

GROWING FIRM STRENGTH

As with any organization, our firm's strength lies in the ability, skill and dedication of its people. We added considerably to the firm's strength in three ways during the past few months. On January 1, 2004 Michelle Leu Zaccone was elevated to shareholder status. Michelle started with the firm many years ago as a legal assistant. She earned her law degree while raising a family and working full time. After working for another law firm for a few years, Michelle rejoined us to focus her practice on litigation and real estate transactional matters. Michelle combines legal knowledge and skill with an energy and tenacity that serves as a model for excellent lawyering and client service. We are pleased and proud to call her our "partner."

Although the muscles of our Estate Planning, Trust & Wealth Transfer group were already bulging (pardon me, Governor Schwarzenegger), we bulked up the team further by adding two additional associates. Laurelle Gutierrez-Lundquist is an experienced and knowledgeable attorney in estate planning having practiced nine years in a highly regarded estate planning firm in San Francisco. As a University of California, Berkeley and a University of San Francisco Law School graduate, Laurelle and her family have deep roots in our community. On the heels of adding Laurelle, we were excited to have Sinclair Hwang join us in February. Sinclair, who grew up in Houston, Texas, is a 1997 Princeton University graduate of the Woodrow Wilson School of Public and International Affairs. He came to sunny California to get his law degree at U.C. Berkeley's Boalt Hall. Although Sinclair always wanted to devote his legal career to Estate & Trust planning, he first honed his skills in a corporate transactional practice of a large law firm in Silicon Valley before joining us. (We have yet to have him entertain us on his acoustic guitar.) We are extremely pleased to have both Laurelle and Sinclair.

In this issue of *Perspectives*, as always, we try to give you a sampling of articles on legal issues of current interest. They range from *Protect Yourself from Online Dangers – Before It's Too Late!* by Barry Parker, our intellectual property law expert, to *State Extends COBRA Benefits* by Elisè Clowes, the head of our Employment practice area. We trust that all the articles will be of both interest and value to you.

Mark Cassanego is President of Carr McClellan.

PROTECT YOURSELF FROM ONLINE DANGERS – BEFORE IT'S TOO LATE!

By Barry Parker, Esq.

The U.S. Commerce Department reports that e-commerce in the U.S. topped \$17.23 billion dollars in the Fourth Quarter of 2003 alone, a 29.7 percent increase over the previous quarter. While this is certainly great news for business, the bad news is that there are serious hidden dangers related to conducting transactions over the Internet. Now more than ever, consumers and businesses alike must stay informed, diligent and proactive in guarding their personal information and proprietary business information from online thieves.

Be Informed

The Federal Trade Commission ("FTC") received over 500,000 complaints for online fraud and identity theft in 2003. In fifty-eight percent of the complaints, consumers were contacted over the Internet. Consumer losses related to Internet fraud are staggering, reaching almost \$200 million in 2003 alone. Not surprisingly, online fraud and identity theft complaints from California consumers led the nation at 76,673. Unfortunately, the trend is expected to increase as the use of hidden tracking software and online scams proliferate.

Many consumers and businesses remain unaware that by merely surfing the Internet, opening email or downloading software, small computer programs commonly referred to as "Adware" and "Spyware" are being downloaded to your computer without your knowledge or consent. These programs are designed to collect and transmit information about you, such as which Web sites you visit, which links or ads you click on, and the duration of your visits. Some of these programs can scan your computer and gather personal information about you or your customers, such as name, age, gender, credit card numbers, passwords, email addresses and more. Some track your keystrokes or the information that you provide when filling out online forms. Some of these programs can dial out and "call home" without your knowledge, incurring long-distance telephone charges. Worse yet, some of these programs give an outsider complete access and *control* over your computer with all the access rights and network privileges of the computer user where the Spyware is installed. see PROTECT YOURSELF, page 6

SPRING 2004



CHARITABLE ORGANIZATIONS

- 2 Rules Regarding Asset Management and Financial Relationships – Part II

EMPLOYMENT LAW

- 4 State Extends COBRA Benefits

CONTRACTS

- 5 Signing Contracts 101 & Unenforceable Noncompetition Agreements



RULES REGARDING ASSET MANAGEMENT AND FINANCIAL RELATIONSHIPS – PART II

By Penelope Greenberg, Esq.
In the Fall 2003 issue of *Perspectives*, Part I of this article covered organizational structure, tax exempt status, and investment rules and standards with special rules applicable to private foundations. (If you would like a copy of Part I, please contact Royal Simpkins at 650.342.9600.) This Part II looks at compensation, self-dealing, enforcement, and practicalities.

