2006 Guide to Trial Support Services

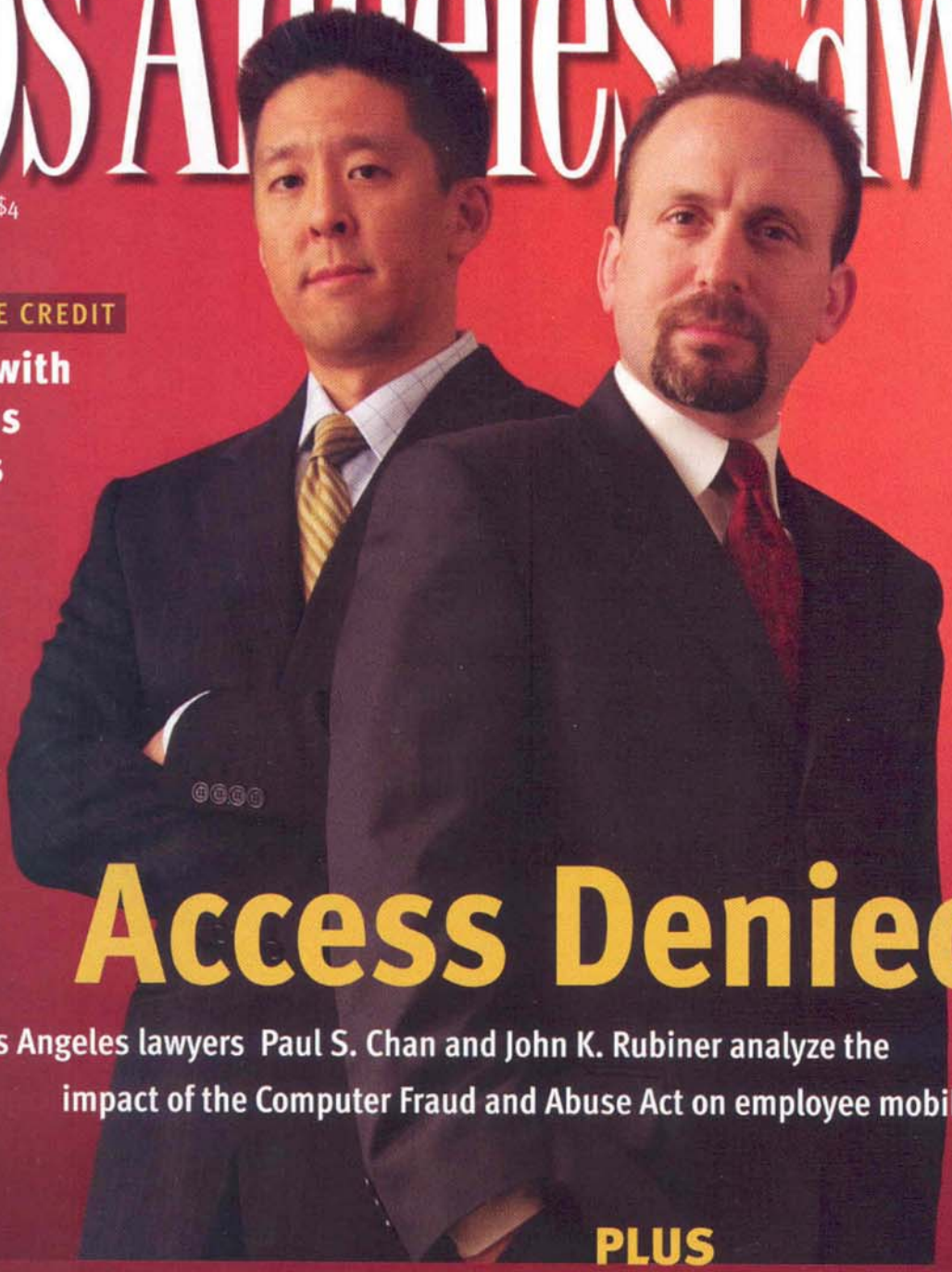
Podcasting for Lawyers
PAGE 47

Los Angeles Lawyer

February 2006 / $4

EARN MCLE CREDIT

Dealing with Vexatious Litigants
page 29



Access Denied

Los Angeles lawyers Paul S. Chan and John K. Rubiner analyze the impact of the Computer Fraud and Abuse Act on employee mobility page 22

