The John Marshall Law Review

Volume 29 | Issue 4 Article 12

Summer 1986

Privacy Implications of Consumer Credit Protection Laws, 19 J. Marshall L. Rev. 941 (1986)

Paul B. Rasor

PRIVACY IMPLICATIONS OF CONSUMER CREDIT PROTECTION LAWS

PAUL B. RASOR*

I. INTRODUCTION

One of the most important attributes of a right of privacy is the right to control information about oneself. Privacy issues naturally arise in the consumer credit process because this process is one of gathering and evaluating information about individuals. Consumer credit legislation such as the federal Consumer Credit Protection Act (CCPA)[1] has an impact on this process. The CCPA can be viewed as a statute designed primarily to regulate the flow of information in consumer credit transactions. Seen from this perspective, its privacy contours become more easily visible. This article maps out and evaluates some of the uncharted privacy topography of the CCPA.[2]

While several different privacy issues can be identified in the consumer credit process, this article will address only two.[3] The first

---

* Professor of Law, Washburn University School of Law. B. Mus., University of Michigan, 1968; J.D., University of Michigan, 1972. Much of the research for this article was originally undertaken for a chapter on financial privacy to be included in PRIVACY LAW AND PRACTICE, a three-volume treatise scheduled for publication in 1986 by Matthew Bender & Co., Inc., under the auspices of the Center for Information Technology and Privacy Law, The John Marshall Law School [hereinafter cited as PRIVACY TREATISE]. As a result, there are some unavoidable similarities between the text of this article and the treatise. To avoid footnote clutter, I have not specifically noted every instance where this occurs.

1. 15 U.S.C. §1601 (1982).

2. A few parts of the CCPA address consumer privacy directly, and these have been discussed repeatedly in the legal literature. The most obvious example is the Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681 (1982), which is Title VI of the CCPA, and in which privacy protection is an express and overriding concern. *See, e.g.*, Note, *Protecting Privacy in Credit Reporting*, 24 STAN. L. REV. 550 (1972). I do not propose to repeat that work here. Instead, I wish to address the hidden impacts of those CCPA provisions which were not intended to evoke privacy.

3. There are other privacy issues which can be identified in the consumer credit process. Disclosure is an example. One could evaluate the rules which limit the ability of institutions to share the information they accumulate. I have omitted discussion of this issue because the only CCPA provision which addresses it is the FCRA, and it does so directly. *See supra* note 2. For detailed treatment, see PRIVACY TREATISE, *supra* note *. Another important issue is government access. This issue is beyond the scope of this article. For further discussion, *see* PRIVACY TREATISE, *supra* note *; Rasor, *Controlling Government Access to Personal Financial Records*, 25 WASHBURN

is content: What information do institutions gather about consumers? The second is access: To what extent do the individuals about whom the information pertains have access to and control over that information? The CCPA affects both of these issues.

The legal issues cannot be grasped without some understanding of the underlying transactional processes. Accordingly, Part II of this article describes the main lines of routine information flow in the consumer credit industry. Parts III and IV discuss the impact of the CCPA on the two privacy issues identified above. Some final thoughts are offered in Part V.

II. Information Flows In The Consumer Credit Industry

The consumer credit process always involves at least two parties, the creditor and the potential borrower. Very often the process also involves third parties such as credit reporting agencies. Information flows constantly among these parties, although in individual cases the flow is concentrated at certain key points. In most cases, the key points are the application process and the billing process.[4]

The Application Process

All credit grantors attempt to evaluate the credit worthiness of their applicants. To do this they need information. This information is gathered right from the beginning of the credit relationship. Consumers themselves supply much of it in their credit applications. For the most part, the creditor is free to ask for any information it wants and then evaluate that information in any way it chooses.[5]

In the application, the creditor will typically ask the potential borrower to divulge identifying information as well as information pertaining to the borrower's employment, assets, and liabilities. Information about family members may also be requested. Even information about former family members may be requested if the applicant relies on income in the form of alimony or child support.[6] This

---

L.J. 417 (1986).

4. There are other points where information may flow more rapidly. One of these is the collection process. Here, however, the flow occurs on a case-by-case basis rather than on a wholesale level. *See* Privacy Treatise, *supra* note *.

5. The general rule on applications is: "Except as provided [below], a creditor may request any information in connection with an application." Federal Reserve Board Regulation B, 12 C.F.R. 202.5(b)(1) (1985) [hereinafter cited as Reg. B]. The rule on evaluation is: "Except as otherwise provided . . . , a creditor may consider any information obtained, so long as the information is not used to discriminate against an applicant on a prohibited basis." *Id.* at 202.6(a).

