Law Office of Edward E. Sharkey LLC



**June 2014**

# BUSINESS LAW DEVELOPMENTS

Legal updates for entrepreneurs and business owners from the Law Office of Edward E. Sharkey LLC.

Dear Friends of the Firm,

This is the June issue of our firm's newsletter, featuring coverage of legal developments important to business owners and entrepreneurs. You are receiving it because you are a client or have previously solicited legal resources from the firm.

Please let us know what you think.

Very truly yours,

Ed

---

## In This Issue



---

## Addressing Data Theft By Employees

Businesses struggle with the challenge of employee data theft pretty frequently. It often occurs when an employee leaves and takes a customer list or proprietary information along with him to a competing business. One legal tool available to businesses in most states is the Uniform Trade Secrets Act (“UTSA”). Maryland, Virginia, and the District of Columbia have all adopted the UTSA.

The UTSA creates a cause of action against a person who misappropriates another’s trade secret. A trade secret is any information that a business works to keep secret and which is valuable precisely because it is not generally known or readily ascertainable by other persons. Under the UTSA, a trade secret can be misappropriated in two ways:

1. Improperly acquiring the trade secret, such as by theft, misrepresentation, or espionage; or
2. Disclosing or using the trade secret.

A recent case decided by the Federal District Court for the Eastern District of Virginia highlights one reason why employers like the UTSA: an employer does not even have to prove that the employee actually disclosed or used the stolen trade secret in order to pursue a claim for misappropriation.

The case concerned the taking of trade secrets by an employee who was told she was fired, effective at the end of the year. Between the notice and the end of the year, the employee downloaded the employer's data onto an external storage device and emailed it to her personal account. The employee did not have authority to download or email the data.

The employer sued the employee under the Trade Secrets Act in Virginia. The employee asked the court to dismiss the claim, in part because the employer could not prove that the employee actually used or disclosed the data. The court rejected the employee's request. In doing so, the court made clear that, to make a claim for misappropriation, an employer need not prove that an employee disclosed or used the employer's trade secrets. It is enough that the employee acquired them through improper means.

Where the data at issue does not meet the legal definition of a trade secret, employers in some states can take advantage of the Computer Fraud and Abuse Act ("CFAA"). The CFAA creates a civil cause of action against a person who, among other things, accesses another's computer system or network without proper authorization or exceeds authorized access.

Employers in some jurisdictions have successfully argued that an employee acts beyond the scope of his authority by taking and using information in violation of company policy. In other jurisdictions, courts have rejected these types of claims. In doing so, these courts hold that the CFAA is meant to address computer hacking and other unauthorized access, not the misuse of information an employee was authorized to access. The court in Maryland's federal circuit, the Fourth Circuit, takes this more narrow view of the CFAA.

For employers in jurisdictions like the Fourth Circuit, and for cases where the data does not meet the legal definition of a trade secret, traditional state law claims are still available. The takeaway is that there usually are options for dealing with employee theft of confidential information. For many of those claims, clear company policies that concern access to, acquisition of, and use of company data are helpful. This means a company will benefit from having an employee manual that deals explicitly with the security and disposition of company data.

---

## Businesses That Suffer Breaches of Credit Card Information May Be Liable to Card Issuers

Data breaches afflicting ordinary businesses are becoming more frequent. Over the past few months, we have devoted a lot of attention to the legal issues businesses face when they experience a data breach. We have looked at the potential for civil liability to customers, fines that may be assessed by regulators, and coverage disputes that may arise with insurers.

In addition to these risks, businesses that suffer a breach of information concerning customers' debit and credit cards may also find themselves in litigation with the financial institutions that issued the cards. Target, in the news for a massive breach of its customers' information, found itself defending

such a lawsuit.

Generally, it will be a lot easier for card issuers than for customers to prove compensable damages caused by a data breach. This is because issuers incur costs to stop the fraudulent use of information that was exposed by the breach. For example, they issue new cards to affected customers and credit unauthorized purchases back to customers' accounts. The issuers' losses are, typically, very large. In the Target case, for instance, the banks estimated the cost of reissuing compromised cards would be more than $150 million.

Businesses collecting personally identifying information must remember to take steps to protect themselves. They must review whether they are properly insured for all the harm a data breach might cause, including harm to card issuers. They must also implement reasonable security measures and policies to prevent against data breaches in the first instance.

---

## Can My Business Be Sued for Enforcing a Dress Code?

Most businesses enforce some standard of dress. Some do so to promote their brand and image. This is why Target employees wear red shirts and Walmart employees wear blue. Other employers enforce policies in an effort to safeguard their workers. It seems logical, for instance, to ask that machinists refrain from wearing long necklaces to work.

This can create an issue when an employee requests an exception for religious reasons. Many religions encourage their followers to wear particular articles, not wear certain types of clothing, or to observe specific grooming habits.

Title VII, which prohibits religious discrimination in employment, requires employers to reasonably accommodate employees' religions, including by making some exceptions to dress and grooming codes. The difficulty for employers is deciding when an exception is required and when the employer's rule may lawfully be enforced.

The EEOC, the federal agency tasked with enforcing Title VII, recently issued guidelines, available at http://tinyurl.com/kdduotr, intended to help employers faced with this decision. Although the EEOC instructs that employers are required to accommodate employees by excusing them from dress rules in most instances, it does recognize that accommodations are not always required.

Some of the most important takeaways for employers are that:

- Title VII protects all types of religious beliefs, including those that are not mainstream and those which an employee has held for only a brief time;
- It is illegal to reassign or move an employee out of the view of customers because of his or her religious dress;
- "Customer preference" is not a justification for refusing an exception;
- Employers are required to make an exception unless the exception would cause an "undue hardship;" and
- Determining whether a particular exception would create "undue hardship" calls for a case-by-case assessment of all the circumstances.

Every business should bookmark the guidelines for reference if such issues ever arise. And, every business should review its policy to ensure that it allows for exceptions to accommodate employees'

religions.

## ABOUT US

The Law Office of Edward E. Sharkey LLC is a firm of dedicated business and trial lawyers in Bethesda, Maryland, concentrating on business law and commercial litigation. Other areas of practice include pension, securities, negligence/professional liability, and construction law.

Disclaimer: This message and any attachments hereto cannot be used for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.

This publication is provided for information purposes. It should not be taken as legal advice for a specific situation. If you need legal advice concerning a business or litigation matter, please seek legal counsel or contact us for a consultation at (301) 657-8184.



In This Issue

Law Office of Edward E. Sharkey LLC
4641 Montgomery Avenue
Suite 500
Bethesda, MD 20814
www.sharkeylaw.com

Tel. (301) 657-8184
Fax (301) 657-8017
Business Hours:
9 a.m. - 5 p.m.
Monday - Friday

**ATTORNEYS**

Edward E. Sharkey
Admitted to Practice in
Maryland and Washington, DC

Jeanine Gagliardi
Admitted to Practice in
Maryland and Washington, DC