Insights, News & Events

‘E-TRADE SECRET’ THEFT ON THE NEW FRONTIER: UNDER AWARE AND OVEREXPOSED

Publication
Oct 1, 2009

Companies need to wake up to the threat of “e-trade secrets” theft, and the recent high-profile cases involving UBS Financial Services and Goldman Sachs Group Inc. are sounding the alarm. In each case, former UBS and Goldman employees are accused of absconding with valuable trade secrets in electronic format – in the form of computer code – from their respective former employers and using the trade secrets to compete unfairly against them. Goldman’s former employee is accused of transferring and encrypting 32 MB of source code for Goldman’s proprietary high-speed trading program. UBS alleged its former employees stole 25,000 lines of source code that enabled UBS to compete more effectively in algorithmic trading.

PROTECTING E-TRADE SECRETS ON THE NEW FRONTIER

Surviving on the new frontier has forced many risk management, general counsel, human resources, and information technology professionals to take a proactive and comprehensive approach to protecting their e-trade secrets. With so many employees connected to the internet and corporate intranets through individual computer workstations, some employers have built e-trade secret infrastructures designed to protect their most valuable assets. These models are cost-effective and relevant to any industry that depends on the control of proprietary assets or information.

These steps include:

Related People

Brent A. Cossrow
Regional Managing Partner
610.230.2135

- Designating an E-Trade Secrets Point-Person
- Recruiting an E-Trade Secrets Team
- Retaining Outside Counsel
- Identifying Your E-Trade Secrets
- Determining Whether Open Source Code Needs To Be Removed
- Reviewing or Drafting Protective Documentation
- Drafting the Playbook
- Conducting Regular Team Meetings

Companies committed to e-trade secret protections have adopted an almost militarized approach to these steps. On short notice, these companies can mobilize a task force consisting of key management personnel, outside e-trade secret "enforcement" counsel, and external computer specialists to lock down corporate computers and digital data storage devices in order to determine whether a departing employee transferred any data from his or her corporate computer. Not surprisingly, timing is of the essence on the new frontier: departing employees intent on stealing e-trade secrets can use e-mail or a thumb drive to transfer thousands of pages of documents in a matter of seconds from one computer to another.

Taking these steps now can make the difference in protecting a company's e-trade secrets from theft or dilution. Our courts are seeing employees who resign with little or no notice and accept employment at a competitor, as alleged in the cases of the former UBS and Goldman employees. These cases tend to involve familiar fact patterns: after the employee resigned, the employer's information technology staff reviewed the former employee's corporate computer and found several emails sent to an unfamiliar e-mail address; and attached to the e-mails were client lists, spreadsheets or power point presentations. In other cases, the digital trash can on the corporate computer is full of deleted files. In some instances, the information technology staff has determined that a former employee attached a thumb drive to the corporate computer within hours of his resignation. The distinguishing feature in these cases tends to be employer's level of preparedness for such contingencies. Where an

employer has made the investment to build an e-trade secret infrastructure customized to its business, the employer can identify quickly whether any data was transferred, whether the data constitutes an e-trade secret, when it was transferred, and the computers and/or devices used to effectuate the transfer. Such employers tend to be well positioned to enforce their rights against a departing employee or competitor intent on stealing e-trade secrets. The central question facing employers on the new frontier is whether they too will take the steps necessary to protect themselves and their most valuable assets.

This article appeared in the October 2009 edition of *Bloomberg Law Reports - Risk & Compliance*.