K&LNG Alert

MAY 2005

Employment Law

Securing Computers and Terminating Employees: A Short (and not very Sweet) Case Study

A recent criminal case in Michigan, affirmed on appeal, has provided a useful case study into some of the adverse consequences that result when employers underestimate the potential damage that can be done to the company's assets by an employee who has been terminated. This Client Alert reviews the factual situation presented in that case and offers suggestions that companies may wish to evaluate in structuring their termination processes.

THE CASE OF THE DISGRUNTLED EMPLOYEE

In Michigan v. Schilke, 2005 Mich. App. LEXIS 1079 (May 3, 2005), the Court of Appeals of Michigan considered an appeal from the criminal conviction of Valrene Mae Schilke. Schilke was convicted by a jury of one count of unauthorized access to a computer, based upon her conduct at the time of, and following, her termination of employment by Express Management Services ("EMS"). In her job at EMS as a "technical analyst," Schilke had administrative access to the EMS computer network as well as the "administrator password" for the system. This password served as a "master key" to the network, allowing complete, unfettered access to add or delete files or users or revoke user access privileges. Schilke also had access from her home computer, through the creation of a "virtual private network," to the EMS network.

While Schilke was at her desk, her supervisor and the EMS human resources director arrived to notify her that her employment was being terminated. While being told, and despite instructions to stop, Schilke continued typing on her computer, proclaiming, in explicit street language, her intent to get even with EMS. When the supervisors left to get someone to disconnect Schilke's computer, they returned to a barricaded office. Only after police were called did the terminated employee leave the premises. By then, Schilke had already done a lot of damage.

Following Schilke's departure, EMS learned that she had disabled the administrative password—the "master key"—thereby making it difficult for EMS to disconnect Schilke's access. Schilke then accessed the EMS network remotely from her home. Ultimately, EMS literally pulled the plug to disconnect their server from the remote access that had been established, thus rendering them unable to function for over 20 hours. Evidence presented to demonstrate the level of damage done by Schilke indicates that EMS incurred nearly $60,000 in lost revenue and system restoration expenses.

The court indicated that Schilke had succeeded in deleting all but three of the network user accounts, deleting the event log on the system (which records the actions taken), changing the designations for computer disk drives and taking other actions which resulted in a significant loss of data in the process. Schilke also admitted she had physically removed, at the time she left the premises, physical backup tapes and CDs containing customer loan information.

Schilke was convicted under a Michigan criminal statute that makes illegal any intentional actions (including actions without authorization or in excess of available authorization) to access or cause access to a computer, computer system or computer network in order to acquire, alter, damage, delete or destroy property or

otherwise misuse any computer program, computer, computer system or computer network (MCL §752.795(a)). Her appeal was denied, based on evidence of the expenses incurred by her employer in loss of business and systems restoration.

RECOMMENDATIONS

In the 21st Century, companies must be aware of the potential damage that employees can cause through computer access to the company network. As indicated by Schilke, even employees without executive responsibilities often lawfully possess the digital tools with which to cause tremendous harm in a very short period of time. Moreover, as described in a Client Alert we recently published (see **USB Drives: Opportunities and Risks for Employers**, March 2005), employees have technology resources that can make the duplication and removal of valued data easy to accomplish. Of course, there is a sliding scale of potential harm to be considered: employees with direct responsibility for security controls, IT infrastructure, database management and similar duties, while vested with some of the most important responsibilities for securing the enterprise, must be subject to appropriate, commensurate controls.

Here are some recommendations for how companies can improve their management of termination events, and reduce the risks that such events may produce disruptions and losses to their operations:

Companies should express in employment manuals and other suitable locations (including online sign-on screens) the ownership rights of the employer with regard to the computing systems made available and obtain the employee's written or electronic acknowledgement that their use of those systems is subject to the employer's policies.

A company's electronic communications policy should expressly reserve to the employer the right to monitor an employee's use of the communications systems in accordance with applicable law.

Companies should explicitly state that employees have no rights to access or use the employer's computing systems at any time before or after their employment. Companies that permit personal use of their computers should address in their employment manuals what policies, if any, exist for allowing employees access to computer-based records of a personal nature (such as rolodex entries) following termination of employment.

In the event an employee is to be terminated, companies should include in their termination process an occasion—prior to giving the employee notice—to evaluate the impact of the termination on computing operations and the level of risk that is associated with the subject employee. Planning is an essential strategy for minimizing events similar to those accomplished by Schilke.

While an employee is in a termination meeting (or perhaps the previous night, provided termination will occur first thing the next morning), employers should be prepared to terminate computer access, computer accounts, passwords, remote access privileges and similar functions. Security badges and other access devices can be deactivated during the termination meeting, as appropriate. If employment is to continue for a set period, IT security personnel can then make adjustments to suitably protect any corporate information or computing functions.