6. *See generally* the model application forms published in Appendix B to Reg. B, *supra* note 5. There are restrictions on the creditor's ability to gather information about spouses and former spouses. *Id.* at 202.5(c) and (d).

information helps the creditor in varying ways. The identifying information, for example, may include the applicant's social security number. This helps the creditor avoid confusion when additional information is sought from credit reporting agencies.[7] Employment information is useful not only because it reveals income, but because it suggests something about the applicant's stability. It also lets the creditor know where the applicant can be found. Location information is extremely helpful in the debt collection process, should that process ever be needed.[8] Financial information is gathered for obvious reasons. Because all this information serves a purpose in the creditor's world, revealing it is nearly always a condition of getting the loan.

In this sense, the inevitable loss of privacy involved in the application process can be said to be a voluntary trade-off for the privilege of receiving credit. But it has often been observed that "[c]redit is essential for the vast majority of Americans."[9] As a result, these disclosures are not really voluntary in any meaningful sense. The loss of privacy may be a trade-off, but it is also an unavoidable consequence of living in a credit-based economy.

The application form is rarely the end of the process. Creditors routinely verify and supplement the information contained in the application, typically through the use of credit reports. Developments in credit reporting technology have affected this process in significant ways. For example, nearly all credit bureau files are now fully automated. Creditors who are regular users of these files often have computer terminals, provided by the credit bureaus, which permit direct access to credit bureau files. The creditor's loan officer can electronically contact the credit bureau's computer and retrieve the customer's entire file, all without leaving the desk and without any human intervention at the credit bureau.[10]

It seems likely that technological developments will soon permit this system to work completely free of human interference. Many large creditors use computerized credit scoring systems to evaluate

---

7. "[C]redit bureaus find the Social Security number a helpful tool for verifying identity." Privacy Protection Study Comm'n, *Personal Privacy in an Information Society* 61 (1977) [hereinafter cited as *Privacy Commission Report*].

8. *See* D. CAPLOVITZ, CONSUMERS IN TROUBLE: A STUDY OF DEBTORS IN DEFAULT 177 et seq. (1974). The federal Fair Debt Collection Practices Act (FDCPA), 15 U.S.C. § 1692 (1982), now prohibits direct contact with the debtor's employer and most other third parties, and even direct contact with the debtor is restricted. *Id.* § 1692(c).

9. D. CAPLOVITZ, *supra* note 8, at 41.

10. Systems of this type are described in Thompson v. San Antonio Retail Merchants Ass'n, 682 F.2d 509 (5th Cir. 1982), and Lowry v. Credit Bureau, Inc., 444 F. Supp. 541 (N.D. Ga. 1978). *See also Privacy Commission Report*, *supra* note 7, at 63-4.

their credit application.[11] In these systems, credit worthiness is determined by weighing mathematically a group of personal characteristics which have been shown statistically to be reliable predictors of the likelihood of repayment. The creditor may treat the score that this process produces in different ways. In a single cut-off system, for instance, the applicant's score is simply compared to a predetermined cut-off level. If the score is above this level, the application is approved; if it is below, the application is denied. In two-stage systems, on the other hand, the score is compared to two predetermined levels. If the score is above the higher cut-off point, the application is granted; if it is below the lower cut-off point, it is denied. A score falling between the two points indicates that more information is needed. This additional information is normally obtained through a credit report. The new information is then factored into the original score, and a final credit decision is based on the resulting new score. In these cases, the creditor's computer presumably could be programmed to contact the credit bureau's computer on its own ("Hello Eniac? This is Hal . . . "), retrieve the appropriate file, add the new information to the consumer's application file, and rescore the application.

The privacy ramifications of this sort of system are obvious. As credit bureaus and credit grantors become more automated, information will be gathered more readily and shared more widely. In addition, the trend is toward nation-wide systems.[12] When these systems are in place, creditors, through their own computer terminals, will have access not only to local files, but also to files of credit bureaus and other record-keepers across the nation.

The Billing Process

In traditional closed-end installment transactions, the flow of information normally stops with the application process. After credit has been approved, the only contact the parties are likely to have is the debtor's monthly check.

In credit card and other open-end accounts, however, modern billing practices create additional information flows. The activity in

---

11. For detailed discussions of credit scoring systems, *see* PRIVACY TREATISE, *supra* note 1; Hsia, *Credit Scoring and the Equal Credit Opportunity Act*, 30 HASTINGS L.J. 371 (1978); Capon, *Credit Scoring Systems: A Critical Analysis*, 46 J. MARKETING 82 (1982).