PLUS

Labor Code Enforcement Actions page 13

Real Property Reassessments page 18

Defamation in Employee References page 34

Claims brought under the CFAA have a less daunting burden of proof than that required by the Trade Secrets Act

ACCESS DENIED

by Paul S. Chan and John K. Rubiner

The Computer Fraud and Abuse Act (CFAA)[1] is a sweeping federal statute that prescribes criminal and civil penalties, including injunctive relief, to halt the unauthorized accessing of computer information. Once confined to cases involving hackers and viruses, in recent years the CFAA has become a powerful litigation tool for employers seeking to exert continuing control over departing employees—and subject the hiring practices of their competitors to judicial scrutiny.

Under the right circumstances, the CFAA enables employers to obtain injunctive and monetary relief against a departing employee—and his or her new employer—without having to confront many of the procedural and evidentiary hurdles posed by traditional trade secrets and unfair competition laws. Among other things, an employer suing under the CFAA can bring its action in federal court; need not necessarily prove that the information accessed by the former employee was a trade secret; and need not show that the defendant is actually using, or threatening to use, the information. Additionally, the CFAA has teeth even in California, where covenants not to compete are disfavored. Indeed, an employer who can establish a CFAA violation may be able to effectively enjoin a former employee from working.

But the comparative ease with which the CFAA can be utilized by companies seeking to rein in departing employees is a double-edged sword. In a world in which information is transmitted instantaneously and employees can change jobs almost as quickly, every company that has a serious interest in protecting its competitive computer information is equally at risk of being accused of stealing someone else's. Liability under the CFAA is not limited to cases of intentional theft or industrial espionage. Every time a departing employee accesses information from a current employer's computers after accepting employment at a new firm, or downloads materials from company computers and forgets to return them before starting a new job, the former employee and the new employer face a risk of exposure to the CFAA's criminal and civil penalties.

The CFAA was enacted in 1984 to protect classified information as well as financial and credit information on government and finan-

Paul S. Chan is a partner and John K. Rubiner is counsel at Bird, Marella, Boxer, Wolpert, Nessim, Drooks & Lincenberg, PC, a Los Angeles firm specializing in business and employment litigation and white collar criminal defense.

KEN CORRAL

cial institution computers.[2] In 1986, the CFAA was amended to provide additional criminal penalties for fraud and related activities affecting "federal interest computers."[3] The Computer Abuse Amendments Act of 1994 added civil remedies, which allow any person who suffers damages or loss resulting from a violation of the CFAA to maintain a civil action against the violator for compensatory damages and injunctive relief.[4]

The scope of these civil remedies was dramatically expanded in 1996 when Congress extended the reach of the CFAA to cover not only governmental computers but also any "protected computer," which was defined to include any computer "which is used in interstate or foreign commerce or communications."[5] Virtually all modern computers can be used now for interstate or foreign communications via the Internet. Thus the CFAA has evolved from a statute that originally concerned only the federal government's interest in specific computers to a law that now covers practically every computer in the United States.

To establish liability under the CFAA, the plaintiff must show that the defendant 1) either fraudulently or "intentionally" accessed a protected computer "without authorization or [in excess of] authorized access," and 2) as a result of this conduct, caused damages of at least $5,000.[6]

"Access" is defined broadly. For example, one court held that a competitor's use of a "scraper" software program to methodically glean prices from a tour company's public Web site, in order to allow systematic undercutting of those prices, exceeded the authorized access otherwise allowed to Web users.[7] Similarly, in America Online, Inc. v. National Health Care Discount, Inc.,[8] a case concerning a defendant who sent e-mail spam, the court held that the CFAA's prohibition against "accessing" computers is violated when someone sends an e-mail message from one's own computer that is then transmitted through other computers (without permission) until it reaches its destinations.

