw his consent to electronic disclosure; the consumer must be informed whether the consent applies to a specified transaction or to identified categories of

Additionally, a financial institution that uses electronic communication to make Reg E disclosures must send the disclosure to the consumer's e-mail (electronic) address or it must make it available at another location (e.g. an Internet Web site) *and* the financial institution must tell the consumer that the disclosure is available by sending notice to the consumer's e-mail (or postal address) and making it available at the Web site for at least ninety days from the notification date.[57] If a *required disclosure* transmitted electronically is returned undelivered, the financial institution must take reasonable steps to redeliver it.[58]

---

records that may be provided during the course of the relationship; the financial institution must describe how the consumer withdraws his consent to electronic disclosure and how to update his contact information; the consumer must be told that after consent, he may request a paper copy. *Id*.

[57] Regulation E Interim Rule, 66 Fed. Reg. at 17,703.

[58] *Id.* If a consumer has contracted for EBPP, the financial institution holding the asset account from which EFTs (i.e., bill payments) are being made is required to send the consumer a periodic statement containing defined information. This periodic statement, which is generally incorporated within the basic checking account statement, is a "required disclosure" under Reg E. E-mail notification and redelivery requirements are applicable in connection with this periodic statement if the financial institution has elected to deliver such required disclosure electronically.

It is unclear whether the e-mail notification provisions are directly applicable to the EBPP provider transmitting "required disclosures" for a biller. Nothing in Reg E specifically requires an *EBPP provider* to send e-mail notification when bills are received at the EBPP Web site; such bills may or may not be "disclosures" that the billers are required to send (and the EBPP provider has no knowledge as to whether or not they are). If the EBPP provider is sending e-mail notification, this is probably done from a product design standpoint in order to enable the consumer to view bills in a timely manner. If there is no regulatory requirement directly applicable to the EBPP provider for e-mail notification, it follows that there should be no regulatory requirement directly requiring the EBPP provider to redeliver such notification (if returned undeliverable) to a different consumer address.

However, certain *billers* may be subject to regulatory requirements where a periodic statement (bill) is being delivered electronically. Such regulatory provisions (*if* they exist in connection with a particular type of bill) would probably be found in the regulation, if any, setting forth basic requirements for the billed service/product. For example, in connection with credit card accounts, Reg Z makes the delivery of bills a required disclosure. Recent changes to Reg Z (which generally parallel those in Reg E) authorize the electronic delivery of required disclosures. Obviously the creditor is only *required* to send one periodic statement per billing period -- if the creditor continues to provide paper disclosures to all consumers then the requirements for e-mail notification and redelivery would not apply to those statements displayed on an Internet site. If the creditor is providing the bill to the EBPP provider as its sole means of delivery, however, it may need to rely upon that provider to transmit the required e-mail notification to the consumer. It would be prudent for the creditor to contractually require such EBPP provider to send e-mail notification and attempt redelivery if the e-mail notification is returned. *Note*: at this time the mandatory effective date for the Reg Z electronic disclosure changes is also on hold and compliance is not required until the FRB issues Final Rules.

A number of the comments provided to the FRB indicated that extremely serious operational issues are raised by the above described notification and redelivery requirements. Based upon these comments, the FRB is considering adjustments to the rules to provide additional flexibility. The amendments were to have had a mandatory effective date of October 1, 2001—by an announcement dated August 3, 2001, the FRB has lifted the mandatory compliance date.[59] It has indicated that institutions may continue to provide electronic disclosures under their existing policies and practices or may follow the amendments until the FRB issues permanent rules.[60]

The new Commentary provisions specifically clarify that E-SIGN authorizes the use of electronic disclosures; it does not affect any other requirement imposed under Reg E and it does not affect the content or timing of disclosures. Electronic disclosures remain subject to Reg E's format, timing and retainability rules.[61]

*Preemption Under Reg E*. The EFTA preempts inconsistent state requirements.[62] However, requirements are not inconsistent if they are more protective of consumers (e.g. if they specify additional fact patterns as "errors" or provide for lesser consumer liability than EFTA).[63] They are considered to be

---

[59] Press Release, Federal Reserve Board, Compliance Date Lifted for Electronic Consumer Disclosures (Aug. 3, 2001), *available at* http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010803/default.htm.

[60] *Id.* The operational difficulties with the redelivery requirement appear to be significant. It appears problematic for the process to be automated. If the process cannot be automated, people would need to manually work the returned e-mails for redelivery. While the degree of difficulty is somewhat dependent on how frequently e-mail notifications are returned; the initial assessment is that consumers change e-mail addresses frequently, and, thus, that return of e-mails would occur far more frequently than return of U.S. mail. *See, e.g.,* Letter from Hudson L. Cook, Hudson Cook, LLP, to Ms. Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System (May 31, 2001) (on file with *The Business Lawyer,* University of Maryland School of Law).

[61] Regulation E Interim Rule, 66 Fed. Reg. 17,786, at 17,793 (Apr. 4, 2001).

