BEYOND *the* NUMBERS

A Roundup of Business and Tax Planning Ideas

JANUARY / FEBRUARY

In This Issue

A New Kind of Employee Theft: Is Your Company Vulnerable?

by David Leffler, Esq. and Seth Marcus, Esq.

EMPLOYERS EVERYWHERE are fearful of a new kind of employee theft — theft of computer data. Taking a few cartons of goods is nothing compared to a dishonest employee emailing your competitor a key customer list or top secret plans to enter into a new market. With a couple of clicks, your most valuable data could be out the door.

Technology solutions to control this situation are often expensive and difficult to implement. However, there is a little known federal statute that can provide relief at a much lower cost.

The Computer Fraud and Abuse Act (CFAA) is a federal statute that was originally passed in 1984 to criminalize particular types of "unauthorized access" to certain information stored on government and financial institution computers.

In 1994 a provision for a civil cause of action was added to the CFAA, which meant that in addition to criminal sanctions, businesses could bring a lawsuit for damages and injunctive relief. Thus was born a new tool for some businesses to protect their data.

The CFAA was greatly expanded in 1996 to include all computers involved in interstate and foreign commerce, which, in these days when most computers are hooked up to the Internet, includes almost all computers. This opened the CFAA as a remedy for any type of business, provided the requirements of the statute are met.

Advantages of the CFAA

Pursuing CFAA claims when a company finds itself the victim of theft of its trade secrets and confidential information can provide several advantages not available under State law alone. While not a comprehensive list, some of these advantages are as follows:

David Leffler, Esq.

Seth Marcus, Esq.

1. Avoiding the problem altogether.

Arranging an employee seminar conducted by company counsel that reviews the CFAA and the consequences of violating its provisions is a powerful tool to reduce a company's vulnerability to employee theft of data. Such a seminar informs employees that obtaining the company's confidential proprietary information through unauthorized access of its computers is a criminal act under Federal law.

When confronting potential criminal law sanctions, most employees will not be willing to take the risk. Of all the remedies discussed here, this can provide the strongest and most cost-effective defense against such vulnerabilities.

2. The CFAA is a criminal statute.

If the harm to the company is sufficiently large or the potential damage that can be inflicted by the conduct that the company has been a victim of could potentially extend beyond the company, counsel may consider pursuing a criminal complaint, either as an alternative to or concomitant with seeking civil remedies. Such a course,

(continued on page 6)

A New Kind of Employee Theft: Is Your Company Vulnerable? *(continued)*

particularly if there is an actual criminal prosecution, sends a clear message that the company takes the protection of its confidential and proprietary information seriously. However, even if the company chooses to use the CFAA for purely civil relief, defense counsel and the defendant will still be aware that there is a criminal statute at issue in the case and the possibility of a criminal prosecution may encourage them to settle more quickly.

3. Easier standards of proof.

It may be easier to establish a valid CFAA claim than it is to establish claims under traditional State law protections of confidential and proprietary information and trade secrets. Typical State law claims require the company to carry the burden of proving a laundry list of items that often include, among other things: (1) that it took affirmative steps to maintain the confidentiality of the information; (2) that the information was somehow unique to the company; and (3) that the information had economic value to the company's business.

Instead of focusing on the steps the company took to maintain confidentiality, the CFAA focuses on whether access to the computer was authorized or not, which could be a far easier to show. Such simplification could be a tremendous advantage, particularly as the most important remedy being sought in such cases is the injunction on the use of the illicitly obtained information. Moreover, the injunction is usually sought as a pre-judgment remedy, which imposes the burden on the company that it must demonstrate to the court that it will likely win the case before the company has had the opportunity to do any discovery. The simpler and more straight-forward the claim (as afforded by the CFAA), the greater the likelihood of success.

4. Greater choice as to where to litigate.

Because the CFAA is a Federal Statute, asserting CFAA claims provide the company with the alternative of bringing its action in Federal as opposed to State Court. As a Federal Court may exercise jurisdiction over State claims when they have the same core of relevant facts as a Federal claim, the company can go to Federal Court without surrendering any remedies that may be available under State but not Federal law. Whether or not the company would ultimately want to go to Federal rather than State Court involves a case-specific strategic analysis. However, if it is deemed advantageous, the CFAA could provide a ticket to Federal court that would not otherwise exist.

Summary of the CFAA

Broadly speaking, the CFAA prohibits the following:

1. Obtaining information from a protected computer without authorization if the conduct involves an interstate or foreign communication;
2. Obtaining something exceeding $5,000.00 in value from a protected computer after accessing it without authorization with an intent to defraud;
3. Causing "impairment to the integrity or availability of data, a program, a system, or information," after accessing a protected computer without authorization.

The term "protected computer" is defined broadly to include any computer "which is used in interstate or foreign commerce or communication."

In addition, the lawsuit must demonstrate losses to the company aggregating at least $5,000.00 during a 1-year period. Here a question arises as to whether this "loss" requirement can be met by asserting losses attributable to things like the value of the proprietary information misappropriated, lost profits from unfair competition, or lost goodwill of the business.

A recent court decision suggests the answer to this question is no. It has been held that the "loss" referred to in the CFAA must be directly related to the computer. Thus, the cost of items such as diagnosing and repairing damage done to the computer, interruption of computer service, and restoring or altering security measures are clearly losses contemplated by the CFAA.

However, other courts have taken a broader view, suggesting that items such as lost goodwill or the value of the misappropriated property can be used to establish the "loss" requirement of a civil CFAA action. Moreover, the narrow reading is not required by the applicable statutory language, which includes "consequential damages incurred because of interruption of service" in the definition of "loss."

If a CFAA claim is successfully established the Act authorizes both compensatory damages and, when appropriate, injunctive relief. Injunctive relief can include items like a court order prohibiting the party who illegally obtained a company's data from making use of it. MK

David Leffler and Seth Marcus are members of the New York City law firm Leffler Marcus & McCaffrey LLC, which represents clients in business matters and commercial litigation. You can write to them at dleffler@lmmlawfirm.com and smarcus@lmmlawfirm.com, respectively.

Putting "Strategy" into Your Strategic Alliances *(continued)*

disagreements become intractable, how (court or ADR?) and where (geographically) will they be resolved? Thinking this through in advance could have prevented the souring of Colin's relationship with Themis.

Strategic alliances are all the rage. But like all other business relationships, and as Colin learned the hard way, they require careful forethought to make sure they are the right fit. And the input of accounting and legal advisors won't hurt either. So before you become bamboozled by the jargon, make sure that there is a viable strategy behind every strategic alliance you create. MK

Nina L. Kaufman is a founding partner of award-winning Paltrowitz & Kaufman LLP, www.palkauf.com, a New York City law firm providing wise counsel for growing businesses® on many of their transaction and litigation needs. Kaufman is also the President of Wise Counsel Press LLC, which sells booklet guides on legal issues for small businesses. For more information, contact WiseCounsel@palkauf.com. This column is for your general information only and is not meant to substitute for legal or accounting advice regarding your specific situation.