STATE OF CALIFORNIA
DEPARTMENT OF CONSUMER AFFAIRS
STATE AND CONSUMER SERVICES AGENCY • GOVERNOR EDMUND G. BROWN JR.
Legal Affairs
1625 North Market Blvd., Suite S 309, Sacramento, CA 95834
www.dca.ca.gov

Legal Guide CR-6

CONSUMER RIGHTS IN ELECTRONIC FUND TRANSFERS

December 2008

- You deposit a check, withdraw cash or transfer funds between bank accounts at an automated teller machine (ATM).

- You purchase groceries and pay at the grocery store's point-of-sale (POS) terminal using your debit card and personal identification number.

- You authorize the telephone company to automatically withdraw the amount of your phone bill from your checking account each month by means of a "preauthorized electronic fund transfer."

These all are examples of electronic fund transfers ("EFTs"). These kinds of transfers have become so accepted and common that you probably never think about them. Nonetheless, there is a comprehensive legal framework behind every electronic fund transfer, and this framework is a major reason that EFTs have flourished.

The federal Electronic Fund Transfer Act[1] and Federal Reserve Regulation E[2] provide a "Consumer Bill of Rights" for electronic fund transfers. These laws set forth the basic rights, financial liabilities, and obligations of both consumers and card issuers (typically banks or other financial institutions) with respect to electronic transfers of funds. They contain numerous consumer protections[3] which are not subject to waiver or modification by the consumer.[4] Their objective is "the protection of individual consumers engaging in electronic fund transfers."[5] They generally meet the needs of both financial institutions and consumers.

This Legal Guide provides an overview of the major consumer protections provided by the federal EFT Act and Regulation E. Detailed coverage of the statute, regulations and court decisions that interpret them is available in other published sources.[6]

Secret Code

The first consumer protection provided by the EFT Act and Regulation E is that the financial institution that issues the card or "access device" must also provide a way to identify the consumer to whom the access device is issued.[7] Typically, the access device is a card embedded with a magnetic strip and embossed with an account number. The issuer typically issues to the consumer, or allows the consumer to chose, a secret code number which the consumer must punch into an electronic terminal in order to use the access device. Only with the access device and secret code can the consumer obtain access to his or her account to withdraw cash or make

other transfers at an electronic terminal.[8]

Other systems of customer identification also are permitted, such as the consumer's signature, fingerprint or photo.

Limits on Liability

The next protection provided by the Federal EFT Act and Regulation E is a limit on the amount of money that a consumer may lose in the event of an unauthorized use of the consumer's access device and secret code.

No Liability

If you lose your EFT card, or if it is stolen from you, you may avoid *any* losses by immediately calling the bank or other institution that issued the card. If the card has not been used before you give notice, you will lose nothing.[9] The financial institution will simply switch off your account and issue you a new EFT card with a new secret code. You can avoid loss in this way even if you were careless in causing the card to be lost.[10]

$50 Liability Limit

If the card *has* been used to draw money from your account before you notify the financial institution, your loss is limited to $50, *provided* that you give notice to the financial institution within *two business days* after you learn of the loss or theft of the card. Your card issuer *cannot* charge you for *any* loss *unless* it has previously given you –

- a written summary of your liability for unauthorized electronic fund transfers,
- the telephone number and address of the person or office that you must notify if you believe that an unauthorized transfer has been made, and
- the days when the financial institution is open for business, called "business days."[11]

$500 Liability Limit

If you do *not* notify the financial institution within two business days of the loss or theft, your risk of loss due to an unauthorized transfer will increase. You will be liable for:

- Up to $50 of loss that occurs during the first two business days, *plus*
- Any loss that occurs after the first two business days and until you actually give the financial institution notice of the loss or theft. However, you are liable for such a loss only to the extent that the loss would not have occurred if you had given notice during the two business days. Your loss also is subject also to an overall upper limit of $500. The financial institution must establish that the loss would not have occurred if you had notified it within the two business days.[12]

Remember that your EFT card ordinarily cannot be used by someone else unless that person knows your secret code. So, if you have not written the code on the card or in your wallet, you

ordinarily will lose nothing if you lose your wallet or card. Nonetheless, you should notify the financial institution that the card has been stolen and ask it to issue you a new card with a new account number and a new secret code.