[62] 15 U.S.C. § 1693q (1994); 12 C.F.R. §205.12 (2001).

[63] A number of states have provided greater limits on a consumer's liability for unauthorized EFTs. The preemption provisions of EFTA and Reg E would not preempt these state laws. *See, e.g.,* KAN. STAT. ANN. § 9-1111d (West Supp. 2000) (consumer's liability for an unauthorized transaction by a machine readable instrument not to exceed $50); MINN. STAT. § 47.69 (2000) (financial institution is liable for all unauthorized withdrawals from an

inconsistent if the state law requires initial or periodic disclosures that are different in content from those required by EFTA except to the extent that they relate to consumer rights granted by state law and not federal law.[64]

*Retention Requirements*. Regulation E requires a financial institution to retain evidence of compliance for not less than two years from the date disclosures are required to be made or action is required to be taken.[65] That period is extended if notice is received of an enforcement proceeding or investigation by the financial institution's enforcement agency.[66] It is not necessary to retain records that the financial institution has given disclosures to each consumer--the financial institution "need only retain evidence demonstrating that its procedures reasonably ensure the consumer's receipt of required disclosures and documentation."[67] Information required to be retained must be retrievable in usable form. If records are not kept in hard copies, the electronic copies must be kept for the entire term of their retention period and not automatically deleted at some earlier period or rendered meaningless due to system changes and conversions or modifications to form letters.

***State Laws.***

Various states have adopted various consumer protection laws that may be applicable to EBPP services. According to one prominent lawyer who has spent many years working with the banking industry and financial electronic commerce:

---

electronic financial terminal unless loss was due to the loss or theft of the customer's machine readable card, in which case the customer is liable for a maximum of $50).

[64] 12 C.F.R. pt. 205, Supp. 1 § 205.12(b)(2)(iv) (2001).

[65] *Id.* § 205.13(b)(1).

[66] *Id. §* 205.13(b)(2).

[67] *Id.* § 205.13(b)(1).

> State EFTA laws that directly regulate EFT transactions generally follow the model of the Federal EFTA. Typically, these laws generally apply to consumer asset accounts, and do not apply to consumer credit accounts or business accounts. State EFT laws also focus primarily on consumer rights, and provide consumer protections that match, or in some cases exceed, the protections contained in the EFTA. Colorado, Illinois, Iowa, Kansas, Massachusetts, Michigan, Minnesota, Montana, and New Mexico all have enacted EFT statutes of this type. State consumer protections generally include limitations on consumer liability for unauthorized transactions, restrictions on unsolicited issuance of cards or other access devices, and initial and periodic disclosure requirements.[68]

Under the EFTA only state laws that are inconsistent are preempted. A state law is not inconsistent if it is more protective of consumers.[69] If a state law is not preempted by the EFTA, whether a contract's choice of law provision would be enforced to render a state's consumer protection statute ineffective in a specific situation depends upon the particular facts at issue. The determination could turn on the state statutory and common law with respect to enforceability of a choice of law provision in the particular state. It is possible that, irrespective of a choice of law

---

[68] THOMAS P. VARTANIAN ET AL., 21st CENTURY MONEY, BANKING & COMMERCE 77-78 & n.196 (1998). Mr. Vartanian cites to the following state laws at n.196 as focusing primarily on consumer rights, and providing consumer protections that match, or in some cases exceed, the protections contained in the federal EFTA: COLO. REV. STAT. ANN. §§ 11-6.5-101 to-111 (West 1990 & Supp. 2000) (commercial banks); COLO. REV. STAT. ANN. §§ 11-48-101 to-107 (West 1990 & Supp. 2000) (savings associations, credit unions, and industrial banks); 205 ILL. COMP. STAT. ANN. 616/1-616/89; IOWA CODE § 527.1-12 (west 2001) (savings associations); KAN. STAT. ANN. § 9-111d (Supp. 2000) (banks), § 17-5565 (1991) (savings and loan associations); MASS. GEN. LAWS ANN. ch. 167B, §§ 1-24 (West 1994 & Supp. 2001) (electronic banking); MICH. COMP. LAWS ANN. §§ 450.831-849 (West Supp. 2001) (electronic transactions); MINN. STAT. ANN. §§ 47.61-.74 (West 1988 & Supp. 2001) (financial corporations); MONT. CODE ANN. §§ 32-6-101 to –309 (2001); N.M. STAT. ANN. §§ 58-16-1 to –17 (Michie 1978 & Supp. 2001 (financial institutions).

[69] 15 U.S.C. § 1693q (1994); 12 C.F.R. § 205.12 (2001).

provision in the contract, a state law may be applicable if enforcement of the contractual provision or practice would hurt the consumer and the law in the consumer's state of residence would provide stronger protection for the consumer.[70]

***Unfair and Deceptive Trade Practices Statutes.***

Under both federal and state law, it is illegal to engage in unfair or deceptive trade practices.[71] Many practices that a consumer would argue to be misleading or unfair/deceptive (including unwarranted or inaccurate claims in advertising materials) can result in allegations that the statutory prohibitions have been violated. Care should be taken to assure that all Web page data is accurate and should reflect the actual product being offered and the practices of the financial institution.