Compensation

Employees. An exempt organization may compensate its employees, and, in fact, most publicly supported exempt organizations and some private foundations do have paid staff. Paid staff members can even include family members of the organization's founders and contributors. The key is that compensation must be in an amount that is no greater than fair market value. The basic rule of thumb is very simple: If the organization would pay an absolute stranger with the same qualifications as possessed by the suggested employee to devote the same amount of time and effort to the job that the suggested employee is planning to devote, then the compensation is probably reasonable. Thus, for example, if a member of the founder's family offers to oversee the investment activities of the foundation's professional financial advisor and wants to be paid a percentage of the assets of the foundation for doing so, the rule of thumb makes it clear that such an arrangement would not pass muster.

There are compensation studies broken down by size of organization, geographic locations, job duties, etc. that provide guidance as to reasonable compensation. There are also the want ads, non-profit publications and organizations that provide employment information and assistance, head-hunters, and other such sources. If there is any doubt about the reasonableness of compensation being contemplated, the organization should document with objective information the justification for the compensation being paid.

Directors. An exempt organization may also compensate directors, although many organizations do not, preferring to conserve assets for charitable uses. According to the Council on Foundation's 2000 *Foundation Management Survey*, only 11% of small private foundations (under \$10 million in assets) compensate all board members, and another 14% compensate some board members. If directors are compensated, care must be taken to observe the rules against inurement/private benefit and self-dealing. As with employee compensation, the exempt organization may pay only what is reasonable. Excessive or unjustifiable compensation for directors (or employees in general) can expose the

“Excessive or unjustifiable compensation for directors (or employees in general) can expose the exempt organization to excise taxes and (theoretically) even revocation of tax-exempt status.”

exempt organization to excise taxes and (theoretically) even revocation of tax-exempt status.

The 49% Rule. Under California Corporations Code Section 5227, no more than 49% of the members of the board of directors may be persons who are currently being compensated by the corporation for services rendered within the past 12 months or persons who are a relative of such compensated person. This is not a tax rule, but rather a corporate rule. Relatives include siblings and siblings-in-law, parents and parents-in-law, children and children-in-law, grandparents, grandchildren, and spouses. Thus, for example, a three-member board consisting of the uncompensated founder plus the organization's paid legal counsel and paid accountant would violate the 49% rule. Assuming that the lawyer and accountant do not want to work for free, the solution would be to expand the board to five, with three of the directors being uncompensated, making the board 3/5 (60%) uncompensated and 2/5 (40%) compensated.

For purposes of the 49% rule, compensation does not include reasonable compensation paid to a director for being director. However, the protection of California Corporations Code Section 5239 (“no personal liability to a third party for monetary damages on the part of a volunteer director...caused by the director's negligent act or omission”) is not available to a director who is compensated for being a director.

Self-Dealing and Inurement/Private Benefit

Inurement/private benefit. Both public charities and private foundations, being organizations exempt under IRC Section 501(c)(3), are covered by that section's proscription against inurement and private benefit (“...no part of the net earnings of [the organization] inures to the benefit of any private shareholder or individual...”). Basically, inurement and private benefit mean using charitable assets for noncharitable purposes to benefit corporate insiders or other private persons. Public charities that violate the rule are at risk for intermediate sanctions. Private foundations that violate the rule or violate IRC Section 4941's provisions against self-dealing (discussed below) are at risk for the self-dealing excise taxes. Both private foundations and public charities may also, as a result, be in violation of the self-dealing rules under California Corporations Code Section 5233.

California Corporations Code Self-Dealing Rules. Corporations Code Section 5233 (which applies to all California nonprofit public benefit corporations, whether private foundation or public charity) prohibits a transaction to which the corporation is a party and in which a director has a material financial interest, unless the following is true:

- (1) the corporation entered into the transaction for its own benefit;
- (2) the transaction was fair and reasonable as to the corporation at the time;
- (3) prior to consummating the transaction the board authorized or approved the transaction in good faith by a vote of a majority of the directors then in office without counting the vote of the interested director and with knowledge of the material facts of the transaction and the director's interest in it; and
- (4) the corporation in fact could not have obtained a more advantageous arrangement with

reasonable effort under the circumstances, or, prior to authorizing the transaction, the board in good faith determined after reasonable investigation under the circumstances that the corporation could not have obtained a more advantageous arrangement with reasonable effort under the circumstances.

So, in other words, it is possible for a public charity to transact business with one of its directors *if* it is good for and fair and reasonable to the corporation and *if* all the board members understood the situation and *if* the interested director did not vote and *if* a more advantageous arrangement was not possible.