12. A decade and a half ago, one noted authority observed that "[t]he trend is toward fully computerized credit bureau networks capable of maintaining an electronic file on every economically viable American." A. MILLER, THE ASSAULT ON PRIVACY 76 (1971). The trend has not changed. A single credit reporting service, TRW Credit Data, maintains computerized credit records on over 120 million United States consumers. *See Online Newsletter*, February, 1986, at 2.

these accounts varies from month to month, and information is furnished to the consumer with each monthly statement. To inform the consumer, creditors must gather and maintain detailed information about each account.

Descriptive billing procedures now used by many, perhaps most, major credit card issuers add to the information flow. Under these procedures, the merchant bank truncates credit card sales slips, and information about the transaction is routed electronically.[13] When this type of processing system is used, federal law now requires that the card issuer include on the monthly statement the name of the merchant and the city and state where each transaction took place, along with the date and the amount.[14] When the card issuer is also the merchant or a related person, as in the case of a department store card, the monthly statement must also include a brief identification of the property or services purchased.[15] This can be quite personal; listed items may include such things as "jewelry," "sporting goods," or "women's clothing." This information may help the consumer read and reconcile the monthly bill, but it also reveals a lot about his or her personal affairs.

It is worth noting that comparable cash transactions do not produce comparable information flows. No personal information is disclosed to the consumer or maintained by the merchant. The advent of machine-readable uniform product codes may produce cash register tapes which say things like "canned peaches," but in cash transactions the tapes are not identified with, nor are files maintained on, individual customers.

The billing process also contributes to the exchange of information between creditors and third parties such as credit reporting agencies. At the billing end of the credit cycle, however, the information flows in the other direction. Creditors routinely contribute information about their customers' accounts to credit bureaus. In fact, other than public records, these contributions constitute the main sources of information which go into credit bureau files. Large creditors with computer-based record-keeping systems simply supply their computer tapes each month, either to a central source to which automated credit bureaus have direct access, or to local credit bureaus directly.[16] The information is routed by coordinating customer ZIP codes with the ZIP code areas each local credit bureau

13. *See* N. PENNEY & D. BAKER, THE LAW OF ELECTRONIC FUND TRANSFER SYSTEMS 19.01[5] (1980).

14. Federal Reserve Board Regulation Z, 12 C.F.R. 226.8 (1985) [hereinafter cited as Reg. Z].

15. *Id.*

16. *Privacy Commission Report*, *supra* note 7 at 47-8.

serves.[17]

III. Impact On Information Gathering

Several provisions of the CCPA have an impact on the information gathering practices of the institutional players in the consumer credit game. Some of these provisions affect the content of the specific information which can be gathered; others affect the uses to which the information can be put. All affect the privacy of the consumers about whom the information pertains.

Rules on Discrimination

The Equal Credit Opportunity Act (ECOA)[18] is intended primarily to prevent discrimination in lending practices; it was never intended to be a privacy statute. Nevertheless, the ECOA has several privacy overtones, and a few of them relate to information-gathering practices.

The ECOA places very few restrictions on the types or amount of information a creditor may gather and evaluate.[19] This approach would normally be expected to encourage the flow of information about consumers. In at least one way, however, the ECOA restricts this normal information flow and mandates a certain degree of creditor ignorance. A creditor may not ask a credit applicant to disclose sex, race, color, religion, national origin, birth control practices, or child-bearing plans.[20] The anti-discrimination idea is that a creditor is unlikely to discriminate on the basis of a personal characteristic it does not even know exists. However, there is also a privacy benefit to this policy. This very personal information is kept out of the creditor's files, and, more importantly, out of the routine flow of information in the consumer credit industry.

The information-gathering policy in home mortgage transactions, on the other hand, takes back some of these privacy benefits. Here, the creditor not only may, but is required to, ask the applicant's race or national origin, sex, marital status, and age.[21] The purpose of this requirement is to monitor compliance with the ECOA. Enforcing agencies cannot detect patterns of discrimination unless they know who is or is not receiving credit, and the monitoring rules

17. *Id.* Even those few credit bureaus that are not yet fully automated can participate in this system. The credit bureau trade organization, Associated Credit Bureaus, Inc., has developed a microfiche service permitting unautomated bureaus access to the same information. *Id.*

18. 15 U.S.C. § 1691 (1982).

19. *See supra* note 5.

20. Reg. B., *supra* note 5, at 202.5(d) (3), (4), and (5).

21. *Id.* at 202.13.

provide the necessary information. While the anti-discrimination purpose is salutary, there is a privacy cost. The information will not only be stored by the creditor,[22] it will also be made available to the federal government and will doubtless become a part of some permanent file somewhere. There is an obvious tension here between the statute's anti-discrimination goals and the individual applicant's privacy interests.

