

RECOGNIZE AND PROTECT YOUR VALUABLE TRADE SECRETS

By David Hoffman

It is not easy to build a successful winery or vineyard. A successful business usually requires having some advantage over the competition. That advantage is often the value of trade secrets.

Wineries and vineyards may have many trade secrets, including business information such as customer and guest lists, wine club member lists, vendor lists, and technological secrets such as methods of making wine or growing the vines. This information can be very valuable. Trade secrets can also include “negative information,” such as what advertising or marketing does not work, what harvesting techniques do not work, what additives or combinations of additives in wine do not work, etc. It is important to take steps to protect your trade secrets, otherwise a court will not enforce them for you.

Theft (misappropriation) of trade secrets can occur even at the highest levels of employees or officers of the company. That is usually where theft of trade secrets is the most damaging. For example, in *Morton v. Rank America, Inc.*, 812 F.Supp. 1062, 1073 (C.D. Cal. 1993), Defendant Robert Earl was alleged to have misappropriated trade secrets while still a director of Hard Rock Licensing Corporation. Hard Rock

asserted that Mr. Earl took those secrets and used them to start and run a competing business, Planet Hollywood. Examples of the secrets he was said to have taken included: actual and projected income, expenses and capital needs of Hard Rock Cafes and other financial information; successful and unsuccessful business strategies and methods; the suppliers who proved reliable and effective and those who have not; and the effective and ineffective methods of advertising and promotion.

When theft occurs at the highest level, it is difficult to stop. However, taking measures to protect the secrets, and making sure those with access to them know what type of information is considered confidential can help provide deterrence. It can also make it much easier to prove that the stolen information was in fact a trade secret.

Enforcing trade secrets can be very difficult. For example, if the trade secret and the steps to protect it have not been documented, it is hard to get protection. Therefore, it is very important to take steps to protect them and to document those steps. For example, hard copies of confidential information should be stamped or printed with “CONFIDENTIAL” or “TRADE SECRET” on them. Hard copies should also be kept in locked

UNIFIED
WINE & GRAPE
SYMPOSIUM

January 27-29, 2015
EXHIBITS: January 28 & 29
Sacramento Convention Center
Sacramento, California

Check our website for details on
Registration, Housing, Program
and Exhibitors.

Register early and save up to \$200!
www.unifiedsymposium.org

Unified
WINE & GRAPE
SYMPOSIUM
PRESENTED BY ASEV & CAWG

ONE PLACE, ONE TIME, ALL THE ANSWERS—
THE UNIFIED!

BY THE INDUSTRY
FOR THE INDUSTRY

cabinets or behind locked doors with appropriate limited access. Computer files should be password protected and only limited access on a need to know basis should be allowed. Additional measures of protection may include maintaining a visitor log, and making sure all employees sign a Nondisclosure Agreement (NDA). Employees should also sign an acknowledgement of the fact that the company has trade secrets, such as mailing lists, customer lists, vendor lists, wine club member lists, formulas and processes, and other trade secrets.

Every state has its own law of trade secrets. California's trade secrets act defines a trade secret as information that has value and is kept secret:

[Trade secret information includes] a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use.

(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Cal. Civil Code §3426.1(d).

Some additional categories and examples of trade secret information include:

- Computer programs and smart phone apps (including comments and flow charts)
- Business Knowledge (what works and what doesn't)
- Specifications, Bill of Materials, Formulas, Recipes, and other related information
- Methods and Processes (including flow charts)
- Formulas (including algorithms)

Distribution Sources and contact information for such sources (where they are not readily available from public sources and/or contain information such as specific names and contact information that is not readily available from public sources)

- Business Methodologies
- Employee list and potential employees
- Marketing plans
- Expansion plans and other business plans
- Customer Lists, Preferences, Wine Club Members, and Other Information
- Financial Information

Vendor and Supplier Lists (where they are not readily available from public sources and/or contain information such as specific names and contact information that is not readily available from public sources)

It is critical to proving that information is a trade secret that the business take as many of the below listed reasonable steps to protect the information:

- NDAs—get a signature by anyone who will have access to a trade secret, before they get access to it.
- Confidentiality Stamps or Legends—stamp documents confidential (or watermark it for computer files). An example of a confidential marking could simply be “CONFIDENTIAL—DO NOT DISCLOSE OR REPRODUCE,” or even just “CONFIDENTIAL.” However, don't mark everything confidential. That defeats the purpose.
- Lock Up Documents and Things—Any hard copy documents or other confidential information should be kept in a locked cabinet or locked drawer, and where necessary or appropriate, a locked room. Confidential information should not be left out on a desk unattended.
- Passwords—Password protect computerized information, e.g., key documents and key folders, and limit access by others, e.g., by keeping this information off of the network and password protecting computers. Consider encrypting files when emailing them or even when they are stored.
- Split Up Information: If possible, do not put all of the trade secret in one document or file. Split it up among two or three documents or files, especially for the most sensitive information.

TIP: *Identify your company's trade secrets. Then, take measures to protect them.*

Turning New Ideas, Names, Products & Computer Programs Into Powerful Intellectual Property

David Hoffman has been an attorney practicing exclusively in intellectual property law (patents, trademarks, copyrights and unfair competition) since 1985. Mr. Hoffman represents multinational companies as well as numerous start up to medium size businesses. He both litigates and procures rights for his clients, and with his philosophy of procuring the broadest rights possible, performing good clearance procedures, and negotiating, has successfully avoided and minimized litigation for clients he counsels.



Mr. Hoffman has taught for a patent bar review class, has authored articles and given lectures on intellectual property, and has been named to Who's Who Millennium Edition and Who's Who Among Rising Young Americans in American Society & Business.



**Hoffman
Patent
Group**

**For More Info...
661.775.0300**

www.dlhpattent.com