MISCELLANEOUS LAWS AND REGULATIONS

***Laws Applicable to ACH Transactions.*** To the extent that payments are made by the EBPP provider via the ACH or that funds are removed from the consumer's deposit account via the ACH, then the NACHA Rules governing the ACH,[72] Regulation J,[73] the EFTA, Reg E, and state laws would be applicable to the processing of such transactions and to resolving problems that arise with respect to such processing.

[70] *See, e.g.*, Langer, *supra* note 31, for a general discussion of state law preemption issues facing financial institutions after the U.S. Supreme Court's decision in *Smiley v. Citibank*, 517 U.S. 735 (1996).

[71] 15 U.S.C. § 45(a)(1) (1994 & Supp. 1999). *See, e.g.*, Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. ANN. 505/1 (West 2000 & Supp. 2001).

[72] NACHA, ACH RULES (2001).

[73] 12 C.F.R. § 210 (2001).

***Bank Service Company Act***. Where a financial institution is providing EBPP services and outsourcing the operations to a third party, the Bank Service Company Act allows the bank regulatory agencies examination authority over such third party.[74] Additionally, the bank is required to notify the Federal agency with examination authority over it of the existence of the relationship within thirty days after the making of the service contract or the performance of the service, whichever is first.[75]

***State Contract Law***. General state contract law principles and statutory provisions govern the contractual relationship between the EBPP provider and its customers.

***State and Federal Criminal Laws***. General state and federal criminal statutes would be applicable in the event or fraud or other misbehaviors by the EBPP provider or by the customer. However, the effectiveness of such laws in regulating EBPP provider or customer behavior may be limited by the willingness of state and federal prosecutors to pursue criminal law violations. The mere possibility that such laws apply does create incentives to act reasonably.

Financial institutions have an obligation to file a Suspicious Activity Report with the appropriate law enforcement agencies and the Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury whenever known or suspected criminal violations of federal law or a suspicious

---

[74] 12 U.S.C.A. §§ 1861-1867 (1994 & Supp. V 1999). Section 1867c provides:

> Whenever a financial institution that is regularly examined by an appropriate Federal banking agency, or any subsidiary or affiliate of such a bank that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises--
> (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises, and
> (2) the bank shall notify such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.

[75] *Id.*

transaction related to a money laundering activity or a violation of the Bank Secrecy Act is detected.[76] Additionally, financial institutions have an obligation to comply with defined record keeping and reporting requirements with respect to transactions in currency and monetary instruments.[77]

***State Escheat Statutes***. States generally have statutory provisions requiring that unclaimed property be turned over to the state.[78] There will doubtless be funds retained by the EBPP provider in connection with EBPP transactions with respect to which the proper owner cannot be identified or cannot be located. Generally, the state of the consumer's last known address is entitled to escheat the unclaimed property of such person, irrespective of where the EBPP provider is located. An EBPP provider would need to determine whether any basis exists for the position that unclaimed funds are not subject to such laws. If no legitimate basis can be determined, procedures must be implemented by the EBPP provider to assure compliance.

***Fair Credit Reporting Act (FCRA).*** The FCRA imposes requirements on entities that collect, transmit, and use information on consumers for the purpose of making credit and certain other business decisions.[79] Businesses are allowed to gather and use their own experience information in making credit decisions and to share certain aspects of that information with credit reporting agencies. Businesses are also allowed to use information from credit bureaus in making credit and certain other decisions, subject

---

[76] 31 C.F.R. § 103.18 (2001).

[77] 31 U.S.C. §§ 5311-5330 (1994); 31 C.F.R. § 103 (2001); 12 C.F.R. §§ 326.8 and 353 (2001).

[78] *See, e.g.*, the Illinois Uniform Disposition of Unclaimed Property Act, 765 ILL. COMP. STAT. ANN. 1025/1-1025/30 (West 2000 & Supp. 2001); Indiana Uniform Disposition of Unclaimed Property Act, IND. CODE ANN. § 32-9-1-1 to -45 (Michie 1995 & Supp. 2000); Iowa Uniform Disposition of Unclaimed Property Act, IOWA CODE ANN. §§ 556.1-.30 (West 2001).