The concepts of "damage" and "loss" are also broadly defined. Congress defined "damage" under the CFAA to mean "any impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals."[9] The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[10] Because the costs involved in adding security and replacing software following an unauthorized access can constitute losses under the statute, the $5,000 loss or damages threshold can be met in most commercial situations. Indeed, the costs for a forensic computer investigation alone will almost always surpass $5,000. For example, in EF Cultural Travel BV v. Explorica, Inc.,[11] the court held that a company's payment of consultant fees for the purpose of assessing whether its Web site had been compromised was a compensable loss under the CFAA, even though there was no physical damage to the company's data or systems.[12]

Most all the initial CFAA cases involved efforts by computer information owners to obtain redress against hackers and spammers who had unlawfully accessed the protected computer database of another for either personal or competitive business purposes.[13] In recent years, however, employers have increasingly seized upon the CFAA as a litigation tool to exert continuing control over departing employees.

Pleading and Proof

Shurgard Storage Center v. Safeguard Self Storage[14] was the first reported decision involving an employer's attempt to state a CFAA claim against a former employee and its business competitor. In Shurgard, the plaintiff and the corporate defendant were competitors in the self-storage business. The plaintiff alleged that the defendant embarked on a systematic scheme to hire away key employees for the purpose of obtaining the plaintiff's trade secrets, and that some of these employees—while they were still employed by the plaintiff but after they had already met with the defendant and had started acting as the defendant's agents—used the plaintiff's computers to send e-mail to the defendant containing the plaintiff's trade secrets and proprietary information.

The defendants moved to dismiss, challenging the scope of a civil claim under the CFAA. The district court denied the motion after finding that the employees' access to the plaintiff's computer was "without authorization," according to the CFAA's use of that term. The court held that even though the employees were still employed by the plaintiff at the time they sent the e-mail, each employee was alleged to have accessed the computer "as an agent" for the defendant. The employees therefore lost the authorization they otherwise had to use the former employer's computer even while they were still employed.[15]

The defendants in Shurgard also argued that the CFAA only applies to information that, if stolen, "could affect the public," and the information from the storage business is not the type of information that the CFAA was intended to protect. The court rejected this argument, finding that the CFAA is "unambiguous" in applying to "any protected computer if the conduct involved an interstate or foreign communication."[16]

The Shurgard court dealt only with the pleading requirements for asserting a CFAA claim. A later case, U.S. Green ber v. Brooks,[17] addressed the CFAA's proof requirements and the showing a plaintiff must make to obtain injunctive relief. The case involved fairly outrageous conduct by a former employee. The defendant, a quality control manager, worked out of her home and kept numerous company documents there. On the day she was terminated, the defendant accessed the company's e-mail system and took various corporate documents from the company, then later accessed the company's computer communications system to solicit other employees.[18] In light of the defendant's blatant refusals to return the company's materials and her post-termination conduct, the court found that the plaintiff was likely to succeed on the merits of all its claims and issued a preliminary injunction. The injunction specifically directed the defendant to return the plaintiff's property and enjoined the defendant from using or disclosing confidential information or soliciting the plaintiff's employees using the plaintiff's communications systems. Notably, the injunction did not prevent the defendant from actually working for a competitor—it focused only on the defendant's use of information.[19]

In Paci c Aerospace & Electronics, Inc. v. Taylor,[20] the plaintiff sued its former employees and their new company alleging violations of the CFAA, misappropriation of trade secrets, and other violations of Washington state law. The district court held that it was appropriate for employers to utilize the CFAA in federal court to sue former employees (and their new companies) who seek a competitive edge through the wrongful use of information taken from their former employer's computer system.[21] After determining that it had jurisdiction based on the plaintiff's allegations of violation of the CFAA, the court then ordered a preliminary injunction based on the plaintiff's claims for misappropriation of trade secrets under the Washington Uniform Trade Secrets Act, breaches of confidentiality, and violations of various common law duties.[22]