On the other hand, if the thief has your card *and* your secret code, and you neglect to give notice to the card issuer within *two* business days after you have learned of the loss or theft, your liability for use of the card by someone else will *increase* to a maximum of $500 – but only to the extent that giving a notice within two business days would have avoided that loss.[13]

No Liability Limit

If you are very careless, there is yet another and higher level of possible loss to you – *unlimited* loss. Unlimited loss to you can occur if –

- the periodic statement that you receive from the card issuer reflects an unauthorized transfer of money from your account, *and*

- you don't report the unauthorized transfer to the card issuer within 60 days after it has mailed you the statement, *and*

- the loss could have been avoided if you *had* given it timely notice. The card issuer must establish that the loss would not have occurred if you had notified it within the 60-day period.[14]

Therefore, it's important that you review your monthly statements when you receive them, and assure yourself that no one is stealing money from your account. If you see anything wrong, it's essential that you contact the card issuer immediately. Otherwise, you can lose the protections of the EFT Act and Regulation E.

Giving Notice of Loss

You can give the card issuer notice of an unauthorized fund transfer in person, by telephone, or in writing.[15]

The law considers that written notice to the card issuer has been given when you deposit the notice in the mail, or when you deliver it for transmission to the issuer by "any other usual means."[16] Notice is effective without regard to whether the card issuer or any employee or agent of the card issuer has actually received it.[17] Notice is also considered given when a card issuer becomes aware of circumstances which would lead to a reasonable belief that an unauthorized transfer has taken place.[18]

If you give notice of the loss or theft by telephone or in person, the card issuer may require you to provide written confirmation of the notice within ten business days of the oral notice. This requirement only applies if, at the time that you give the oral notice, the card issuer specifically requests that you confirm your oral notice in writing, and also gives you the address to which your written confirmation must be sent.[19] Your failure to provide the card issuer with the requested written notice within the specified time may affect certain rights that you otherwise would have during the error resolution process. (Those rights are discussed on page 4.)

If you are unable to give the card issuer notice within the time limits described above, and have a very good reason, the issuer should extend the time limits to a "reasonable" period.[20]

Fraud and Robbery

If you give your EFT card and secret code to a relative or friend to withdraw a certain amount, and the person *drains* your bank account, are you protected? The answer is *no*.[21] Since it is *you* who have compromised the security of the system, the loss is yours, not the bank's. It's like signing checks in blank and giving them to someone else.

There is some protection, however. If you have given your access device and secret code to someone, and now suspect that that person may misuse it, you can terminate that person's ability to use the access device by contacting your financial institution and requesting that the authority be terminated.[22]

Also, if you are forced to initiate a transfer at an ATM, or if a person initiating a transfer obtained your access device from you through fraud or robbery, you are protected.[23] It is important, however, that you notify the card issuer of the loss as soon as you become aware of it, so the thief gets away with as little as possible.

Limits on Withdrawals

Another protective device for consumers is a limit on the amount of money that can be withdrawn from your account (whether by you or anyone) during any given period.[24] For example, most financial institutions limit cash withdrawals to $200 or $300 per day. This helps to limit aggregate loss in the event of loss or theft of the card by enabling you to report a loss or theft before much damage is done.

Unsolicited Cards Prohibited

Another protection for consumers is the EFT Act's prohibition against issuance of a debit card or other EFT access device without the card-holder's consent. The unsolicited distribution of access cards is generally prohibited.[25]

A card issuer can send an access device to an account owner or potential account owner only if the access device is requested, or is supplied as a renewal or replacement of an access device that was previously issued and accepted. A card issuer can send an *unsolicited* access device to a consumer only if it is not "validated" (that is, the issuer has not yet performed all of the procedures that would enable a consumer to initiate an EFT using the device).[26] The consumer is not liable for an unauthorized transfer that results from a violation of these rules.[27]

Compulsory Use of EFT Prohibited

No credit transaction or employment or government benefit may be conditioned on the payment or receipt of funds electronically.[28] A decision to authorize receipt or payment of money by electronic means must be yours alone – an important consumer benefit. However, a creditor may offer reduced interest rates if the borrower voluntarily agrees to pay electronically, but a non-electronic payment option must be provided.[29] Also, an employer may require direct deposit of salary by electronic means if employees are allowed to choose the institution that will

receive the direct deposit.[30]

Error Resolution Process

A highly important consumer protection is the EFT Act's comprehensive and detailed error resolution process.[31]

When notifying a financial institution of an error – such as a transfer of money that you did not authorize – you should call or write the financial institution that issued the EFT card or other access device, and provide the following information:

- Your name
- The number of the affected account
- Why you believe there is an error
- What kind of error it is
- The dollar amount involved
- The date of the unauthorized transfer or other error.[32]

If the error appears in your periodic statement, you must give notice to your financial institution within 60 days after it mailed the periodic statement to you.[33] If you first reported the error to the financial institution in person or by telephone, the financial institution may require that you confirm this information in *writing* within *ten* business days. If the institution requests that you do this, it must provide you the address where the written confirmation must be sent at the time that you give your oral notice.[34]