There is some leavening in these monitoring provisions, however. The creditor is supposed to tell the applicant that the federal government is requesting the information only for monitoring purposes. And even though the creditor is required to ask about race and the like, the applicant is not required to answer.[23] It is not known how many applicants refuse to divulge this information. If the number is significant, presumably the government is getting a distorted picture of the creditor's lending practices, and the compliance data would seem to be less than completely useful. The 1985 amendments to the relevant federal regulations will no doubt remove some of the distortion inherent in voluntary monitoring. Creditors are now required to note the applicant's race or national origin and sex on the basis of visual observation or surname.[24] Again, there is a privacy trade-off.

Rules on Disclosure

Disclosure legislation such as the Truth in Lending Act (TILA)[25] is intended primarily to give consumers the transactional information necessary for intelligent credit shopping. Creditors must disclose a whole battery of specific information about credit costs and other contract terms to individual consumers in each transaction. These disclosures are of several types. Some, such as the initial disclosures required for open-end credit accounts, apply on a wholesale basis and set ground rules for the life of the account. Others, such as periodic statements in open-end accounts and most disclosures in closed-end transactions, reflect specific information relevant only to a particular transaction or series of transactions. In all cases, however, the purpose is to provide appropriate information to consumers so that they can "avoid the uninformed use of credit."[26]

---

22. Creditors are required to retain most records pertaining to the ECOA for at least 25 months. *Id.* at 202.12.

23. *Id.* at 202.13(c).

24. *Id.* at 202.13(b). The picture is further distorted by the fact that monitoring is restricted to home mortgage loans.

25. 15 U.S.C. § 1601 (1982).

26. *Id.* § 1601(a). Detailed discussion of the disclosure requirements of the TILA is beyond the scope of this article. *See generally* R. ROHNER, THE LAW OF TRUTH IN LENDING (1984).

The Electronic Fund Transfer Act (EFTA)[27] follows the same pattern for EFT accounts. Like the TILA, the EFTA requires financial institutions to disclose account information to consumers. The EFTA applies only to accounts in which transfers of funds are initiated through electronic means, but the disclosures parallel those required for open-end credit accounts. These include a set of initial disclosures of the general terms and conditions of the account, specific disclosures for individual transactions, and monthly or other periodic statements reflecting cumulative activity.[28]

These disclosure rules have important privacy implications. For example, the TILA requires most major credit card issuers to use the descriptive billing procedures described in part II. These procedures generate enormous quantities of information. This information becomes part of the creditor's permanent files, and it is available for government monitoring as well as dissemination to credit reporting agencies and other third parties.[29] The significant point is that legal rules which benefit the consumer by providing more information also affect the consumer's privacy by increasing the information which is available to participants in the consumer credit process. "As a consequence [of these rules], credit-card issuers must now capture and store more information on individual transactions than they would otherwise record."[30]

Similar problems exist under the EFTA. For example, the EFTA requires financial institutions to provide consumers with written documentation of all transfers of funds initiated at any electronic terminal.[31] This requirement applies equally to simple EFT transactions like cash withdrawals from automated teller machines and to more complex EFT transactions such as point of sale transfers.[32] As a result, banks and other EFT providers have had to develop the technology necessary to enable the terminals to generate and print the required documentation. Today, most terminals supply little cards or other pieces of paper after the customer has completed the transaction. The documentation must include several specific items, including the amount and date of the transfer, the type of transfer, the type of account involved (for example, "withdrawal from checking" or "transfer from savings to checking"), a code

27. 15 U.S.C. § 1693 (1982). The EFTA is Title IX of the CCPA.

28. For detailed treatment of the disclosure and other aspects of the EFTA, *see* N. PENNEY & D. BAKER, *supra* note 13.

29. TILA records must be kept at least two years, although regulatory agencies may require longer retention. All records are available for inspection by the appropriate regulatory agency. Reg. Z, *supra* note 14, at 226.25.

30. *Privacy Commission Report*, *supra* note 7, at 46.

31. 15 U.S.C. § 1693(d).

32. For a description of these and other EFT systems, *see* PRIVACY TREATISE, *supra* note 1.

which identifies the customer or the access device used, the location of the terminal, and the name of any third party to or from whom funds are transferred.[33] Many institutions provide additional information such as current account balances. It is worth noting that far more information is generated in EFT transactions than in comparable transactions in which the consumer pays for goods or services by check or cash.

The consumer benefit here is similar to that for credit card accounts. The consumer now has something resembling a receipt which will help when it comes time to balance the checkbook. The trade-off for this convenience is, as in the credit process, a diminishing sphere of privacy. The rule requiring documentation forces banks and other financial institutions to create records and information flows in many cases where none existed before. Current technology permits these records to be easily stored and retrieved.