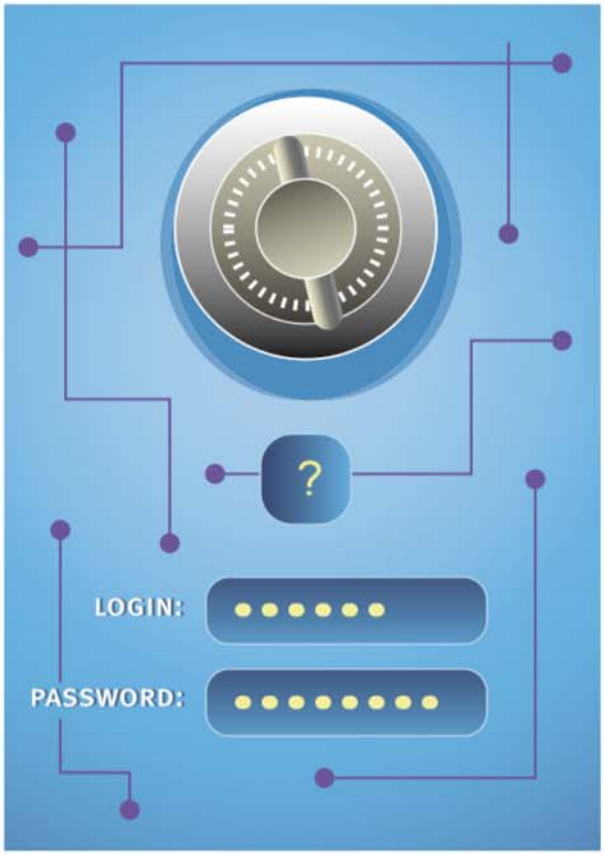
Comparing CFAA Claims to Other Actions

As these cases highlight, the CFAA offers a number of potential advantages to employers seeking to regulate the conduct of former employees. Among other things, an employer suing under the CFAA may 1) bring its action in federal court, 2) face more liberal plead-

ing and proof requirements than under traditional unfair competition laws, and 3) obtain potentially broader injunctive relief.

In employment cases involving the unauthorized access of protected computer information, the CFAA gives federal courts jurisdiction over employee mobility disputes that would otherwise be restricted to state court unfair competition actions. The availability of federal jurisdiction can be a marked advantage for plaintiff employers in cases that would otherwise be governed by state laws and procedures favorable to employees.

For example, because of the strong public policy in California in favor of employee mobility, most noncompetition agreements are unenforceable under California law.[23] California also does not recognize the doctrine of "inevitable disclosure"[24] with respect to trade secrets misappropriation, making the use of the CFAA—and its federal forum remedies—an attractive alternative to state court. An employer whose employment relationship with a former employee would otherwise be governed by California law has the option of avoiding these restrictive state court doctrines if it can state a federal claim under the CFAA.



In many cases, the CFAA's pleading standards will be easier to satisfy than those required to state claims for trade secrets misappropriation or breach of employment contract. There is no requirement that the plaintiff allege the existence of actual trade secrets or the misappropriation or unauthorized use of those trade secrets. There is no requirement that the plaintiff allege the existence of an enforceable noncompetition agreement. Nor is there any requirement that the plaintiff allege the existence of an enforceable confidentiality agreement or the use of measures to maintain the confidentiality of the information at issue.

To state a claim under the CFAA, all an employer need allege is that 1) a former employee was acting as an agent for the new employer, 2) the former employee was doing so at the time he or she accessed a company computer without authorization, and 3) this unauthorized access caused at least $5,000 in losses. The allegations involving agency and access often can be satisfied when an employee continues working at the current employment for a period of time after an interview with, or job offer from, another employer, and accesses a protected computer during the interim period for nonwork purposes. These circumstances are fairly common in today's workplace.

Assume, for example, that an employee interviews and accepts a position with a new company but continues to work for the former employer for a few weeks. In that period the employee downloads information from the former employer's computers or otherwise accesses the former employer's computers. If the former employer can demonstrate a good faith belief that specific instances of accessing the computer system by the employee after accepting the new position (or even after the first interview with the new employer) were for the benefit of the new employer and not the former employer, the employer may allege that the employee's actions constitute a violation of the CFAA. As a practical matter, the departing employee will then need to respond to each alleged instance of improper access by showing that he or she accessed the former employer's computer to further the employee's job duties for the former employer and not to benefit the new employer in any way. This showing may not necessarily be easy to make in situations in which the departing employee cannot articulate legitimate, work-related reasons for each and every time the employee accessed the former employer's computers.