Some transactions are excluded from these self-dealing rules. For example, the board may fix the compensation of directors and officers without worrying about the self-dealing rules. A transaction in which the interested director is unaware that he or she has an interest and which involves no more than \$100,000 (or no more than 1% of the corporation's gross receipts for the previous year, if that is less than \$100,000) is also ok.

If a transaction occurs in violation of these rules, the interested director will be required to make payments or restitution or otherwise fix the problem in whatever manner the court deems fair. The interested director may also be liable for damages and even exemplary damages if the violation was fraudulent or malicious. In other words, self-dealing is to be avoided.

IRC Section 4941 Self-Dealing Rules. Specifically for private foundations, IRC Section 4941 applies more stringent "self-dealing" rules. The following transactions are not allowed between the foundation and "disqualified persons" ("DQPs") (substantial contributors, directors, officers, trustees, persons having similar authority, family members of all these [ancestors, spouse, descendants, spouses of descendants], owners having at least 20% control of companies that are substantial contributors, corporations owned 35% or more by disqualified persons counted together):

- (1) sale, exchange, or lease of property (in either direction);
- (2) loan of money or other extension of credit (in either direction);
- (3) payment of compensation (by a private foundation to a DQP);
- (4) transfer of the foundation's income or assets to a DQP or for his or her use or benefit
- (5) agreement by the foundation to pay money or other property to a government official (except for certain pending employment of an ex-official by the foundation).

However, there are exceptions to these prohibitions. The more important exceptions are:

- (1) A DQP can lend money to the foundation at no interest if the foundation uses the money for its charitable purposes.
- (2) A DQP can supply goods, services, or facilities to the foundation for free if the foundation uses them for its charitable purposes.
- (3) The foundation can furnish goods, services, or facilities to a DQP under the same circumstances as the foundation furnishes them to the general public.

“What you can’t do is fly your whole family to Maui at the foundation’s expense just for the fun of holding the board meeting there.”

(4) The foundation can pay compensation and expenses to a DQP for personal services that are reasonable and necessary to carrying out the exempt purposes of the foundation if the compensation and expenses are not excessive.

(5) A transaction between the foundation and a corporation that is a DQP is allowed pursuant to a liquidation, merger, redemption, recapitalization, or similar event of the corporation if the securities held by the foundation are treated no differently from the others in the same class and if the foundation receives fair market value.

So what does all this mean? It means that you as a director can give your foundation an office in your home or your commercial building as long as you don't charge the foundation rent. It means that you can lend money to the foundation to help get it started or to address a sudden charitable need and later get the money back from the foundation but with no interest. It means that you can buy a ticket to the art show sponsored by your foundation at the same price that the general public pays for a ticket. Most importantly, your foundation can hire you and compensate you *if* your services are really needed and the compensation is fair.

What you can't do is fly your whole family to Maui at the foundation's expense just for the fun of holding the board meeting there. You can't hire your son to open the mail and handle correspondence and pay him handsomely for the two hours a month he devotes to this task.

Violating the self-dealing rules puts the foundation in line for excise taxes along the lines of those for jeopardizing investments (discussed in Part I): 5% followed by 200% on the foundation, 2% (max. \$10,000) followed by 50% (max. \$10,000) on the foundation manager.

Oversight and Enforcement

IRS/Franchise Tax Board. Once the IRS and the FTB grant tax-exempt status to an organization, their focus on the organization usually ceases, so long as the organization files the proper returns, forms, and reports when required. However, if information later reaches these agencies that the organization may have violated or be operating in violation of applicable law, the IRS or FTB may come to audit or investigate. Revocation of tax-exempt status, although theoretically possible in extreme cases of misuse of assets or other violations, is rarely used. More common are various taxes and penalties. Under federal law, for public charities, there are the intermediate sanctions under IRC Section 4958, which imposes the taxes on excess benefit transactions that occurred on or after September 14, 1995. These taxes are the counterpart to the self-dealing excise taxes imposed on private foundations.

An excess benefit transaction occurs when a public charity pays a disqualified person too much for goods or services. The amount above what was reasonable is the excess benefit. The DQP receiving the excess benefit is assessed a 25% tax on the excess benefit and, with some exceptions, any organization manager (i.e., officer, director, trustee, or person with similar authority) who participates (or remains silent when having a duty to speak up) is assessed a 10% tax. If the excess benefit is not

returned to the charitable organization (along with whatever more is needed to make the organization whole) within the required time period, the DQP is assessed an additional tax of 200%. If it is the manager that received the excess benefit, he or she could be liable for both the DQP and the organization manager taxes.