Because the law requires much of this documentation to be provided on the spot, many EFT transactions raise another privacy implication. This grows out of the fact that EFT systems operate increasingly on-line and in real time.[34] This makes it possible to locate individuals whenever and wherever they conduct financial transactions. Even the trail of records produced in off-line systems makes it relatively easy to reconstruct the activities of most people.[35] However, in on-line systems, it will be possible for anyone who has access, including law enforcement agencies, not only to know where consumers *were* when they conducted particular transactions, but to know where they *are*.

Piecemeal documentation for individual EFT transactions is only part of the information flow; periodic statements add to the burden. For checking accounts which have EFT features, most financial institutions simply combine the required disclosures with the traditional monthly bank statement. The information required for periodic EFT statements is similar to that required for documentation at the terminals in individual transactions.[36] In the periodic statement, however, the information flow is increased because the information must be gathered and disclosed for every electronic transaction which took place during the month, not just for those that were initiated at electronic terminals. Again, while these disclosure rules help the consumer in some ways, their privacy costs should not be overlooked.

---

33. 15 U.S.C. § 1693(d) (a).

34. One study has predicted that by 1995, all banking transactions will be posed in real time. *See* Greguras, *EFT and Privacy*, 26 SECURITY MGMT. 24, 25 (1982) (citing a study by Electronic Banking, Inc., of Atlanta).

35. *See* A. MILLER, *supra* note 12, at 8.

36. The disclosure requirements are spelled out in 15 U.S.C. § 1693(d)(c).

IV. Impact On Consumer Access

Among the most important consumer privacy rights is the right of access to records. The consumer needs some way to discover the existence of records, to learn of disclosures which have been made, and to discover and correct errors. The CCPA has a few provisions which permit consumer access to certain financial institutions' records. Unlike the rules discussed in part III with respect to information gathering, however, the CCPA provisions on consumer access have, for the most part, a positive privacy effect. The main problem is that there are not enough of them, and those which do exist are remarkably weak.

Learning of Records

Before a consumer can obtain access to records maintained on him, he must know that the records exist. When the consumer has a direct relationship with an institution, the problem is easy. The consumer is likely to know whether he has a credit card or a bank account, and if he wants to see his records he knows where to start looking.

Records held by third-party institutions, however, are another matter. The individual consumer ordinarily has no direct contact with credit reporting agencies or credit card authorization services, for example, and he may not be aware of the detailed records these institutions keep. Business debtors and sophisticated consumers may know that their creditors routinely use credit reports, and curious credit card users or check writers may suspect that records exist when a skeptical merchant makes a phone call or consults a notebook before accepting payment. But not everyone is this aware, and there should be a place for laws requiring that record-keeping practices be made known.

With respect to consumer financial records that private institutions keep, there are few such laws. Only two parts of the CCPA address this problem, and then only in a limited fashion. First, the FCRA provides that when a potential creditor relies on information contained in a credit report either to deny credit or to increase the charge the creditor must disclose to the consumer the name and address of the reporting agency who issued the report.[37] In addition, the ECOA requires that a creditor provide the consumer with specific reasons for denial of credit or for any other adverse action.[38] If those reasons include a bad credit report, then this must be

37. 15 U.S.C. § 1681(m).
38. *Id.* § 1691(d).

disclosed.[39]

While these provisions are significant, they have serious shortcomings. The most important is that they apply only when the credit applicant is turned down or otherwise treated adversely. If credit is granted on the terms the applicant requests, the creditor is not required to disclose the fact that a credit report or other outside source of information was used in the decision-making process.[40]

Learning of Disclosures

Individual consumers rarely learn of the information sharing and disclosure practices described in Part II of this article. Statutes requiring that consumers be told about credit reports when adverse decisions are made solve only a small part of the problem. Absent a statute or a fiduciary relationship, it is unclear whether an institution is obligated to tell the consumer what disclosures it has made. While the bank-customer relationship may be considered fiduciary for some purposes,[41] in general the debtor-creditor relationship is not a fiduciary one. Moreover, there are few applicable statutes. The FCRA requires that credit reporting agencies disclose to the consumer, on request, the identity of anyone who has been furnished a credit report during the preceding six months.[42] To keep fully informed of all credit reports issued on him, a consumer would have to check with the credit bureau every six months. This is hardly feasible, and it is no substitute for a law which requires that consumers be notified of all disclosures made about them.