Finally, the allegation of loss can be satisfied as long as the employer can allege, in good faith, that the injury from the unauthorized access exceeds the jurisdictional amount. In most instances, it will not be difficult to allege that the injuries resulting from unauthorized disclosure of the accessed information exceed $5,000, especially since remedial expenses have been deemed to constitute losses.

In California, an employer seeking to state a claim for misappropriation of trade secrets against a departing employee or the new employer (or to enforce a noncompetition agreement to the extent that it prohibits the disclosure of trade secrets) must establish, at a minimum, that the misappropriated information constituted trade secrets. The Uniform Trade Secrets Act (UTSA) defines a "trade secret" as information, including 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, and

2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[25]

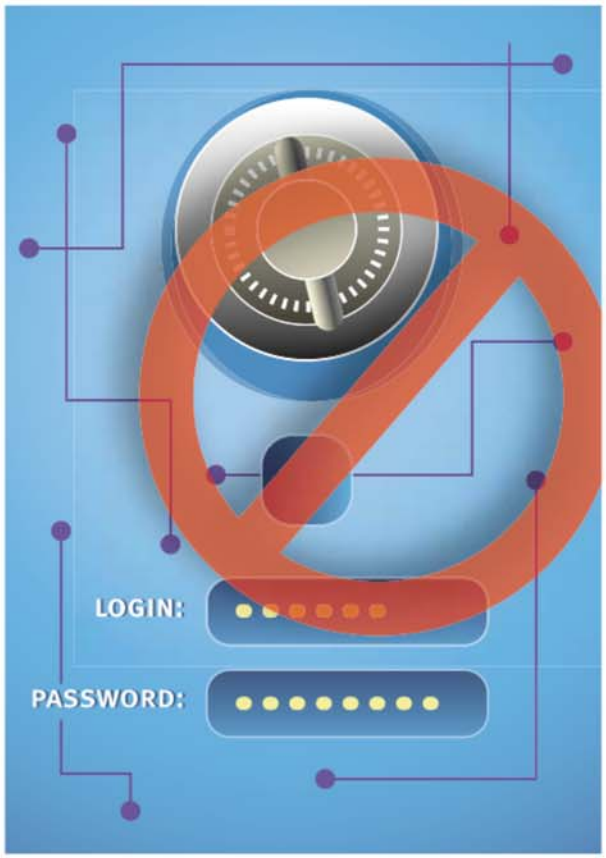
Alternatively, an employer may state a claim of breach of a confidentiality agreement by a departing employee. The former employer must prove 1) the existence of a valid and enforceable confidentiality or nondisclosure agreement, and 2) that the information allegedly disclosed constituted confidential information, for which there were reasonable efforts made to ensure its confidentiality.

By contrast, to prove a CFAA claim there is no requirement that the accessed information be a trade secret or even confidential. Moreover, a plaintiff is not required to allege the existence of a valid confidentiality or noncompetition agreement. All that is required to prove a CFAA claim is the showing that an unauthorized computer access caused a loss in excess of $5,000. CFAA claims therefore can apply to a much broader range of cases involving the unauthorized access of computer information. For example, an employer may devote substantial resources toward the research and development of a new project but—because of carelessness or oversight—not place sufficient emphasis on maintaining the confidentiality of the project. The employer may fail to have employees sign confidentiality agreements or institute other measures to maintain the secrecy of the project. If a departing employee intentionally accesses computerized information for the benefit of a new employer and then leaves with the information, the former employer may have a difficult time establishing that the accessed information was a trade secret or subject to sufficient confidentiality safeguards. But the former employer may be able to state

a claim under the CFAA, so long as it can demonstrate that the costs resulting from the unauthorized access exceed $5,000.