If a consumer notifies a financial institution of an error, the institution must promptly investigate the matter and determine, within 10 business days, whether an error occurred.[35]

If the investigation *takes more than ten days*, the amount of the unauthorized transfer must be *provisionally credited* to your account pending the completion of the investigation. The institution must inform you of the amount and date of the provisional crediting within two business days after the crediting, and must give you full use of those funds during the investigation.[36] If the asserted error constitutes an unauthorized transfer, and the financial institution has a reasonable basis for believing that an unauthorized transfer has occurred, the financial institution may withhold a maximum of $50 from the amount credited to your account, pending completion of its investigation. The financial institution may withhold the $50 only if it has given you the required notice of your potential liability for unauthorized transfers.[37]

The financial institution is not required to provisionally credit your account if it has requested from you, but does not timely receive, your written confirmation of your oral notice of the error.[38]

Where the financial institution's investigation of the error takes more than ten days and the amount of the unauthorized transfer has been credited, the investigation nevertheless must be completed within *45* days.[39] If the error involves a point-of-sale (POS) transfer, the 45-day investigation period is increased to *90* days.[40]

The financial institution must notify you of the results of the investigation within three business days after completing it. If, after its investigation of the reported error, the financial

institution determines that an error *did* occur, it must correct the error within one business day of that determination. [41]

If the financial institution determines, after its investigation, that the reported error did *not* occur, or that an error occurred in a different manner or amount than you asserted, it must provide you with a written explanation of its findings, including a notice of your right to request the documents on which it relied in making its determination.[42] The financial institution also must notify you that it is taking the provisionally credited amount out of your account, the amount that it will take out of your account, and the date that will happen. The financial institution also must notify you that it will nevertheless honor checks and preauthorized transfers to third parties from your account, without charge, for five business days following the notice.[43]

Information Disclosures

One of the EFT Act's most important protective measures for consumers is the information disclosures that it requires banks and other card issuers to provide to their customers.

Disclosures of relevant information are required to be provided to the customer (a) before the first transaction on the account,[44] (b) any time that a fund transfer is made at an ATM or other electronic terminal,[45] and (c) periodically (typically every month).[46]

The EFT Act and Regulation E specify exactly what information these disclosures must provide:

- Initial disclosures are required to be made when the consumer contracts for services or before the first electronic transaction. They include, for example, a summary of the consumer's liability for unauthorized transfers, what fund transfer services are provided, and fees.[47]

- At the time of an electronic transfer initiated at an electronic terminal, the financial institution must provide or make available a receipt that identifies the customer's account, the nature and amount of the transfer, the date, and the location of the terminal.[48] That receipt is evidence that the transfer was made and can be used for that purpose in judicial proceedings.[49]

- If the electronic terminal is owned and operated by someone other than your financial institution, the terminal owner may charge you for using the terminal, but only if the amount of the charge is disclosed on the receipt and displayed on or at the terminal.[50]

- A financial institution also must provide a periodic statement for each monthly cycle in which an electronic transfer has occurred. The statement must include specific information about your account and its activity.[51] If there has been no electronic transfer during a monthly cycle, no statement is required, except that a statement must be provided quarterly in any event.[52]

Preauthorized Transfers

A "preauthorized transfer" is one of a series of recurring electronic fund transfers at substantially regular intervals.[53] A preauthorized transfer cannot be made from your account at a

financial institution unless (a) you have given advance authorization in writing, and (b) a copy of your written preauthorization has been given to you by the party obtaining it.[54]

When preauthorized transfers from your account vary in amount from month to month, either the financial institution, or the person authorized to receive the funds, must give you a notice of the amount of the transfer and the scheduled transfer date at least ten days in advance of the scheduled transfer date.[55] You may, however, elect to receive such notices only when the transfer does not fall within a specified range, or when it differs from the most recent transfer by more than an agreed-upon amount.[56]

You may stop future preauthorized transfers at any time by notifying the financial institution at least three business days before the scheduled date of the next transfer that you want to stop.[57] Since this right cannot be waived,[58] it is a right that you may exercise without regard to the terms of any contract that you may have entered into with the recipient of preauthorized payments (for example a health studio or a public utility). This also means that your financial institution may not lawfully refuse to terminate automatic transfers on the basis that you have entered into an agreement with someone else for electronic payments. If your financial institution refuses to honor your request to stop payments, it is important that you register a formal complaint with the federal or state agency that regulates that financial institution.

If your stop payment notice is given orally, the financial institution may require that you provide written confirmation of your stop payment instruction within 14 days of your oral notification. A financial institution can require a written confirmation only if it informs you of that requirement, and gives you the address where you must send the written notification, at the time you give the oral notification.[59]

If the financial institution requires written confirmation of a stop payment instruction, your oral stop-payment instruction is no longer binding 14 days after it has been made.[60] At that point, your previously authorized automatic transfers will resume. It is important, therefore, that you promptly provide a written confirmation of a stop payment order if one is requested.