Credit reports are only part of the information picture, and other kinds of disclosures are harder to discover. As discussed above, many creditors routinely share their computer tapes with credit bureaus. In addition, credit card issuers routinely disclose information about their customers to independent card authorization services. Further, merchants disclose customer information to check-authorization services and check-guarantee services.[43] These so-

39. Reg. B., *supra* note 5, at Appendix C.

40. A different rule applies if a so-called investigative consumer report was used. The institution must tell the consumer that it has requested the report and that the consumer is entitled to further information about it. 15 U.S.C. § 1681(d)(a). This rule will not have much impact on consumer awareness in the credit process, however, since in industry practice investigative reports are used primarily by insurance companies, and rarely by creditors. For a general discussion of investigative reports, *see* PRIVACY TREATISE *supra* note *.

41. *See generally* Symons, *The Bank-Customer Relation: Part I—The Relevance of Contract Doctrine*, 100 BANKING L.J. 220 (1983); and Symons, *The Bank-Customer Relation: Part II—The Judicial Decision*, 100 BANKING L.J. 325 (1983).

42. 15 U.S.C. § 1681(g)(a)(3).

43. For a discussion of these practices, *see* PRIVACY TREATISE *supra* note *.

called bad check lists have been held to be within the FCRA,[44] and as a result customers can exercise their rights under the FCRA and discover disclosures which may have been made. The FCRA probably covers independent card authorization services as well.[45] But having statutory rights does not help if the customer does not know that the record exists, and this is not likely.[46] In fact, with the sole exception of adverse decisions under the FCRA and the ECOA, record-keepers are not generally required to reveal disclosures which have been made to others. This is one of the major weaknesses of the law of financial privacy.

There has been some recent progress in this area. The EFTA requires that financial institutions disclose to their customers the circumstances under which they will "in the ordinary course of business disclose information concerning the consumer's account to third persons."[47] While this is not quite a full disclosure rule, it is a step in the right direction. This provision is limited, however, to consumer EFT accounts. No comparable provisions exist under the TILA or elsewhere for open-end credit accounts or non-EFT depository accounts.

TRW Credit Data, the nation's largest consumer credit data holder, has taken a more interesting private step toward full access and disclosure. For a fee of $30 a year, consumers will receive a password which will permit direct, on-line access to their own credit files. In addition, for the same fee, consumers will be notified whenever anyone receives a credit report on them.[48] While this service may benefit only those consumers who have access to a personal computer and who would think to look in TRW's files in the first place, it is a start.

Access to Records

Access to financial records which are maintained about individuals is an important attribute of privacy. As the Privacy Commission has noted, "[f]or the individual, necessary fairness protections

---

44. Greenway v. Information Dynamics, Ltd., 399 F. Supp. 1092 (D. Ariz. 1974), *aff'd per curiam*, 524 F.2d 1145 (9th Cir. 1975); Peasley v. Telecheck of Kansas, Inc., 6 Kan. App. 2d 990, 637 P.2d 437 (1981).

45. The FCRA specifically excludes "in-house" authorizations, 15 U.S.C. § 1681(a)(d)(3)(B), and the implication is that independent services are covered. The F.T.C. has noted the distinction between in-house and independent authorization services. *See* F.T.C., *Compliance with the Fair Credit Reporting Act* 1973 & rev. 1977, 1979, *reprinted in* 5 CCH Cons. Cred. Guide 11,301 et seq.

46. The Privacy Commission noted that "[i]t is doubtful . . . that many of the [credit] card holders on whom an independent service reports derogatory information . . . know that it exists." *Privacy Commission Report*, *supra* note 7, at 45.

47. 15 U.S.C. § 1693(c)(a)(9).

48. *Online Newsletter*, *supra* note 12, at 2.

include a right of access to records about himself for the purpose of reviewing, copying, and correcting or amending them as necessary . . . ."[49] Unfortunately, the law regarding customer access does not measure up to this lofty standard.

With respect to primary institutions such as creditors and banks, there is no law which provides for customer access to financial records. The disclosures required to be made in monthly statements for open-end credit accounts and EFT accounts provide some information, as do the disclosures the ECOA requires for adverse decisions. But these rules do not adequately substitute for a right of access. The individual consumer is not entitled to see a credit grantor's files to learn the actual items of information behind an adverse credit decision or even to learn generally what information is kept on him. And no law gives a customer the right to see information a depository institution maintains or which may have been used as the basis for an adverse depository decision. The Privacy Commission recommended that creditor and depository institution files be opened up to consumers,[50] but no law on this subject has been enacted.

With respect to third-party institutions such as credit reporting agencies, the only federal law specifically permitting consumer access is the FCRA.[51] The rights provided here are significant, yet they suffer from many weaknesses. Perhaps the most significant is that the agency must disclose only the "nature and substance"[52] of the information in its files. This standard means that agencies need not provide customers with copies of their credit reports or other information in their files nor, indeed, even let the consumer see any of the file information.[53] This standard has been widely criticized, and even the credit bureau trade association has recognized that a disclosure limited to the "nature and substance" of a file can cause anxiety and uncertainty for the individual.[54] Many credit bureaus go beyond the minimum statutory requirement and provide copies of credit reports or other information to the consumers, as the described TRW service indicates. But these extra disclosures are purely voluntary. The Privacy Commission recommended that the law be changed in a way that would require credit reporting agencies to allow an individual to see and copy any recorded information about that individual.[55] This change has never been made.