In any termination situation, the termination meeting should be held in a location different from the location at which the employee performs his or her work. Additional management personnel should be aware that a termination meeting is occurring and available to intervene if required; of course, if the circumstances suggest the need for greater security, arrangements for security personnel can be considered. As the Schilke case illustrates, a lot of damage can be rendered to data and systems in a very short period of time while security personnel are sought. But a conspicuous or public display of security can also provide the basis for an employee to claim harassment, false arrest or slander by actions.

When employees are provided with keys, laptops or other mobile devices, their continued use of those assets should be suspended. Companies may wish to expressly require that any final termination payment be conditioned upon the return in satisfactory condition of all company resources; however, to be implemented, that approach requires careful legal review. In some states, payroll setoffs are not allowed. For example, in California, it is unlawful to withhold *any* pay from an employee pending return of property;

rules require an employee to be given their final paycheck at the time and place of termination, including all accrued earned vacation, as well as wages earned through the last day of employment. *See* Cal. Labor Code §201.

When employees are being considered for termination, companies will often elect to review and access the employee's electronic mail to determine whether their communications records provide further cause for termination. Companies should use care in doing so, particularly if the business has not previously adopted policies that establish the company's right of access to those records. At the Federal level, the Electronic Communications Privacy Act, 18 U.S.C. §§2510, et seq., prohibits certain types of active monitoring, but generally permits the review of employee e-mail records after they have been transmitted and stored. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003) (that type of surveillance and monitoring must be properly engineered in order to avoid potential difficulties that could disrupt the planned termination). But in some jurisdictions, notably Delaware, employers are required to provide written prior notice of any monitoring or interception of telephone, Internet or e-mail use (*see* 19 Del. Code Ann. §705).

Taking steps such as those suggested above can significantly reduce the chance that a terminated employee will be able to cause any harm to the company or its computers.

Jeffrey B. Ritter
jritter@klng.com
202.778.9396

Hayes C. Stover
hstover@klng.com
412.355.6476

Linda L. Usoz
lusoz@klng.com
650.798.6702

K&LNG regularly advises our clients regarding the intersection between employment law and information technology, providing counsel to our clients across several different legal disciplines, including:

- Employment and Labor Law
- Privacy, Data Protection and Information Management
- Technology
- Corporate

For further information regarding our experience, as well as additional Client Alerts addressing related topics, please visit www.klng.com or contact any of lawyers listed below.

Boston	Henry T. Goldman	617.951.9156	hgoldman@klng.com
	Mark D. Pomfret	617.261.3147	mpomfret@klng.com
Dallas	Jaime Ramón	214.939.4902	jramon@klng.com
Harrisburg	Carleton O. Strouss	717.231.4503	cstrouss@klng.com
London	Paul Callegari	+44.20.7360.8194	pcallegari@klng.com
Los Angeles	Thomas H. Petrides	310.552.5077	tpetrides@klng.com
	Paul W. Sweeney, Jr.	310.552.5055	psweeney@klng.com
Miami	April L. Boyer	305.539.3380	aboyer@klng.com
	Carol C. Lumpkin	305.539.3323	clumpkin@klng.com
	Michael C. Marsh	305.539.3321	mmarsh@klng.com
Newark	Rosemary Alito	973.848.4022	ralito@klng.com
	Vincent N. Avallone	973.848.4027	vavallone@klng.com
	Marilyn Sneirson	973.848.4028	msneirson@klng.com
New York	Eva M. Ciko	212.536.3905	eciko@klng.com
Palo Alto	Linda L. Usoz	650.798.6702	lusoz@klng.com
Pittsburgh	Stephen M. Olson	412.355.6496	solson@klng.com
	Michael A. Pavlick	412.355.6275	mpavlick@klng.com
	Hayes C. Stover	412.355.6476	hstover@klng.com
San Francisco	Jonathan M. Cohen	415.249.1029	jcohen@klng.com
Washington	Lawrence C. Lanpher	202.778.9011	llanpher@klng.com
	Jeffrey B. Ritter	202.778.9396	jritter@klng.com

Kirkpatrick & Lockhart Nicholson Graham LLP

www.klng.com

BOSTON ▪ DALLAS ▪ HARRISBURG ▪ LONDON ▪ LOS ANGELES ▪ MIAMI ▪ NEWARK ▪ NEW YORK ▪ PALO ALTO ▪ PITTSBURGH ▪ SAN FRANCISCO ▪ WASHINGTON

Kirkpatrick & Lockhart Nicholson Graham (K&LNG) has approximately 950 lawyers and represents entrepreneurs, growth and middle market companies, capital markets participants, and leading FORTUNE 100 and FTSE 100 global corporations nationally and internationally.

K&LNG is a combination of two limited liability partnerships, each named Kirkpatrick & Lockhart Nicholson Graham LLP, one qualified in Delaware, U.S.A. and practicing from offices in Boston, Dallas, Harrisburg, Los Angeles, Miami, Newark, New York, Palo Alto, Pittsburgh, San Francisco and Washington and one incorporated in England practicing from the London office.