(Note that it won't work to claim after the fact that an excess benefit was intended to be part of the DQP's compensation. That has to have been "clearly indicated" by the charitable organization at the time the benefit was conferred and not just offered up later as a justification – and, of course, the total compensation must still be reasonable.)

For purposes of the intermediate sanctions, a DQP is any person who, at any time during the five years leading up to the excess benefit transaction, was in a position to exercise substantial influence over the affairs of the organization. This includes board directors, presidents, CEOs, COOs, CFOs, treasurers, etc. Also included in this category are family members of the DQP (the same ones as in the private foundation self-dealing rules plus whole and half siblings and their spouses) as well as entities controlled 35% or more by DQPs.

The California Attorney General. Coming at exempt organizations from another angle is the California Attorney General, who represents the interests of all charitable beneficiaries and stands ready to ensure that directors are not mismanaging or defrauding the organization and that charitable assets and services are reaching the intended beneficiaries. As stated in California law, "A corporation is subject at all times to examination by the Attorney General, on behalf of the state, to ascertain the condition of its [the corporation's] affairs and to what extent, if at all, it fails to comply with trusts which it has assumed or has departed from the purposes for which it is formed. In case of any such failure or departure the Attorney General may institute, in the name of the state, the proceeding necessary to correct the noncompliance or departure." (Corporations Code Section 5250)

Thousands of complaints are submitted to the AG's Office from the general public, news reporters and other interested parties. All complaints are reviewed, but the small size of the investigative staff and its limited resources restrict the number of investigations that can be undertaken. Problems commonly investigated include self-dealing transactions; loans; sudden loss of assets; speculative investment losses; excessive payments for salaries, benefits, travel, entertainment, legal fees, etc.; illegal use of funds; or diversion of funds from their charitable purpose. If violations are found, the Attorney General may sue to have directors removed and misappropriated assets restored. Under the Supervision of Trustees and Fundraisers for Charitable Purposes Act (Government Code Sections 12580 – 12599.5), the AG has ten years after the fact to file an action to enforce the law.

Practicalities

Observance of Corporate Formalities. Larger exempt organizations with a number of employees, a real office, and the usual trappings of business, albeit a nonprofit, tax exempt business, generally are fairly see Rules, page 8



STATE EXTENDS COBRA BENEFITS

*“As of
September 1, 2003,
employees
who opted for
COBRA after
1/1/03 may
extend their
18 months
of federal
COBRA
benefits by
tacking on
18 months
Cal-Cobra
benefits.”*

By Elisè Clowes, Esq.

Under a recently enacted California law, insurers and HMOs will be required to provide COBRA continuation coverage for 36, rather than 18, months from an employee's "qualifying event." As of September 1, 2003, employees who opted for COBRA after 1/1/03 may extend their 18 months of federal COBRA benefits by tacking on 18 months Cal-Cobra benefits. This applies to all group health plans and HMOs, but may not apply to sponsors of self-insured plans. (Employers should check with counsel as to the type of plan.)

Cal-COBRA applies primarily to employers with less than 20 employees. Employees covered by Cal-COBRA will be eligible for 36 months of continued benefits at the Cal-COBRA rate of 110% of group health cost. Employees covered by COBRA will have continuation benefits for the first 18 months under federal COBRA, at the rate of 102% of the former group health cost. After the first 18 months, the employees will be eligible for another 18 months of continuation coverage under Cal-COBRA at the 110% rate. If an employee is disabled, his or her COBRA rate can be 150% of the group rate for the Cal-Cobra months.

Under Cal-COBRA, plans must notify individuals when their extended coverage terminates.

Employers need to make sure that their plan sponsors update the summary plan descriptions to inform plan participants, and revise the employee handbook and COBRA notices to allow for 36 months of benefit continuation.

Elisè Clowes is a member of the Employment Group.



SIGNING CONTRACTS 101

By Lori Lutzker, Esq.

One of the main reasons individuals create corporations or other limited liability entities is the desire to avoid personal liability for contractual obligations. What many don't realize is that an officer or agent who signs a contract for the corporation must sign it in a particular manner to avoid personal liability.

An agent who signs a contract is personally liable unless the name of the principal is disclosed so as to make it appear on the face of the instrument that the parties intended to bind the principal and not the agent. And a disclosure only of the principal's *trade name* is not a sufficient disclosure of his identity to relieve the agent of personal liability. Also, the person who signs the contract should always be sure that the principal's name is listed by the signature block and the individual should include his office (such as "president" or "agent") under his signature.