[79] 15 U.S.C.A. §§ 1681-1681u (1994 & Supp. V 1999).

to obligations that are imposed when credit or access to other services or opportunities is denied on the basis of information contained in the credit report.[80]

Each EBPP provider needs to review its procedures and policies and determine whether FRCA is applicable. A major EBPP provider, CheckFree, was sued under FCRA in connection with a credit score that it obtained without the consumer's consent. CheckFree had ordered credit scores on over 1.3 million customers from the Experian credit bureau. The court concluded that because there was a legitimate business transaction initiated by the consumer, CheckFree was not subject to liability under FCRA for obtaining the credit score.[81]

***FDIC Official Advertising Statement***. Every insured depository institution's on-line system top level page, or "home page" is considered by the FDIC to be an advertisement. Consequently any such financial institution should display the official advertising statement ("Member FDIC" or the FDIC symbol) on their home page unless subject to one of the specified exceptions. Further, each subsidiary page of an on-line system that contains an advertisement should display the official advertising statement unless subject to one of the specified exceptions.[82]

***Intellectual Property: Patent Law***. Historically, property rights "have not attached to the infrastructure of exchange." In other words, nobody owned the system of making payments by writing, presenting, and clearing paper checks or the concepts of paying and selling by means of a payment card.

[80] *Id.* §1681b(a)(3).

[81] CheckFree was concerned with its customers' creditworthiness because under ACH rules, an ACH debit from an account was reversible for a period of time. Under its processes, CheckFree initiated the credit side of a bill payment transaction in advance of the due date but did not electronically debit the consumer's deposit account until the actual due date. Kvalheim v. CheckFree Corp., No. CIV. A. 99-0135-RV-C, 2000 WL 209058 at *3 (S.D. Ala. Feb. 17, 2000).

[82] FFIEC Financial Services Guidance, *supra* note 18 at 6-7.

With the advent of electronic commerce, a large number of patent applications have been filed for systems related to electronic commerce and a large number of very broad electronic commerce patents have been granted.[83]

In the recent past, CheckFree has claimed the patent for an entire system, "a system for use by a service provider to pay bills rendered to a consumer by billing entities."[84] Patents have also been granted in recent years to OnLine Resources & Communications, Inc. and Visa in connection with bill payment systems.[85] When a financial institution proposes to offer EBPP services, the intellectual property status of any information technology that it proposes to implement should be discussed with legal counsel

***Privacy.*** Financial institutions are subject to federal and state laws governing financial privacy.[86] The Right to Financial Privacy Act restricts government access to information in a financial institution's records.[87] Some state privacy laws may have broader coverage than this; specifically, some state laws cover disclosures to any person (not just the government) and have broad definitions of financial records.[88] The Electronic Communications Privacy Act generally prohibits any person or entity from divulging the contents of an electronic communication while it is in transmission or in electronic

---

[83] For a thorough discussion of intellectual property issues in relation to electronic payment systems, see Robert D. Fram, et al., *Altered States: Electronic Commerce and Owning the Means of Value Exchange*, 1999 Stan. Tech. L. Rev. 2, ¶¶ 114 – 146 (1999), at http://stlr.stanford.edu/STLR/Articles/99_STLR_2. *See also* John W. Bagby, *Business Method Patent Proliferation: Convergence of Transactional Analytics and Technical Scientifics*, 56 BUS. LAW 423 (2000).

[84] Fram, *supra* note 83, ¶122.

[85] *Id.*¶¶ 133-146.

[86] *See, e.g.,*, THE REPORT OF THE CONSUMER ELECTRONIC PAYMENTS TASK FORCE 24-29 (Apr. 1998), *available at* http://www.occ.treas.gov/emoney/ceptfrpt.pdf (hereinafter TASK FORCE REPORT). This Task Force was established by Secretary of the Treasury Robert E. Rubin in 1996. Its mission was to identify consumer issues raised by emerging electronic money technologies and explore the extent to which innovative responses are being developed that are consistent with the needs of this developing market. *See also* Muller, *supra* note 17 at 419-422.

[87] Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1994 & Supp. V 1999).

[88] *See* TASK FORCE REPORT, *supra* note 86, at 28 & n. 93. *See also* Muller, supra note 17 at 420-421.

storage.[89] The EFTA and Reg E require financial institutions to disclose to consumers the circumstances in the institution's ordinary course of business under which it will disclose information about the consumer's account to third parties.[90] The Gramm-Leach-Bliley Act prohibits a financial institution from disclosing any nonpublic personal information to a non-affiliated third party prior to providing notice of its privacy policies to the consumer[91] Financial institutions are required (subject to exceptions set out in the applicable regulations) to disclose their privacy policies at the time of establishing a customer relationship with a consumer and at least annually thereafter with respect to: (i) disclosing nonpublic personal information about both customers and former customers and (ii) protecting the nonpublic personal information of consumers.[92]

An institution's failure to honor its own stated privacy policy could constitute a deceptive practice prohibited by section 5 of the Federal Trade Commission Act[93] or under a state's "little FTC Act." Additionally, in some cases, the consumer might have remedies for breach of contract or negligent misrepresentation.[94]

---

[89] 18 U.S.C §§ 2510-2520 (1994 & Supp. V 1999).

[90] 15 U.S.C. § 1693c(a)(9) (1994 & Supp. V 1999); 12 C.F.R. § 205.7(9) (2001).