---

49. *Privacy Commission Report*, *supra* note 7, at 17-18.
50. *See id.* at 77, 109.
51. 15 U.S.C. § 1681(g). For a general discussion of this provision, *see* PRIVACY TREATISE *supra* note *.
52. 15 U.S.C. § 1681(g)(a).
53. *See* Equifax Services, Inc. v. Lamb, 621 S.W.2d 28 (Ky. App. 1981).
54. *Privacy Commission Report*, *supra* note 7, at 80.
55. *Id.* at 81.

The "nature and substance" standard, while weak, is not worthless. In many cases, seeing an actual credit report might do little good for the average consumer since most reports are made in a standardized format consisting mainly of coded references only trained personnel can decipher.[56] The FCRA even helps here by requiring that the reporting agency "provide trained personnel to explain to the consumer any information furnished to him."[57] In addition, the individual may bring along "one other person of his choosing"[58] when he visits the agency. This person, of course, could be a lawyer or other confidant who is not bashful about asking pertinent questions. Finally, even within the limits of the "nature and substance" standard, the agency must cooperate. Credit reporting agencies have been held liable for punitive damages for systematically blocking the consumer's access and for providing only incomplete synopses of the consumer's record.[59]

Correcting Inaccuracies

The final aspect of consumer access is the right to challenge and correct inaccuracies which appear in institutional files containing personal financial information. The CCPA addresses this issue in three separate places. As with other provisions on access, these provisions offer some protection for consumer privacy interests; the trouble is that they do not go far enough.

Credit Reporting Agency Files

The FCRA establishes procedures to be followed in cases in which the consumer, having discovered the "nature and substance" of the information in his file, disputes its accuracy. The first step is reinvestigation, which the agency is required to undertake.[60] The statute does not say what sort of reinvestigation is required. At the very least, the agency should verify the disputed information with its original source. If the dispute concerns a credit account, for example, a call to the creditor may clarify the problem. Also, if the consumer provides independent sources to support his version of the

---

56. Form "Crediscope 2000" was devised in 1977 by Associated Credit Bureaus, Inc., the trade association, to standardize credit reporting practices. Information flyers describing the format are available from ACB and from most credit bureaus. For an example of the types of problems which can be generated by this format, *see* Koropoulos v. Credit Bureau, Inc., 734 F.2d 37 (D.C. Cir. 1984).

57. 15 U.S.C. § 1681(h)(c).

58. *Id.* § 1681(h)(d).

59. *See, e.g.*, Millstone v. O'Hanlon Reports, Inc., 383 F. Supp. 269 (E.D. Mo. 1974), *aff'd* 528 F.2d 829 (8th Cir. 1976).

60. 15 U.S.C. § 1681(i)(a). The agency need not reinvestigate, however, if "it has reasonable grounds to believe that the dispute . . . is frivolous or irrelevant." *Id.*

story, the agency would be wise to contact them as well. More than one reinvestigation may be necessary.[61]

If reinvestigation does not resolve the dispute, the consumer has the right to file with the reporting agency a statement of his own explaining the nature of the dispute.[62] While this helps, there are two limitations which make this procedure less than completely satisfactory. First, there is no requirement that the agency reveal the consumer's right to do this,[63] although many agencies do. Second, the agency may limit the statement to one hundred words if it provides the consumer with help in writing it.[64] If the consumer does file such a statement, the agency must clearly note in any subsequent report that the information is disputed.[65] Along with the report it must also provide either the consumer's statement or "a clear and accurate codification or summary thereof."[66] The agency is relieved of these duties, however, if it has reasonable grounds to believe that the statement is frivolous or irrelevant.[67] Otherwise, if the consumer has filed a statement, it is a violation of the FCRA for the agency to fail to send it.[68]

Finally, in any case involving disputed accuracy, the agency is required, at the consumer's request, to notify any person who received a report containing the disputed information within the previous six months. The notice must state that the item has been deleted, if that is the case, or include the consumer's statement of the dispute. The agency is required to tell the consumer of his right to make this request.[69] Whether these notices cause many credit grantors to reevaluate adverse decisions is not known; but this procedure, as limp as it is, does contribute to the goal of accuracy and fairness in financial record keeping.