In the case of *Otis Elevator Co. v. Berry*, the contract was for the repair of an elevator located in a hotel operated by the "Berry Hotels System," a corporation. The plaintiff addressed an offer to the "Hotel Berry Systems." The defendant accepted the offer as follows: "Signed and accepted in duplicate, Sept. 17, 1926. B. S. Berry." B. S. Berry was secretary of the company and was authorized to enter into contracts on its behalf. Over objection, the trial court admitted oral evidence that Berry signed the contract as agent of the corporation and that the plaintiff knew that this was the fact. The appellate court held that the finding to this effect was supported by evidence, but that the evidence had been erroneously admitted. Berry argued that an ambiguity was created because the offer was addressed to the "Hotel Berry Systems," and then signed "B. S. Berry." The court held that there was no ambiguity, and that extrinsic evidence should not have been admitted. The court explained:

The rule is that where a person signs his own name to a written contract, without qualification and without disclosing that he acts solely as agent, extrinsic evidence is inadmissible to prove that he acted solely as agent and was not a party to the contract...An agent, who has signed his own name unqualifiedly, may introduce extrinsic evidence to show that he is not a party to the contract, only where the contract itself contains some phrase or provision which shows that he was acting in a representative capacity. Applying this rule to the instant case, it is apparent that no such ambiguity existed. The mere fact that the proposal was addressed to the defendant's principal is not enough, for the contract might also have been intended to bind the agent as well. Aside from the address,

"An agent who signs an agreement in his own name is personally liable unless he indicates on the writing itself his intention to bind the principal only."

there is no reference in the contract to defendant's principal, and there is no clause in the contract which, either expressly or by implication, indicates that defendant acted in a representative capacity. Defendant signed his name without indicating the identity of his principal, or even the fact that he was acting as agent. Under these circumstances, he cannot now assert that he is not a party to the contract.

In *Southern Pac. Co. v. Grangers' Business Assn.*, the court said:

The rule has been long and continuously settled that an agent who signs his own name instead of that of the principal when he intends to bind the latter, becomes himself liable, the contract being considered his own...To exclude the personal liability of an agent who signs a contract in his own name, the capacity in which he signs must appear upon the face of the instrument. If, upon the face of the instrument, the agent signs his own name only, without referring to any principal, then he will be held bound personally although he was known to be or avowedly acted as agent.

Thus, an agent who signs an agreement in his own name is personally liable unless he indicates on the writing itself his intention to bind the principal only. Be sure you write the name of your principal and your office where you sign a contract if that information is missing.

UNENFORCEABLE NONCOMPETITION AGREEMENTS

In California, most noncompetition agreements are unenforceable. There are narrow exceptions such as where a person sells the goodwill of a business or where a partner agrees not to compete in anticipation of dissolution of the partnership. Otherwise, every contract by which anyone is restrained from engaging in a lawful business, trade or business is void.

Until recently, it was unclear whether an employer could prevent an employee from soliciting or having any dealings with the employer's customers or potential customers upon leaving employment. The theory behind the enforceability of such an agreement is that it does not prevent an employee from continuing in his business or trade, from working for a competitor or a customer, from accepting the business of former customers if they solicit him, or from soliciting former customers with whom he had no dealings.

In a recent California Court of Appeal case, *Thompson v. Impaxx*, the court held that such a contract provision was unenforceable because the identity of the employer's customers was not confidential and was not a trade secret. The Court explained that in the absence of a protectable trade secret, the right to compete outweighed the employer's right to protect its clients from competition from former employees.

If that computer has full access to your financial and/or proprietary business information, your information may be seriously compromised.

Alarmed? You should be. Spyware programs are not generally detected by anti-virus software. They are not stopped by operating system security patches and by physical and software firewalls because these programs do not exploit holes in computer security measures. Rather, they take advantage of the open connection you create when accessing Web sites and emails. Sometimes these programs are secretly piggybacked on software that you purchase and download to your computer. Sometimes Spyware is *purposely* embedded within the software that you purchase and download to your computer. Read your end user license agreements! Some agreements actually grant the software vendor and its affiliates the contractual right to track, collect, share and use personal information about the users of the software.