[91] 15 U.S.C. § 6802(a) (Supp. V 1999); 12 C.F.R. § 216 (2001).

[92] 15 U.S.C. §6803(a) (Supp. V 1999); 12 C.F.R. §§ 216.4-.5 (2001).

[93] 15 U.S.C. § 45(a)(1) (1994 & Supp. V 1999). The statute provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." The FTC is empowered by § 45(a)(2) to prevent various persons and entities (except banks, defined savings and loan institutions and defined Federal credit unions) from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce. Even though the FTC does not have enforcement authority with respect to banks, actions taken by the FTC can provide guidance to state authorities in making "unfair and deceptive" determinations under their state "little FTC Acts."

[94] *See* TASK FORCE REPORT, *supra* note 86, at 34-35 & n. 114.

***Regulation D***. Regulation D imposes withdrawal and transfer restrictions on passbook savings and money market deposit accounts (MMDA).[95] "[P]ayments to third parties initiated by a depositor electronically from a personal computer are included as a type of transfer subject to the six transaction limit imposed on passbook savings and MMDA accounts."[96]

***Uniform Commercial Code (U.C.C.)*.** If payments are made by the EBPP provider via a "check and list" or "laser check," state law provisions (specifically the U.C.C.) will probably govern the presentment and collection of that check.[97]

**REGULATORY GUIDANCE WITH RESPECT TO OFFERING EBPP SERVICES**

In recent years, federal regulatory authorities have attempted to identify and assist financial institutions in understanding and managing the risks involved with electronic and Internet banking activities. From a practical standpoint, this guidance is as important to the financial institutions as any law or regulation in that it defines what the federal examiners will be looking at in the examination process. Failure to comply with this guidance may cause regulatory concern that the financial institution is not adequately protecting itself against risks.[98]

GUIDANCE WITH RESPECT TO OUTSOURCING ARRANGEMENTS

[95] 12 C.F.R. § 204.2(d)(2) (2001).

[96] FFIEC Financial Services Guidance, *supra* note 18, at 4.

[97] *See* Article 4 of the U.C.C. which defines rules applicable to bank deposits and collections, U.C.C. §§ 4-101 to 4-407 (2001).

[98] *See generally* Douglas, *supra* note 27. Mr. Douglas sets forth an extensive summary of current regulatory guidance.

With respect to the outsourcing arrangements typically involved when a financial institution is providing EBPP services, federal regulators are concerned that the risk management measures commonly used by a financial institution (e.g. internal controls and procedures) are generally under the direct operational control of the EBPP provider, rather than the financial institution. The financial institution, however, "[b]ears the associated risk of financial loss, reputational damage, or other adverse consequences."[99] Recent guidance from the Federal Financial Institutions Examination Council (FFIEC) clearly states that the boards of directors and senior management of financial institutions are expected to oversee and manage outsourcing relations.[100] The FFIEC guidance clarifies that the financial institution should have an outsourcing process that includes the following: risk assessment; due diligence in selecting a provider; a written contract that outlines duties, obligations, and responsibilities; and ongoing oversight of the services being provided.[101] Additionally, when the services involve use of the Internet the financial institution must pay attention to maintaining secure systems, detecting intrusions, developing reporting systems, and verifying and authenticating customers. A senior bank counsel recently commented that:

> All transactions entail risks, but whether they are identified and how they are dealt with are issues that are directly related to the type and amount of due diligence put into a transaction. . . .[f]ollowing good due diligence techniques helps avoid the great personal

---

[99] Letter from Richard Spillenkothen, director, Board of Governors of the Federal Reserve System (SR 00-4 (SUP)) (Feb. 29, 2000), *available at* http://www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0004.htm.

[100] *See* Fed/ Fin. Insts. Examination Council, Guidance on Risk Management of Outsourced Technology Services (Nov. 28, 2000), *available at* http://www.ffiec.gov/exam/InfoBase/documents/02-ffi-risk_mang_outsourced_tech_services-001128.pdf (hereinafter FFIEC Risk Management Guidance).

[101] *Id.*

> and professional embarrassment that comes from being associated with a transaction that later blows up.[102]

According to the same writer, "[d]ue diligence is nothing more than the art of asking the appropriate questions at the proper time."[103] Among the areas of factual inquiry that should be considered by a financial institution in doing due diligence prior to entering into a contract are: determination of the vendor's reputation and experience (including the checking of references); thorough understanding of the product; understanding of who will actually perform the work; on-site visit at the EBPP provider's offices and operations center; review of the vendor's financial condition; review of the vendor's disaster recovery plan; and review of the vendor's internal procedures and controls.[104]

