

# 9th Circuit Ruling Gives Owners of Famous Trademarks a Boost

By Craig Anderson  
Daily Journal Staff Writer

Owners of famous trademarks got some good news from the 9th U.S. Circuit Court of Appeals on Tuesday when a three-judge panel revived Levi Strauss & Co.'s trademark dilution lawsuit against Abercrombie & Fitch Trading Co. over Levi's familiar blue jeans logo.

In its decision, the appellate panel overturned a San Francisco federal judge's 2009 ruling dismissing the Levi's trademark lawsuit over a similar stitching design on the back pocket of Abercrombie's jeans. The case was remanded to U.S. District Judge Jeffrey S. White.

Abercrombie still could defeat

the Levi's lawsuit, but now must do so under a different legal standard established in a federal law, the Trademark Dilution Revision Act of 2006.

"It is good for owners of famous marks," said John W. Crittenden, a San Francisco-based partner with Cooley LLP who is not involved in the case, although his firm represents Levi's in other matters.

Under the old standard, based on a previous version of the law, Levi's had to prove the Abercrombie mark was identical or nearly identical to the familiar arching design on the back pocket of its blue jeans.

An advisory jury concluded that the Abercrombie design was not identical or nearly identical, and

White agreed, ruling that it failed to cause trademark dilution.

But the 9th Circuit, following

'The plain language of [the 2006 law] does not require that a plaintiff establish the junior mark is identical, nearly identical or substantially similar to the senior mark in order to obtain injunctive relief.'

— Judge Kenneth A. Ripple

on the heels of a similar ruling by the 2nd U.S. Circuit Court of Appeals last year in a case involving Starbucks Corp., ruled that White was following an outdated legal

standard.

Under the new law, plaintiffs can prevail if a defendant's name or de-

and the famous mark; the mark's distinctiveness; the degree of recognition of the mark; and whether the defendant intended to create an association with the famous mark.

"Thus, the plain language of [the 2006 law] does not require that a plaintiff establish the junior mark is identical, nearly identical or substantially similar to the senior mark in order to obtain injunctive relief," Judge Kenneth F. Ripple wrote in the decision.

"Rather, a plaintiff must show ... that a junior mark is likely to impair the distinctiveness of the famous mark," he added. *Levi Strauss & Co. v. Abercrombie & Fitch Trading Co.*, 09-16322.

Gregory S. Gilchrist, a San Fran-

cisco-based partner with Kilpatrick Townsend & Stockton LLP who represents Levi Strauss, said he was "re-ally gratified to see the outcome."

Gilchrist said he was not surprised by the decision, saying it is consistent with the changed legal standards regarding trademark dilution in the 2006 federal law. "I think it has particular importance in the context of a design mark," he said.

"We do believe [Levi's stitching design] is eroded by similar but not identical marks," Gilchrist added.

J. Michael Keyes, a Spokane, Wa.-based partner with K&L Gates LLP, said he had not had a chance to read the ruling as of press time.

craig\_anderson@dailyjournal.com

# New Electronic Data Privacy Laws Protect Businesses and Consumers

By Diane L. Becker

Technology has changed the way we do business in the 21st century and changed the way we think about electronic data privacy and security. Businesses are no longer concerned solely about keeping people out of computer data, but also about letting the right people into the data and about the ability to use and share data in a legal manner. Increasing regulations and new laws in 2011 will force businesses to review the handling of private information including electronic data, and require them to implement new programs to minimize their legal risks.

The Federal Trade Commission (FTC) has enacted new rules known as the "Red Flag Rules" pursuant to Sections 114 and 315 of the Fair and Accurate Credit Transactions (FACT) Act of 2003. These rules require businesses that maintain certain types of "covered accounts" to develop and implement written identity theft prevention programs, designed to identify, detect, respond to, prevent and mitigate identity theft. The program is intended for "creditors" with "covered accounts" to detect "red flags," which are patterns or activities that indicate the possible existence of an identity theft threat. The regulations provide that each program be tailored to the specific business entity, and that there is no "one size fits all" solution.

Increasing regulations and new laws in 2011 will force businesses to review the handling of private information including electronic data, and require them to implement new programs to minimize their legal risks.

The FTC delayed enforcement of the Red Flag Rules until Jan. 1, 2011. On Dec. 18, 2010, President Barack Obama signed a law narrowing the definition of which businesses are "creditors" to which the rules will apply. The Red Flag Rules now apply to businesses that "regularly and in the ordinary course of business" obtains or uses a credit report, furnishes information to a credit reporting agency, or advances funds to another. The full definition of a creditor is set forth at 15 U.S.C. Section 1681m(e)(4)(A). The goal of the amendment, according to Sen. Chris Dodd, was to clarify that "lawyers, doctors, dentists, orthodontists, pharmacist, veterinarians, accountant, nurse practitioners, social workers, other types of health care providers and other service providers will no longer be classified

as creditors for purposes of the Red Flag Rules, just because they "do not receive payment in full from their clients at the time they provide services." Many businesses including some service companies, are subject to this new law and will need to develop and implement a program immediately.

In order to adopt a program, a business will first need to determine whether it maintains a "covered account." The business must then identify red flags for the covered account, by examining all data entry points of the covered account and determine what red flags would be relevant to those points. A business must draft a written program that describes how the identified red flags will be detected and addressed, in a manner that it is appropriate for the specific red flag.

Next, written policies and procedures must be drafted to prevent and mitigate identity theft. This includes responses to red flags.

Finally, the business is required to update the program's policies and procedures periodically and provide for effective oversight by conducting a risk assessment on at least an annual basis to determine whether the program needs to be updated due to changes in the risks to the business.