A newer trend in online scams designed to steal your personal information is a technique called “phishing.” This is where a misguided party steals the identity of a business and uses the company’s trade name, trade dress, trademarks and confusing similar domain names to send out “legitimate looking” email or create Web sites that mimic (“spoofs”) the identity of the real company. By posing as a legitimate company email (or Web sites), consumers are asked to confirm or update account or billing information. As a result of these official looking emails, nearly twenty percent of consumers are fooled into divulging personal information, resulting in identify theft, financial loss and other fraudulent activity. Government entities and organizations are not immune either. Recently, the Australian High Tech Crime Center warned that criminals are using emails claiming to be federal police and fooling recipients to click on certain links and tracing keystrokes with Spyware to record the input of online bank passwords.

Be Diligent and Proactive

So how do you protect yourself from online fraud and identity theft?

- Keep your operating system up to date with all available security updates and patches. For Windows operating system users, go to www.microsoft.com and click on “Windows Update,” then scan and install the security updates available for your operating system. This will help protect against known security vulnerabilities in the operation system.

- Use and keep your anti-virus software up to date.
- Use a firewall, especially if you have a high-speed or an “always on” connection to the Internet. Consider turning off your high-speed modem and/or computer when not in use.

- Use and keep up to date Adware / Spyware detection and blocking programs. Many available versions of Spyware detection and blocking software are shareware and available for personal use for no charge (donations accepted). (See e.g., *Adaware* at www.lavasoftusa.com or *SpywareBlocker* at www.javacoolsoftware.com/spywareblaster.html). Commercial users typically must purchase a license.

- Use Privacy software. This type of software allows you to identify and block specific personal

“Read your end user license agreements! Some agreements actually grant the software vendor and its affiliates the contractual right to track, collect, share and use personal information about the users of the software.”

information from being sent from your computer without your permission. Some programs will alert you each time your computer attempts to send your personal information outside of your computer. Some anti-virus protection programs are building this privacy functionality into the software.

- Protect access to your computer by using strong passwords that comprise a combination of at least nine letters, numbers and symbols. Do not use your name, family name, pet name or other names or words that may be easy to guess. Do not store your passwords in unencrypted files on your computer and certainly not in a folder or file entitled “passwords.” Avoid using automatic login features that save your user name and passwords. Log-off when you’re done!

- Consider using secure, removable storage for sensitive information and secure it away in a safe and secure place under lock and key.

- Read Web site privacy policies. They should answer questions about the access to and accuracy, security and control of personal information the site collects, as well as how sensitive information will be used, and whether it will be provided to third parties. When in doubt, “just say no!”

- Whenever you input personal and/or financial information on the Internet, make sure that the third party Web site is using a secure browser – look for the “lock” icon on the status bar on the lower right hand side of your computer monitor. It’s a symbol that your information is secure (encrypted) during transmission. If you are not sure of the secure nature of the transaction or you are not sure whom you are dealing with, follow the rule: “when in doubt, don’t give it out!”

- Review your credit card statements and bank accounts used on the Internet as soon as you receive them and look for unauthorized charges. If your statement is late more than a couple of days, call your credit card company or bank to confirm your account balances and to ensure that someone has not changed your billing address to avoid detection.

- Do not reply or click on links in emails asking you to take any action to input personal information, user names, passwords, dates of birth, social security numbers, account numbers or other billing information. Contact the company by telephone using a number obtained from a source other than the email.

- Do not open SPAM! When in doubt, delete, delete, delete!

- Avoid emailing personal or financial information or other sensitive documents.

- Before you dispose of your computer, delete all personal and business information stored on your computer by using a “wipe” disk utility program (perhaps several times to be safe).

The Tell Tale Signs of Identity Theft

- You find unexplainable charges on your accounts or withdrawals from your bank accounts;
- Your bills don’t show up on time or at all, indicating an identity thief has changed your address;
- You receive credit cards you did not order;
- New credit accounts show up on your credit report; and
- You receive calls from debt collectors or companies about merchandise or services that you didn’t purchase.

Reporting Identity Theft - Consumers

What do you do if you even think you are the subject of online identity theft? Take the following four steps immediately - don't hesitate:

1. **Call the below three credit bureaus to place a fraud alert on your credit report.** This will help prevent an identity thief from opening accounts in your name. As soon as the credit bureaus confirm your fraud alert, all three reports will be sent to you free of charge. Review the reports carefully and advise them of any inaccurate or suspicious activity.

- **Equifax** – To report fraud, call: 1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241

- **Experian** – To report fraud, call: 1-888-EXPERIAN (397-3742), and write: P.O. Box 9532, Allen, TX 75013

- **TransUnion** – To report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

2. **Notify all your creditors and check all your accounts** – with banks, credit card companies and other lenders, phone companies, utilities, Internet Service Providers, and other service providers.