The review of a vendor's financial condition can be a somewhat tricky undertaking. It is necessary to ensure the quality and continuity of service and to assure that the vendor can back up his contractual promises and liabilities. If the financial institution determines that its preferred vendor is financially weak, the financial institution must assess the risks and make a reasoned judgment as to whether the vendor will be in business a year or five years from now. It must understand the operational and legal consequences should the vendor go bankrupt or out of business. If the vendor is financially weak, even finely crafted contract provisions may not provide the financial institution with much protection. A financial institution cannot collect a damage award if the vendor has no money or assets with which to pay it. A vendor cannot provide a contractually required level of service if it has no money to pay employees. If the vendor is experiencing financial difficulties and is providing a service that the financial institution's customers value, as a practical matter the financial institution may be forced to

---

[102] Antonio P. Salazar, *In a Global Marketplace, Caveat Emptor Means "Banker Beware,"* ABA BANK COMPLIANCE, Mar/Apr. 2001, at 14. The author and attorney, Antonio P. Salazar, is a Senior Vice President and Deputy General Counsel of Provident Bank of Maryland.

[103] *Id*. at 13.

invest capital or provide other assistance to keep the vendor in business until an acceptable substitute can be found. The basic question that must be answered is whether the risks of entering into a relationship with a financially weak vendor are worth the benefits that the financial institution thinks it will get from the introduction of a particular product.

Alternatively, if the financial institution does not want to assume the risks, it can attempt to identify a different vendor, build the product internally, or simply pass on offering the service at this time. A basic analysis that should be performed in making this judgment is to plan out how the financial institution will continue to offer the product or to terminate it if the vendor goes out of business. One prime question with respect to EBPP services is how would the financial institution handle getting the customer's electronically delivered bills (or bills that are mailed directly from the biller to the EBPP provider) redirected to the customer or to a substitute vendor should the original EBPP provider go out of business? Additionally, how would the financial institution handle pre-authorized recurring payments? Would the delivery of notice that the EBPP service is being terminated be sufficient to avoid problems with the customer? The financial institution officer responsible for making the decision to offer a new product must keep in mind that hindsight is 20/20; if problems with the vendor materialize, he may be asked to justify the thought process involved in getting into a business relationship with a financially weak vendor. This can be especially difficult if widespread customer dissatisfaction arises because of termination of the EBPP service.

In connection with this vendor review, a lawyer should be careful to question the idea that it is simple to substitute services and vendors, particularly in the EBPP arena. Contingency planning should be done to pin down exactly how an EBPP vendor could be replaced. In the new Internet world, "plug and chug" strategies for getting into new lines of business have appeared—these strategies are based upon the concept that a financial institution can instantly "plug" in a new service provided by an outsourcer and

---

[104] *Id.* at 15.

"chug" along by rolling it out instantly to consumers. The strategies contemplate changing vendors by simply unplugging the old vendor and plugging in a new vendor. While the strategies may sound forward thinking, actual implementation (e.g. unplugging and plugging in with a new vendor) is rarely as easy as a marketer makes it sound. It is not necessarily easy from an operational standpoint to terminate a contractual relationship and replace one vendor with another.

The key to the successful offering of an oursourced product is vendor selection. As recently noted by the FDIC "selection of a competent and qualified service provider is perhaps the most critical part of the outsourcing process. . . . [the goal is] selection of a viable service provider that meets the procurement needs and objectives of the financial institution."[105] Of course, the vendor selected should be rational, reasonable, competent, and know the business.

Another key to the successful offering of an outsourced product is execution of a contract between the financial institution and the EBPP provider that is reasonable and mutually beneficial. If the contract is too one-sided, it may be difficult to make the relationship work over an extended period of time. The vendor must be prepared to obligate itself to do what it tells the financial institution it will do. The financial institution, as with any contractual agreement, must recognize that the vendor is in business to make money and that the vendor will be out of business if it does not do so. The financial institution must also realize that a reasonable vendor will not take on uncontrollable or unlimited risk. As one commentator recently noted:

> [A] well-presented contract is the mark of a competent vendor. . . .[b]ecause banks, in most vendor situations, bear the bulk of the performance risk inherent in the transaction,

[105] FDIC, EFFECTIVE PRACTICES FOR SELECTING A SERVICE PROVIDER (2001), *available at* http://www.fdic.gov/regulations/information/btbulletins/brochure1.pdf..

be wary of vendors that provide contracts that are either so short that they fail to address important issues or so vague that they fail to clarify the parties' duties and responsibilities. A weak contract indicates that a vendor either lacks the sophistication necessary to appreciate the nuances of its business or lacks the interest or resources needed to build and maintain a strong foundation for the relationship.[106]

With respect to arranging for the outsourcing of EBPP services, regulatory guidance is available which is extremely useful in thinking about important protections and provisions that should be included in the vendor selection and contracting processes. The FDIC recently released three informational brochures that provide practical information on how to select EBPP providers, draft contract terms, and oversee multiple EBPP providers when outsourcing for technology services and products; they are not examination procedures or official guidance.[107]

The FRB has also described the types of provisions that should be specified in outsourcing contracts, subject to the proviso that the level of detail should be commensurate with the scope and risks of the outsourced activity.[108] In general terms, these include "all relevant terms, conditions, responsibilities and liabilities of both parties" with specific examples given.[109] Since it remains the financial institution's responsibility to make sure that the EBPP product offered under its name is in compliance with applicable laws and regulations, the contract should clearly designate the party responsible for the day-to-day work of complying with laws and regulations. With respect to ongoing

---

[106] Salazar, *supra* note 102, at 19-20.