Billing Disputes

Billing practices used in open-end credit accounts were described above. Errors may appear, or consumers may dispute charges or other items which appear on the monthly statement. The Fair Credit Billing Act (FCBA)[70] provides a mechanism for dealing with these errors and misunderstandings. While it would serve no

61. Dynes v. TRW Credit Data, 652 F.2d 35 (9th Cir. 1981).
62. 15 U.S.C. § 1681(i)(b).
63. Roseman v. Retail Credit Co., 428 F. Supp. 643 (E.D. Pa. 1977).
64. 15 U.S.C. § 1681(i)(b).
65. *Id.* § 1681(i)(c).
66. *Id.*
67. *Id.* No standards are provided for determining frivolity or irrelevance.
68. Alexander v. Moore & Associates, 553 F. Supp. 948 (D. Haw. 1982).
69. 15 U.S.C. § 1681(i)(d).
70. *Id.* § 1666 (1982). The FCBA is part of the Truth in Lending Act.

purpose to describe the mechanics of these provisions,[71] it should be noted that the FCBA has several important privacy features, mostly positive. Indeed, the very existence of a statutory right to challenge the accuracy of information contained in the creditor's file, at least in so far as it appears on a billing statement, is itself an important privacy development. Under the FCBA, the creditor is required to provide the consumer with a summary of these rights in the initial disclosure statement,[72] and every monthly statement must contain an address the consumer can use to give the creditor notice of any alleged error.[73]

Another important privacy feature appears during the time any billing dispute is pending. The consumer has the right to withhold payment of the disputed portion of the bill, and the creditor may not make or threaten to make an adverse credit report because of the consumer's failure to pay this portion.[74] This protects against the accumulation of extraneous and possibly erroneous information in the consumer's files. This is an important provision apart from its privacy benefit, since even a threat of an adverse credit report could intimidate the consumer into paying. This would seriously dilute the right to withhold payment. Further, this right applies in situations in which the consumer's real dispute is with the merchant and the consumer is exercising his right to assert defenses against the card issuer by withholding payment.[75] Even here, the card issuer may not report the disputed amount as delinquent until the dispute is settled or judgment is rendered.[76]

The concern over adverse credit reports is so great that a special rule was included in the FCBA to cover cases in which the consumer is unsatisfied with the resolution of the dispute. If the consumer gives a second notice that an error still exists or that the same item is still in dispute, the creditor may not report the account as delinquent unless it also reports it as being in dispute. If the creditor does this, it must also give the consumer written notice of the names and addresses of everyone to whom the creditor makes this report, and it must follow up by reporting any subsequent resolution to the same persons.[77] The creditor need not, however, reinvestigate the error following a second notice of the same dispute.

---

71. Detailed treatment can be found in R. ROHNER, THE LAW OF TRUTH IN LENDING ch. 9 (1984).

72. Reg. Z, *supra* note 14, at 226.6(d) and 226.9(a). This disclosure must be repeated at least annually. *Id.*

73. *Id.* at 226.7(k).

74. *Id.* at 226.13(d)(2). *See* Saunders v. Ameritrust of Cincinnati, 587 F. Supp. 896 (S.D. Ohio 1984).

75. *See* 15 U.S.C. § 1666(i).

76. Reg. Z. *supra* note 14, at 226.12(c)(2).

77. *Id.* 226.13(g).

Errors in EFT Accounts

The EFTA contains error resolution procedures which apply to errors or disputes in periodic statements sent with EFT accounts.[78] The procedures and the privacy impacts are similar to those for open-end accounts under the FCBA, and no separate discussion is required.[79] It is again worth noting the limitations, however. EFT accounts are normally deposit accounts to which certain EFT privileges apply. No dispute resolution procedures exist for ordinary, non-EFT deposit accounts, or for closed-end credit transactions.[80]

V. Conclusion

Consumer credit protection laws like the CCPA constitute a mixed privacy bag. In many respects, as in the access and error resolution procedures, the CCPA has added significantly to the privacy rights of consumers. But in other important ways, the overriding concern for disclosure increases the privacy risks to individual consumers by increasing the flow of information in the consumer credit process. These privacy implications are often hidden. In most cases, consumers are probably unaware of the extent to which personal information about them is passed around in the industry. While much, probably most, of this information flow is unavoidable, there is need for a mechanism which would make consumers aware of the privacy costs. Perhaps the disclosure laws need to disclose this as well.

78. 15 U.S.C. at § 1693(f).

79. For a detailed discussion, *see* N. Penney & D. Baker, *supra* note 13, at 12.02.

80. *See* Jacobs v. Marine Midland Bank, 124 Misc. 2d 162, 475 N.Y.S.2d 1003 (Sup. Ct. 1984).