

SAFEGUARDS FOR ELECTRONIC BANKING



In banking as in so many other areas, the trend is clear: We continue to move steadily away from traditional paper transactions toward high-tech means of conducting our business. It will not happen overnight, though, and even the most technophobic among us should be assured that there are some federal laws and regulations in place that will make the transition easier and more secure.

ELECTRONIC FUND TRANSFER ACT

The methods for electronic fund transfers (EFTs) are already commonplace for many bank customers. They include ATMs, debit or check cards, preauthorized deposits and withdrawals, and telephone transfers. The federal Electronic Fund Transfer Act answers some basic questions about using EFT services. The Act is especially important when things go wrong, providing rules for the correction of errors and dealing with loss or theft.

Financial institutions must provide documentation of EFTs in two forms: terminal receipts and periodic statements. Among other pieces of information, both documents must include the type of transfer, the amount and date of the transaction, and the location of the terminal. For preauthorized transfers that occur at regular intervals, the institution must provide a notice that the transfer occurred as scheduled.



As with credit cards, financial institutions must investigate and promptly correct any EFT errors reported by the consumer, but there are some differences in the details. For errors like unauthorized or incorrect EFTs, or omission of an EFT from a statement, a consumer should contact the institution as soon as possible, and no later than 60 days after receiving the statement showing the error. As a general rule, the institution must promptly investigate and resolve the matter within 45 days. If more than 10 days pass, it must make the correction, subject to the results of the investigation. Such a recredit is made final if the institution finds an error; if it does not, it must explain the outcome of its investigation in writing to the consumer.

LOSS LIMITS

If your credit card is lost or stolen, your loss is limited to \$50 per card. That is also the general rule for an EFT card or code, but with the important caveat that procrastination in reporting a lost or stolen EFT card or code can be much more expensive. The exposure limit jumps to \$500 for a consumer who does not report the loss or theft within two days of learning of it. Not only that, but failure to report an unauthorized

(continued on inside flap)

PRSR STD
U.S. POSTAGE
PAID
Permit #2470
Las Vegas, NV

HUTCHISON & STEFFEN
ATTORNEYS

PECCOLE PROFESSIONAL PARK
10080 WEST ALTA DRIVE, SUITE 200
LAS VEGAS, NEVADA 89145
702-385-2500 • FAX 702-385-2086 • 877-HSNVLAW
HSNVLAW.COM

Business and Commercial Litigation

Corporate and Transactions

Employment Law

Appellate Law

Insurance Defense

Trust and Probate Litigation

Healthcare Professional's Advocacy

Real Estate Law

Construction Law

Landlord/Tenant

Administrative Law

Creditor's Rights and Bankruptcy

Environmental Law

Immigration Law

Family Law

Personal Injury

Alternative Dispute Resolution



Safeguards for Electronic Banking



Disposal of Consumer Credit Information

HUTCHISON & STEFFEN
ATTORNEYS

Legal Matters

Winter 2006

OPTION CARE VICTORY

Hutchison & Steffen's partner **Joseph Ganley** and associate **Patricia Thompson** scored a major victory in a groundbreaking case involving complicated provisions of the federal Prompt Payment Act in the 8th Judicial District Court, Clark County, Nevada, Department 15.

Hutchison & Steffen represented Option Care Inc., a healthcare provider, against Nevada Care, an insurance company, for improperly denying claims. Option Care Inc., was victorious and awarded nearly \$1 million as a result of the suit. Judge Sally Loehrer rendered the final decision in December 2005, resulting from a week-long trial that concluded in May 2005. ■



Joseph Ganley, Partner



Patricia Thompson, Associate

TASTER'S CHOICE MODEL WINS BIG

A two-hour photo shoot paying \$250 has turned into a jury verdict of over \$15 million for the model, but it took almost 20 years and some good luck for it to happen. Russell had his photo taken for use on labels by a major coffee maker. He did not think much more about it until many years later, when he saw the photo of himself savoring a cup of coffee.

According to the modeling agreement, which Russell had kept in his records, he was supposed to be paid additional sums if the photo was actually used in marketing. The company had never paid more money to Russell, even though



his photo had ended up on countless jars of coffee around the world for a six-year period. Nor did the company get his permission for the use of his image.