Close any accounts that have been tampered with or opened fraudulently. If there have been any fraudulent charges, purchases or debits, ask the company about their fraud dispute policy and whether or not the company accepts the ID Theft Affidavit (available at www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf). The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card or any other electronic way to debit or credit an account. It also limits your liability for unauthorized activity if you act promptly (\$50 if reported within 2 days; \$500 if reported within 60 days; no limit if reported after 60 days). If your checking account number has been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. Contact the following major check verification companies and ask that retailers who use their databases not accept your checks.

- **TeleCheck** – 1-800-710-9898 or 927-0188

- **Certegy, Inc.** – 1-800-437-5120

- **International Check Services** – 1-800-631-9656
Call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.

3. **File a report with your local police or the police in the community where the identity theft took place.** Obtain the police report number and a copy of the report to validate your claims to creditors.

4. **File a complaint with the FTC.** To file a complaint or to learn more about the FTC's Privacy Policy, visit www.consumer.gov/idtheft. If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Reporting Security Breaches – Agencies and Businesses

Effective July 1, 2003, California Civil Code §§ 1798.29 and 1798.82 require agencies and persons and businesses that conduct business in California that own or license computerized data that includes

“The State of California leads the nation in providing protection to identity theft victims and important tools to ameliorate the impact of the crime.”

personal information to expediently notify effected California residents of any breach of the security of the system following discovery or notification that an unauthorized person may have acquired the data (if unencrypted). Under the Code, “personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number.

2. Driver's license number or California Identification Card number.

3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Any failure to provide the required notice gives the injured consumer a civil cause of action to recover damages against the business.

Federal and State Criminal Statutes

Identity theft is a crime punishable under both the federal Identity Theft and Assumption Deterrence Act and California Penal Code §530.5-530.8. Under federal law, violations of the Act are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and Social Security Administration's Office of the Inspector General. The U.S. Department of Justice prosecutes Federal identity theft cases. A conviction for identity theft under federal law carries a maximum penalty of 15 years imprisonment and a fine and forfeiture of any personal property used or intended to be used to commit the crime. Schemes to commit identity theft or fraud also may involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties – in some cases, as high as 30 years in prison as well as fines and criminal forfeiture.

The State of California leads the nation in providing protection to identity theft victims and important tools to ameliorate the impact of the crime. Under California Penal Code §530.5-530.8, the crime of identity theft is specifically defined; the law enforcement agency in the victim's area is required to take a police report; the victim is allowed to get an expedited judicial ruling of factual innocence; the Department of Justice is required to establish a database of identity theft victims accessible by law enforcement and victims; and financial institutions are required to release information and evidence related to identity theft to a victim with a police report or to the victim's law enforcement representative. For lesser offenses, the crime is punishable by imprisonment in the county jail for not more than a year and a fine not exceeding \$1,000. For more serious cases, the crime is punishable by imprisonment in the state prison and a fine not to exceed \$10,000.

Under California Penal Code sections 182 and 529.7, Courts can impose fines of up to \$25,000 on individuals convicted of felony conspiracy to commit Identity theft.

Under California Penal Code sections 853.5-853.6 and Vehicle code sections 40303, 40305, 40305.5,

40500 and 40504, victims can clear their records when an identity thief is arrested using the victim's name.

Under California Civil Code section 1748.95 and California Financial Code sections 4002 and 22470, the law requires certain types of financial institutions to release to a victim with a police report or to the victim's law enforcement representative information and evidence related to identity theft.

In addition, consumers may have other civil causes of action and legal remedies.

While the legal remedies for identity theft and online fraud are many, the practicalities of apprehending and enforcing the law against distant and evasive perpetrators remains difficult and a frustrating reality. Thus, we must be reminded of the principles of caveat emptor ("buyer beware") and the application of the old adage, "an ounce of prevention is worth a pound of cure." For more information and excellent federal and state resources on identity theft, visit <http://caag.state.ca.us/idtheft> and www.consumer.gov/idtheft. Be aware and be safe out there!

Barry Parker is a member of the firm's Intellectual Property Group.

RULES, continued from page 4

diligent about holding regular board meetings, keeping minutes, filling board vacancies when they arise, electing directors and officers at the proper intervals, filing tax returns when required, obtaining appropriate accounting assistance, and so forth. Smaller organizations, particularly those with small boards and no employees, may be tempted to be less meticulous, but that is not advised. For many reasons, including limiting liability, documenting prudent financial management, maintaining credibility in the nonprofit and greater business community, and preserving the organization's tax exempt status, it is important to observe the corporate formalities, to conduct the organization in accordance with the rules applicable to corporations and public or private charities, and to be sure that decisions and actions are recorded and properly documented. A stitch in time definitely saves nine.