In addition, users of consumer reports are required to develop and prevent policies and procedures to address discrepancies. To be effective and to comply with the Red Flag Rules, a board or a senior management employee needs to provide oversight over the program. Also, employees must be trained on how to spot red flags and how to address them. Service providers that may have access to covered accounts (such as a billing company) need to have an appropriate program in place.

Another important law called "Do Not Track" is aimed at behavioral advertising or behavioral targeting, which uses technologies to anonymously track and tabulate consumer online activities. Cookies are used to monitor and track Web habits including Web site visits, the length of time spent on Web pages, and the content viewed. While the consumer information collected may not seem to be personally identifiable, as it generally does not identify individuals by name or address,

the practice has the ability to collect and allocate extensive amounts of personal information. The inventory of data collected by behavioral advertising is analyzed in order to predict a consumer's future behavior and target future advertising consumer based on their Web searching history.

Behavioral advertising is a wide spread practice used by Web publishers, Internet marketers and service providers to increase the effectiveness of their advertising campaigns by tracking consumer activities online, and it is a very important component of many companies' marketing strategies. The FTC and Congress have been closely monitoring this

create policies for securely handling location-based information. With the rise of tracking by security cameras, traffic light cameras, mobile communication device and vehicle GPS information, companies must protect personal identifiable location-based information of employees, customers and business associates. Companies that have access to information concerning where people spend their time and where they can be located at a given time, will need to develop formal written policies to treat this information as confidential for security and privacy reasons.

Additionally, companies are moving to encrypt increasing amounts of data, and are implementing more reliable ways to send files securely. As a result, companies are creating more acceptable use policies as they tailor them to their content and the need to protect sensitive data. Many businesses are also beginning to use innovations such as Facebook, Twitter and other social networks for marketing purposes. In order to use these innovations safely and effectively, companies need to implement better security policies and technology controls on their corporate e-mail systems, as they move away from outright bans on social networks, instant messaging, and webmail. Due to the risk of damage to a business through social network communications, companies are applying stricter corporate policies and are increasing the security of their Web gateways. At the same time, companies are learning the risk of damage to the reputation of the company and its employees, loss of private personal information and loss of confidential information.

To avoid these problems, companies are developing written social media policies and are enforcing these policies through both technology and training.

In today's legal risk environment, it is important that companies create written electronic data privacy and security policies that are in compliance with current law. Businesses are also wise to consider the use of encryption, acceptable use policies, Web filtering and secure data management and transfer procedures.

issue and the FTC has set regulatory guidelines for online behavioral advertising.

In response to the "Do Not Track" law, the FTC recommended recently that industry adopt "privacy by design" principles (the internal company procedures to protect consumer privacy), in the design and development of a company's products and services, and in its marketing and tracking activities. The FTC also wants to make consumer data more available, which will allow for increased consumer access to the data that is being collected, stored, and disseminated about them. Entities that are collecting consumer data should be setting up internal procedures and rules that will provide consumer privacy compliance and protection, but at the same time still allow the business to continue to collect the data, and also review all applicable FTC guidelines and industry standards to remain legally compliant.

In today's environment, the use of mobile devices with personal identifiable locations emphasizes the need for confidentiality policies relating to location-based information. Companies will need to



**Diane L. Becker** is a partner at Nordman Cormany Hair & Compton LLP. She is chair of the firm's General Counsel Services Practice Group and the Corporate and Business Practice Group. She can be reached at dbecker@nchc.com or (805) 988-8307.

## 2011 Holiday Calendar

	Daily Journal	California Superior Courts	State Offices	California Appeals Courts, Supreme Court	U.S. Courts & Offices	Federal Reserve	Los Angeles City Offices	Los Angeles Law Library	Los Angeles/San Francisco County Offices	San Francisco Law Library	San Diego County Offices	San Diego County Law Library	Orange County Offices	Orange County Law Library	Post Office, Banks
■ <b>New Year's Day</b> Friday, Dec. 31 2010 (Observed)	Closed	Closed	Closed	Closed	Closed	Open	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Martin Luther King Jr. Day</b> Monday, Jan. 17	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Lincoln's Birthday</b> Friday, Feb. 11 (Observed)	Open	Closed	Open	Closed	Open	Open	Open	Open	Open	Open	Open	Closed	Closed	Open	Open
■ <b>Presidents Day</b> Monday, Feb. 21	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>César Chávez Day</b> Thursday, March 31	Open	Closed	Closed	Closed	Variable <sup>1</sup>	Open	Closed	Open <sup>9-4</sup>	Open	Open	Closed	Closed	Open	Closed	Open
■ <b>Memorial Day</b> Monday, May 30	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Independence Day</b> Monday, July 4	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Labor Day</b> Monday, Sept. 5	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Columbus Day</b> Monday, Oct. 10	Open	Closed	Closed	Closed	Closed	Closed	Closed	Open <sup>3</sup>	Closed	Closed	Open	Closed	Closed	Open	Closed
■ <b>Veterans Day</b> Friday, Nov. 11	Open	Closed	Closed	Closed	Closed	Closed	Closed	Open <sup>9-4</sup>	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Thanksgiving</b> Thursday, Nov. 24	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed
■ <b>Day After Thanksgiving</b> Friday, Nov. 25	Open	Closed	Closed	Closed	Variable <sup>2</sup>	Open	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Open
■ <b>Christmas Day</b> Monday, Dec. 26	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed <sup>4</sup>	Closed

<sup>1</sup> U.S. District Court and U.S. Bankruptcy Court for the Southern Districts will be closed.

<sup>2</sup> U.S. District Court and U.S. Bankruptcy Court for the Northern, Central, and Southern Districts will be closed.

<sup>3</sup> Branches will be closed.

<sup>4</sup> Library will also be closed Christmas eve.