[107] FDIC, *supra* note 105; FDIC, TOOLS TO MANAGE TECHNOLOGY PROVIDERS' PERFORMANCE RISK: SERVICE LEVEL AGREEMENTS (2001) [hereinafter FDIC, PERFORMANCE RISK]; AND FDIC, TECHNIQUES FOR MANAGING MULTIPLE SERVICE PROVIDERS (2001). These brochures, available at http://www.fdic.gov/regulations/information/btbulletins/technology.html, resulted from discussions between the FDIC, bankers and other experts and are intended to be a resource for community bankers.

[108] Letter from Richard Spillenkothen, *supra* note 99, at 3.

[109] *Id.*

oversight of EBPP services, the program should be formally included in the financial institution's compliance and audit program and the contract should evidence the vendor's consent to this. One practical problem that smaller financial institutions may have is dealing with the reluctance of vendors to agree to the type of on-site compliance/audit review that is typically done internally in connection with the financial institution's general operations.[110]

One of the brochures recently published by the FDIC advocates the use of Service Level Agreements (SLAs) as tools "to measure, monitor and control the operational and financial risks associated with outsourcing technology services."[111] The brochure further points out that "[e]ssential to this process is establishing realistic performance metrics and continuous problem tracking and resolution."[112] Ultimately, one must keep in mind that the SLA provisions are just words – if appropriately designed and reported/tracked they can be very helpful, if poorly conceived they can damage a relationship and be detrimental.[113]

ADDITIONAL REGULATORY GUIDANCE ON ELECTRONIC BANKING ACTIVITIES

---

[110] This author became aware of this issue during a June 20, 2001 ABA Regulatory Compliance conference presentation on EBPP. In response to a recommendation that financial institutions do regular compliance audits of the EBPP provider's operations, members of the audience indicated that community banks may not be able to get vendors to agree due to the possibility of disrupting their operations by multiple audits. The impression from the discussion was that the large financial institutions had the leverage to insist on compliance audits of the vendor's operations but that the smaller financial institutions might not.

[111] FDIC, PERFORMANCE RISK, *supra* note 107, at 4.

[112] *Id.*

[113] Examples of SLAs might include that: the vendor's system will be available for use 99.5% of the time; there will be no more than thirty minutes of consecutive down time or one hour of intermittent down time during any rolling seven day period; customer service phone calls will be answered within thirty seconds, 90% of the time. Regulatory compliance requirements can be embedded within the standards established--for example, one such SLA might require the vendor to resolve customer claims of errors within 45 days of receipt of error notification. Monthly charting and reporting of SLAs can enable the financial institution to closely track the service levels its customers are receiving. Standards defined within the SLAs should measure factors that are important to running an efficient and legally clean business. They should be defined with the expectation that they will be met each month and should not be conceived as impossible goals. See FDIC, PERFORMANCE RISK, *supra* note 107, app.2, for a sample SLA.

The following additional regulatory publications are generally applicable to electronic banking activities (including EBPP); they address the risks involved with offering such activities and advise on appropriate steps to take in managing them:

- FFIEC, *Guidance on Risk Management of Outsourced Technology Services* provides guidance on financial institution's management of risk arising from technology services supplied by outside firms.[114] It emphasizes that "the board of directors and senior management are responsible for understanding the risks associated with outsourcing arrangements for technology services and ensuring that effective risk management practices are in place."[115]

- FFIEC, *Guidance on Electronic Financial Services and Consumer Compliance* summarizes the principal federal consumer protection laws that address electronic financial services and provides guidance to financial institutions on designing compliance policies for the on-line environment.[116] The principal message from this document is that moving transactions on-line does not immunize them from regulation, and that the same general requirements and restrictions that apply to paper transactions will apply.

- FFIEC, *Information Systems Examination Handbook* is an interagency guide to assist regulatory examiners in examining information systems operating in financial institutions and independent

---

[114] FFIEC, Risk Management Guidance, *supra* note 100.

[115] *Id.*

[116] FFIEC, Financial Services Guidance, s*upra* note 18.

service bureaus. [117] It provides guidance for financial institutions with respect to technology outsourcing arrangements and the essential contractual elements to be contained in any outsourcing agreement.

- FFIEC, *Guidance on Authentication in an Electronic Banking Environment* provides guidance to financial institutions on the risk-management controls necessary to authenticate the identity of customers, both new and existing, in accessing electronic financial services. This guidance is intended to help financial institutions reduce fraud and promote the legal enforceability of their electronic agreements and transactions.[118]

- FRB SR 00-4(SUP), *Outsourcing of Information and Transaction Processing* reiterates and clarifies the FRB's expectations regarding the management of risks that may arise from the outsourcing of information and transaction processing activities by banking organizations.[119] This letter outlines certain terms that would normally be included in a contract between a bank and a service provider. The guidance generally applies to outsourced services rather than products purchased or licensed from technology vendors.