Endowments. An endowment is a fund whose principle is intended to be kept intact to produce income that is spent for charitable purposes. The Uniform Management of Institutional Funds Act defines "endowment fund" as "an institutional fund, or any part thereof, not wholly expendable by the institution on a current basis under the terms of the applicable gift instrument." "Gift instrument" means "a will, deed, grant, conveyance, agreement, memorandum, writing, or other governing document (including the terms of any institutional solicitations from which an institutional fund resulted) under which property is transferred to or held by an institution as in institutional fund." (Emphasis added.)

Confusion sometimes arises between endowments that are created by the donor of the

funds and so-called endowments that are created by the board of directors using funds that were contributed to the exempt organization without any restriction by the donor. Donor-restricted endowments must be honored according to the terms of the restriction (unless the original purpose is so frustrated that the law may substitute another purpose under the rule of *cy pres*). The use of board-restricted funds, however, is not so limited. A subsequent board, or even the same board that imposed the restriction, may change the charitable purpose for which the fund is used and/or spend as much of the principle as the board wishes.

To avoid misunderstandings by board and public alike (and to avoid inadvertently creating an endowment when none was intended – see the underlined portion above of the definition of "gift instrument") and to preserve the organization's flexibility in meeting future charitable needs, fundraising campaigns should not speak of "endowments" or promise that money contributed will fund an "endowment" unless it really is the intent of the donor community and the exempt organization that the contributed funds will be locked up forever and only the income will be available.

Note that the Uniform Management of Institutional Funds Act in Section 18507 provides that the governing board may lift or change a restriction on funds, with the donor's consent, or, if the donor is unable to consent because of death, disability, unavailability, or impossibility of identification, the governing board may, with the approval of the local superior court and the participation of the Attorney General in such proceeding (if the court finds that the original restriction is "obsolete or impracticable") change the charitable use of an endowment – but not its status as an endowment. Note too that if the donor merely refuses to consent and is not dead, disabled, unavailable, or unidentifiable, the institution is stuck with the endowment as is unless relief is available under the doctrine of *cy pres*, which applies only if it is impossible or illegal to fulfill the original charitable purpose, a higher standard to meet than that of Section 18507.

Conclusion

Exempt organizations perform a vital role in American society and reflect the selfless efforts of countless individuals. The federal and state rules applicable to these organizations are designed to help them stay on the right track, ethically and financially, and to provide assurance to the organizations' donors and recipients of services that the organizations are handling their assets wisely and for the benefit of the public.

Penelope Greenberg is a member of the Exempt Organizations Group.

CARR McCLELLAN
INGERSOLL THOMPSON & HORN

Professional Law Corporation

CARR McCLELLAN
216 PARK ROAD
BURLINGAME
CALIFORNIA 94010


P 650.342.9600
F 650.342.7685

WWW.CARR-MCCLELLAN.COM

PERSPECTIVES ON LAW
IS PUBLISHED BY CARR
McCLELLAN INGERSOLL
THOMPSON & HORN
PROFESSIONAL LAW
CORPORATION. OUR GOAL
IS TO PROVIDE CLIENTS
AND FRIENDS OF THE FIRM
WITH MORE THAN JUST
UPDATES ON HOW THE LAW
IS EVOLVING. WE HOPE TO
SHARE OUR *PERSPECTIVES*
SO THAT YOUR BUSINESSES
AND FAMILIES CAN MAKE THE
MOST OF THE OPPORTUNITIES
BEFORE YOU.

CARR McCLELLAN,
FOUNDED IN 1945, IS LOCATED
IN BURLINGAME. THE FIRM
PROVIDES FULL-SERVICE LEGAL
ADVICE TO MANY CLOSELY-HELD
BUSINESSES AND MAJOR
CORPORATIONS IN THE BAY
AREA'S LEADING INDUSTRIES,
AS WELL AS TO INVESTORS
AND FAMILIES.

THIS NEWSLETTER IS FOR GENERAL
INFORMATION PURPOSES ONLY AND IS
NOT INTENDED TO OFFER LEGAL ADVICE
ON SPECIFIC CASES. PLEASE CONTACT
YOUR CARR McCLELLAN ATTORNEY
TO DETERMINE HOW THIS INFORMATION
MIGHT AFFECT YOU.

 THIS NEWSLETTER IS PRINTED ON RECYCLED PAPER.