The jury award was based not just on the company's obligations under the agreement, but also on a percentage of the profits derived from the use of the image. Russell was able to show that his face, appearing as it did in all kinds of advertising, not just the jars of coffee, helped to sell a lot of coffee. As a result, the company's misappropriation of his image carried a very big price tag. ■

"Supposing is good, but finding out is better."
- Mark Twain

CAREFUL! NEW RULE AFFECTS THE DISPOSAL OF CONSUMER CREDIT INFORMATION

In the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Congress required the adoption of rules for the proper disposal of consumer

report information and records. The legislation was prompted by the growing risk of consumer fraud and related problems,

including identity theft, that arise from the improper disposal of consumer information for which there is no longer a business need or purpose. FACTA and the rule stemming from it are meant to make it tougher for dumpster divers and miners of computer data to profit from sloppy disposal methods.

The Federal Trade Commission's Disposal Rule went into effect June 1, 2005, but affected businesses will

have six months from that time to come into compliance. After that, failure to comply could trigger a range of civil enforcement actions by the Government or affected consumers.



While there is room for interpretation of the Disposal Rule's meaning, and how it should

be applied as circumstances change, the Rule's essential standard is all in one sentence:

Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

WHAT IS COVERED?

Consumer information covered by the Rule means any record about an individual, in any form, that is a consumer report or is derived from a consumer report. The definition includes a compilation of such records. If the information does not in some fashion identify individuals, however, such as information in aggregate form, the Disposal Rule does not apply. The obvious ways in which individuals may be identified are names, Social Security numbers, driver's license numbers, telephone numbers, physical addresses, and e-mail addresses. But even pieces of information that, by themselves, do not identify someone can, in combination, be regarded as identifying information.



If an entity can obtain a consumer report for one or more of the business purposes mentioned in the Fair Credit Reporting Act, it is safe to assume that the entity and the information it obtained are subject to the Disposal Rule. Disposal and records management companies also fall under the Rule.

REASONABLE MEASURES

The Rule uses the flexible term "reasonable measures" to describe the duty regarding disposal because perfect destruction of consumer information in every instance is unattainable. Variables that may be taken into account include the sensitivity of the information, the nature and size of the entity's operations, the costs and benefits of different disposal methods, and ongoing changes in technologies. It is also noteworthy that the concept of "disposal" also covers the sale, donation, or transfer of any medium on which consumer information is stored.

The Rule provides a nonexhaustive set of examples of "reasonable measures." To prevent the reading or reconstruction of records in paper form, policies should be adopted, and their implementation monitored, for the burning, pulverizing, or shredding of such papers. The same approach is

advisable for policies on destruction or erasure of electronic media. Since simply deleting information stored on a computer is usually insufficient to safeguard the information, use of some low-tech methods of destruction on some high-tech methods of storing information may be in order. For example, the Federal Trade Commission has suggested, at least for small businesses, the nearly cost-free method of disposing of electronic media by smashing the material with a hammer.

A covered person's due diligence



also should extend outside the office when disposal of information is contracted out to a provider of such a service. One of the "reasonable measures" mentioned in the Rule refers to taking steps to determine the competency and integrity of the disposal company, such as reviewing an independent audit of the company, getting references, requiring that the company be certified by a trade association, or reviewing and evaluating the disposal company's policies and procedures on information security. ■

safeguards for electronic banking

(continued)

transfer within the 60-day period for doing so creates unlimited exposure to losses from transfers made after the 60-day period.

PROCEED WITH CAUTION

The federal Government provides some EFT protection for old hands and novices alike, but the best approach is to combine that protection with your own safe practices. Keep a low profile for thieves and scam artists by protecting your personal information, such as bank account



numbers, passwords, and Social Security numbers. Never respond with such information to unsolicited telephone calls or e-mails. Verify the legitimacy of a website address before providing personal information on the site. It is a good idea to have virus protection and a "firewall" on your computer to keep hackers out. Finally, keep good banking records and review each bank statement promptly so that you can report anything suspicious you see in time for it to do you the most good. ■

Actual resolution of legal issues depends upon many factors, including variations of fact and state laws. This newsletter is not intended to provide legal advice on specific subjects, but rather to provide insight into legal developments and issues. The reader should always consult with legal counsel before taking any action on matters covered by this newsletter.