- FRB SR 98-9(SUP), *Assessment of Information Technology in the Risk-Focused Framework for the Supervision of Community Banks and Large Complex Banking Organizations* provides FRB examiners with guidance in evaluating the effectiveness of a financial institution's ability to manage

---

[117]FFIEC, FFIEC INFORMATION SYSTEMS EXAMINATION HANDBOOK (1996), *available at* http://www.fdic.gov/regulations/information/information.

[118] *See* FFIEC, Guidance on Authentication in an Electronic Banking Environment (Aug. 8, 2001), *available at* http://www.fdic.gov/news/news/financial/2001/fil0169a.html.

[119]Letter from Richard Spillenkothen, *supra* note 99.

the risks associated with information technology.[120] This supervisory letter highlights the critical dependence of the financial services industry upon information technology; it provides a basic framework and a common vocabulary to be used in the above-described evaluation.

- Federal Reserve Bank of New York, *Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks* is a circular provided to financial institutions in the Second Federal Reserve District.[121] A team from the Federal Reserve Bank of New York interviewed Second District financial institutions, service providers, consultants, lawyers, and academics and identified the key risks and prudent business practices developed by financial institutions to mitigate outsourcing risk; these were compiled as industry practices. The circular provides an overview of the issues/risks accompanying outsourcing of banking activities and a benchmark for internal efforts.

- FDIC FIL 68-99, *Risk Assessment Tools and Practices for Information System Security* attempts to provide financial institutions and examiners with background information and guidance on various risk assessment tools and practices related to information security and describes the steps for establishing a sound information security policy.[122] In doing so it emphasizes the three primary components of a sound information security program: prevention, detection and response.[123]

---

[120] Letter from Richard Spillenkothen, Director, Board of Governors of the Federal Reserve System, (SR 98-9 (SUP)) (Apr. 20, 1998), *available at* http://www.federalreserve.gov/FRBdocs/SRLETTERS/1998/SR9809.htm.

[121] FEDERAL RESERVE BANK OF NEW YORK, OUTSOURCING FINANCIAL SERVICES ACTIVITIES: INDUSTRY PRACTICES TO MITIGATE RISKS (Circular 11193) (1999), *available at* http://www.newyorkfed.org/bankinfo/circular/11193.html.

[122] Financial Institution Letter from James L. Sexton, director, FDIC (FIL-68-99), *available at* http://www.fdic.gov/news/news/financial/1999/fil9968.html.

[123] *Id.*

- FDIC, *Electronic Banking Safety and Soundness Examination Procedures* identifies EBBP as a level III electronic activity (which level is subject to the most thorough FDIC examination procedures) and defines essential elements of technology-related risk management programs.[124]

- *Comptroller's Handbook on Internet Banking* deals solely with Internet banking.[125] It provides guidance to bankers and examiners on identifying and controlling the risks associated with Internet banking activities. It categorizes the various types of Internet banking, discusses the varieties of risk confronting financial institutions in relation to their Internet banking activities, and sets forth a three step risk management process. This publication addresses in great detail internal control systems and in-house development versus outsourcing of Internet services.

[124] FDIC, ELECTRONIC BANKING SAFETY AND SOUNDNESS EXAMINATION PROCEDURES (1998), *available at* http://www.fdic.gov/regulations/information/electronic/elecbank.pdf.

[125] OCC, COMPTROLLER'S HANDBOOK ON INTERNET BANKING (1999), *available at* http://www.occ.treas.gov/handbook/intbank/pdf.

**Occasional Paper Series**

Why  Don’t Consumers Use Electronic Banking Products?
Towards a Theory of Obstacles, Incentives, and Opportunities
*Brian Mantel* EPS-2000-1

Legal Analysis of a Banking Industry Online Identity and Attribute Authentication Service for Consumers and Merchants: The Financial Services Technology Consortium’s FAST Initiative
*William Gram* EPS-2000-2

Who Pays for Credit Cards?
*Sujit Chakravorti and William R. Emmons* EPS-2001-1

A Study of the Interrelated Bilateral Transactions in Credit Card Networks
*Sujit Chakravorti and Alpa Shah* EPS-2001-2

Credit, Debit and ACH:
Consequences & Liabilities
A Comparison of the Differences in Consumer Liabilities
*Ann H. Spiotto* EPS-2001-3

Competition and Innovation in the Consumer e-Payments Market:
Considering the Demand, Supply, and Public Policy Issues
*Brian Mantel and Timothy McHugh* EPS-2001-4

Electronic Bill Payment and Presentment:  A Primer
*Ann H. Spiotto* EPS-2001-5