Misappropriation of trade secrets is an intentional tort.[26] Thus, a former employer must show more than the employee's mere possession of the alleged trade secret, or (in most jurisdictions, including California) that use or disclosure of the trade secret is "inevitable" given the nature of the new employment. Instead, an employer must show that the former employee has actually used or disclosed the trade secret, or that there is a "substantial threat" of use or disclosure.[27]

Similarly, to establish a violation of a confidentiality or nondisclosure agreement, a former employer must prove that the former employee has in fact breached the obligation by disclosing or threatening to disclose the confidential information. The former employer generally must have at least some evidence about what the departing employee is doing at the new employment—such as the position that the employee now holds, and the substantive areas in which the employee is now involved.



By contrast, a plaintiff suing under the CFAA is frequently in control of all facts needed to establish the violation. The former employer usually can establish, through a forensic computer examination, when, how, and to what extent its computers were accessed by the departing employee. The former employer usually will be able to determine by itself whether the access was authorized. Moreover, a former employer need only show costs of $5,000 required to investigate and remedy the problem caused by the departing employee in order to satisfy the CFAA's loss requirement. Thus, the CFAA plaintiff need not set forth specific evidence about what the former employee is doing at the new employment in order to establish a violation.

According to the act, "[a]ny person who suffers damages or loss by reason of a [CFAA violation] may…obtain injunctive relief and other equitable relief."[28] The successful CFAA plaintiff should be able to obtain an injunctive order that, at a minimum, requires the former employee to return all the company's improperly accessed materials, refrain from using any accessed information, and desist from further accessing the company's computer system.

Also, because the CFAA allows a plaintiff to obtain "other equitable relief,"[29] the successful plaintiff actually may be able to obtain an even broader injunction than one obtainable under a trade secrets or breach of confidentiality theory. For example, a plaintiff may be able effectively to prevent a former employee from working in a certain field or subject area by seeking an injunction preventing the use of any information that could have been derived from improperly accessed information on the former employer's computer. This may be a far broader injunction than one limiting the former employee's use of trade secrets.

Prevention and Defense

In view of the incentives to former employers to use the CFAA, it is important for new employers to take preventive steps when hiring new employees—especially those who worked previously for a competitor. Moreover, because a federal court examining a proposed injunction sits in equity, preexisting preventive measures can play an important role in limiting the scope of any potential injunction.

Employers hiring employees who worked with computers at their former employment should consider taking a number of precautionary steps. The most effective way to prevent CFAA claims is to limit the scope of information "taken" by a new hire from the former employer. During the interview process, the new employer should make clear that potential employees must not gather information from their former employer at any time. Once hired, the new employer should require the new employee to certify that the employee has returned all computerized information to the prior employer before beginning work. Further, the new employer should instruct the new employee to refrain from transferring any preexisting data or information to the new employer's computer without the express consent of the new employer. The new employee's compliance with these requests should be clearly documented. Because a new employee's direct supervisor may not be aware—or may choose to remain ignorant—of the risks associated with a new hire bringing information taken from a former employer, preventive measures like these should be incorporated into the normal hiring process.

Still, litigation is sometimes unavoidable despite the presence of an employer's preventive measures. For employers forced to defend against CFAA claims, a number of litigation strategies could potentially limit exposure to, or defeat, a CFAA cause of action.

A defendant employer may be able to defend against a CFAA claim by showing that the employee's access to the former employer's computer system was for legitimate, work-related reasons. This is a highly fact-based showing that will focus on the former employer's specific allegations of unauthorized access and the circumstances under which the employee actually accessed the information. While it is conceivable that an employee may have accessed a computer at the behest of the future employer, simply because an employee, in fact, accessed the computer after accepting a job (or even after an interview) obviously does not establish that all further use of the computer was unauthorized.

Therefore, simply because unauthorized access can be easily alleged does not mean that it should be conceded—especially in the context of a motion for a preliminary injunction. Counsel for the departing employee and new employer should work closely together to determine the precise factual circumstances surrounding each alleged access of the former employer's computer system. The objective is to establish that the conduct was benign.

Depending on the dynamics of the situation, the new employer may want to distance itself from the new employee. The employer may want to establish that, even if the former employee engaged in unauthorized access, he or she was neither acting as the new employer's