*****

Prepared by: Richard A. Elbrecht, Supervising Attorney, and John C. Lamb, Senior Staff Counsel, Legal Services Unit, May 2003. The December 2008 update was prepared by George Ritter, Senior Staff Counsel.

ENDNOTES

1. 15 USC § 1693 *et seq.*, 92 Stat. 3728; Pub. L. 95-630.
2. 12 CFR § 205 *et seq.*; see also the Federal Reserve Board's Official Staff Commentary on Regulation E, Federal Reserve Regulatory Service, vol. III, or at www.findlaw.com (click on Code of Federal Regulations link; type "12 CFR Part 205.17" in the boxes; click on Retrieve; scroll to Supplement I to Part 205 – Official Staff Interpretations).
3. 12 CFR § 205.1(b).
4. 15 USC § 1693*l* states in part: "No writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or action created by [the Electronic Fund Transfer Act]...." See also Official Staff Commentary on Regulation E, § 6(b). See California Civil Code § 1748.32.
5. 12 CFR § 205.1(b).
6. See, *e.g.*, Baker & Brandel, *The Law of Electronic Fund Transfer Systems*, rev. ed. (Arlington, VA: A.S. Pratt & Sons, looseleaf.)
7. 12 CFR §§ 205.2(a)(1), 205.6(a), and Official Staff Commentary on Regulation E, § 6(a).
8. See 12 CFR § 205.3(b).
9. See 12 CFR § 205.6(b)(1), and Official Staff Commentary on Regulation E, §§ 6(b), 6(b)(1).
10. See Official Staff Commentary on Regulation E, §§ 6(b), 6(b)(1).
11. 12 CFR §§ 205.6(a), 205.7(b)(1)-(3).
12. 12 CFR § 205.6(b)(2).
13. 12 CFR § 205.6(b)(2).
14. 12 CFR § 205.6(b)(3).
15. 12 CFR § 205.6(b)(5)(ii), (iii).
16. 12 CFR § 205.6(b)(5)(iii).
17. 12 CFR § 205.6(5)(i).
18. 12 CFR § 205.6(5)(iii).
19. 12 CFR § 205.11(b)(2).
20. 12 CFR § 205.6(b)(4).
21. 12 CFR § 205.2(m)(1), and Official Staff Commentary on Regulation E, § 2(m)(2).
22. 12 CFR § 205.2(m)(1), and Official Staff Commentary on Regulation E, § 2(m)(2).
23. 12 CFR § 205.2(m), and Official Staff Commentary on Regulation E, § 2(m)(3),(4).
24. 12 CFR § 205.7(b)(4).
25. 12 CFR §§ 205.2(a), 205.5, 205.6.
26. 12 CFR § 205.5.
27. 12 CFR § 205.6(a).
28. 12 CFR § 205.10(e). But see 12 CFR § 205.15.
29. Official Staff Commentary on Regulation E, § 10(e).
30. 12 CFR § 205.10(e)(2), and Official Staff Commentary on Regulation E, § 10(e)(2).
31. 15 USC § 1693f; 12 CFR § 205.11.
32. 12 CFR § 205.11(b)(1).
33. 12 CFR § 205.11(b)(1)(i).
34. 12 CFR § 205.11(b)(2).
35. 12 CFR § 205.11(c)(1).
36. 12 CFR §§ 205.11(c)(2)(i),(ii).
37. 12 CFR § 205.11(c)(2)(i).
38. 12 CFR § 205.11(c)(2)(i)(A).
39. 12 CFR § 206.11(c)(2).
40. 12 CFR § 205.11(c)(3).
41. 12 CFR § 205.11(c)(1),(2)(iii),(iv).
42. 12 CFR § 205.11(d).
43. 12 CFR § 205.11(d)(2).
44. 12 CFR § 205.7.
45. 12 CFR § 205.9(a).
46. 12 CFR § 205.9(b).
47. 12 CFR § 205.7(b).
48. 12 CFR § 205.9(a).
49. 15 USC § 1693d(f).
50. 12 CFR § 205.9(a)(1); see also California Financial Code § 13080(b).

51. 12 CFR § 205.9(b).
52. 12 CFR § 205.9(b).
53. 12 CFR § 205.2(k).
54. 12 CFR § 205.10(b).
55. 12 CFR § 205.10(d).
56. 12 CFR § 205.10(d).
57. 12 CFR § 205.10(c).
58. 15 USC § 1693*l*. See footnote 4.
59. 12 CFR § 205.10(c).
60. 12 CFR § 205.10(c)(2).