HINSHAW

Implementing a Policy Review to Ensure You Are Protected Under The Computer Fraud and Abuse Act, Part 1: Why You Should Conduct a Policy Review

2 min read

Oct 10, 2017

By: Ambrose V. McCall

Ambrose McCall will be presenting "The Computer Fraud and Abuse Act: Navigating the New Normal of Workplace Technology and Cybersecurity" on Thursday, October 12, 2017, at the 22nd Annual Labor & Employment Seminar. This year's Seminar will be held at the Hilton Chicago-Northbrook in Northbrook, Illinois. Please visit our website for more details.

One size rarely fits all, especially where technology is concerned. So too is employer coverage under the Computer Fraud and Abuse Act ("CFAA"). Cookie-cutter molds for aspects of your business simply do not work.

Certain situations readily qualify for coverage under the CFAA, such as when current or former employees hack into employer databases or files that were always off-limits to the employee, such as:

- Databases that contain highly protected financial data with account numbers that employees could use to misappropriate funds;
- Digital files that contain confidential business strategies that the employee accesses to alter, delete, or erase its digital files so that the employer must reconstruct the file, which usually involves significant costs to the employer; and
- Digital files with confidential proprietary client contact and marketing data that a current employee, acting as a conduit to a former employee who now lacks authorized access, removes or transfers with the purpose of permanently damaging the digital files at great cost to the employer.

The employer's protections under the CFAA, however, extend beyond these more common examples. The CFAA also can protect employers that enforce existing policies against current employees who may have arguably exceeded their authorized access to the employer's computers, networks, and digital files.

© 2025 Hinshaw & Culbertson LLP

The humility that comes with experience has taught many of us that no magic policy language exists that can transform an employee's marginal violation of your authorized access policy into a clear violation which is covered by the CFAA. Therefore, employers should examine their policies and processes as a whole with an eye toward determining whether their policies and practices work cohesively to prohibit an employee's access to designated computers, networks, and digital files, and that the employer is adequately protected from employee misconduct under the CFAA. In Part 2 of this series, we will provide detailed guidance on how to conduct your policy review and questions that you should consider throughout the policy review to ensure you are protected under the CFAA.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Topics

CFAA, Compliance Audit